Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2024/004

Audit of information and communications technology governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change

Strategic direction, governance, security and project management need to be strengthened to fully leverage the benefits of investments in information and communications technology

12 February 2024
Assignment No. AT2023-241-01

Audit of information and communications technology governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change (UNFCCC). The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes relating to ICT governance, operations, security and project implementation at UNFCCC. The audit covered the period from January 2020 to September 2023 and included a review of: (i) strategic direction and governance; (ii) operations; (iii) security; and (iv) project implementation.

The audit showed that UNFCCC's strategic direction, governance, security and project management need to be strengthened to fully leverage the benefits of investments in ICT.

OIOS made 14 recommendations. To address the issues identified in the audit, UNFCCC needed to:

- Establish an ICT strategy aligned with its business objectives; approve strategic and tactical plans to ensure effective implementation of the ICT strategy; and establish priorities to implement an enterprise architecture thereby reducing fragmentation of systems and eliminating silos;
- Establish an ICT Governance Committee and ICT Technical Committee and document their detailed terms of reference;
- Consider the two previous external studies on the size and placement of its ICT function and establish an effective ICT service delivery model; assess the risks and costs of excessive dependency on external parties for project management, business analysis, testing, quality assessment and ICT security; and identify its short and long term ICT staffing requirements to effectively address current bottlenecks in responding to business needs;
- Establish an ICT risk assessment process integrating ICT risks into its Enterprise Risk Management covering its entire ICT landscape (including ICT services, systems, projects, cybersecurity and data privacy) with appropriate risk response plans;
- Establish a data governance and management framework with procedures, roles and responsibilities; and implement data privacy procedures including protection of sensitive personal information stored in its ICT systems;
- Implement a roadmap to modernize its aging infrastructure running out of vendor support and applications using obsolete authentication systems; document business continuity plans with expected recovery time and recovery point objectives; and document and test the disaster recovery plans for all its applications;
- Establish an ICT security roadmap that is approved by management, with appropriate resources assigned; and document procedures for periodic vulnerability assessment and patch management;
- [redacted]
- [redacted]
- Update its ICT service catalog with all services provided, including professional services; and determine service rates using a transparent methodology;

- Establish a service monitoring process; conduct periodic client satisfaction surveys; and (c) take action to close the gap between expected service levels and ICT capacity;
- Fully implement the configuration management system; establish procedures for configuration management, security incident response and change management; and capture all incidents and changes in central repositories;
- Document a detailed breakdown of the cost of the new project replacing the Digital Platform for Climate Change Events; approve the business case and project plan; and document a procurement plan to implement the project; and
- Complete the comprehensive detailing of all remaining user stories for the Enhanced Transparency Framework Reporting Tools project taking into account their integration, flow (user journeys) and dependencies; establish a realistic time and cost schedule for delivery of the remaining user stories; and strengthen project management by defining and monitoring key performance indicators.

UNFCCC accepted the recommendations and has initiated action to implement them. Actions required to close the recommendations are indicated in Annex I.

CONTENTS

Audit of information and communications technology governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change (UNFCCC).

2. The UNFCCC secretariat supports all institutions involved in international climate change negotiations, particularly the Conference of the Parties (COP), the meeting of the Parties (CMP), the subsidiary bodies that advise the COP/CMP, and the COP/CMP Bureau which deals mainly with procedural and organizational issues arising from the COP/CMP.

3. The ICT sub-division is one of the three sub-divisions of the Administrative Services/Human Resources/ICT (AS/HR/ICT) Division that reports to the Director for Operations Coordination. The ICT sub-division is the central service provider of ICT infrastructure and user support services as well as information systems development, maintenance and application support in UNFCCC. It is made up of five units, viz. Project and Service Management Unit, Application Development Unit, Infrastructure and Systems Unit, Customer Support Unit and International Transaction Log (ITL) Unit.

4. The ICT sub-division employed 39 staff which were augmented with consultants and contractors as needed. The ICT sub-division supported about 650 staff users of ICT services and had Framework Division Agreements (FDAs) to provide ICT services to UNFCCC Divisions. UNFCCC migrated the majority of its applications and infrastructure to Microsoft Azure Cloud in 2019. Workplace infrastructure and residual legacy SharePoint services were stored in an on-premises data centre.

5. The core operations of UNFCCC were funded from contributions of the Parties. The ICT sub-division was funded from the core budget and seven other funding sources. The total ICT funding for the 2022-2023 biennium was over Euro 28 million as shown in Table 1.

Table 1: UNFCCC ICT budget and expenditure for the 2022-2023 biennium by funding source

Funding source	Budget 2022-23 Euro (000)	Expenditure Jan 22 – Sep 23 Euro (000)	Funding source percentage of expenditure
Core budget	3,754	3,290	16
ITL Trust Fund	2,740	1,609	8
Framework Programme Agreements	13,322	9,965	48
TCO	5,983	5,185	25
Bonn Fund	338	363	2
Other Supplementary funded projects	2,825	284[1]	1
Total	**28,962**	**20,696**	**100**

All figures exclude programme support costs.

6. Comments provided by UNFCCC are incorporated in italics.

[1] Low expenditure was because actual available supplementary funding from donors was much lower than the budget.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

7. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes relating to ICT governance, operations, security and project implementation at UNFCCC.

8. This audit was included in the 2023 risk-based work plan of OIOS due to high risks in the areas of ICT governance, operations, security and project implementation at UNFCCC.

9. OIOS conducted this audit from July to October 2023. The audit covered the period from January 2020 to September 2023. Based on an activity-level risk assessment, the audit covered risk areas pertaining to ICT which included: (i) strategic direction and governance; (ii) operations; (iii) security; and (iv) project implementation.

10. The audit methodology included: (a) interviews with key personnel; (b) reviews of relevant documentation; (c) analytical review of data; (d) questionnaires; (e) physical observation; (f) walkthrough of processes; and (g) review of ICT systems and infrastructure.

11. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

III. AUDIT RESULTS

A. Strategic direction and governance

Need to reestablish an ICT strategy and implement an enterprise architecture

12. Successful achievement of UNFCCC's objectives relies on efficient and effective ICT governance and management. Development and implementation of an ICT strategy that serves as a roadmap for utilizing ICT to achieve organizational goals is an integral part of ICT governance. The strategy should define key ICT priorities, investments and deliverables with a specified timeframe, aligned with the organization's mandate, strategic plans and operations.

13. UNFCCC's ICT strategy was approved by its Management Committee in 2015 outlining key objectives, strategic initiatives, and priorities. However, when UNFCCC initiated an entity-wide restructuring process in 2018, the ICT strategy was neither reassessed nor updated. The changing priorities and ICT resources were not discussed in the Management Committee.

14. An effective ICT strategy considers enterprise architecture, maximizing the use of common, reusable components. Major projects such as the Enhanced Transparency Framework (ETF), annual COP conferences and the ITL system received individual funding that was used solely for those projects. They operated independently without alignment through a common enterprise architecture which is essential for efficiency. The ICT sub-division recognized the risks and documented a draft enterprise architecture model to promote reusability across divisions, covering areas such as identity and access management, event and stakeholder relationship management, a centralized data warehouse, and a content management system. However, this initiative was not presented to the Management Committee and as a result, it did not advance to the status of a strategic objective.

15. The absence of an approved ICT strategy resulted in existing ICT resources being allocated to various projects on an ad-hoc basis to address the most immediate needs. Several systems were developed

and operated in isolation, despite serving similar functions, without alignment with an enterprise architecture and strategy. For example, there were 11 registration systems, all serving similar purposes. Additionally, some systems were independently developed and maintained by individual business divisions, resulting in further fragmentation. Several outdated systems did not receive adequate attention for upgrades due to lack of prioritization and funding which led to critical vulnerabilities. Lack of integration among multiple data repositories and data sources hindered effective use of data in UNFCCC.

(1) UNFCCC should: (a) establish an ICT strategy aligned with its business objectives; (b) approve strategic and tactical plans to ensure effective implementation of the ICT strategy; and (c) establish priorities to implement an enterprise architecture thereby reducing fragmentation of systems and eliminating silos.

UNFCCC accepted recommendation 1 and stated that it is in the process of establishing a new ICT strategy. Subject to the endorsement of the strategy, the ICT sub-division will take appropriate measures for its implementation. Within its processes, ICT will continue to seek out opportunities for efficiency in services and modes of operation.

Need to establish ICT governance committees

16. The ICT Governance Committee (or ICT Board) plays a pivotal role in an organization by facilitating the alignment of ICT initiatives with the strategic goals of the business. Its primary function is to ensure that ICT investments, projects and priorities are in sync with the overall business objectives. It serves as a forum for evaluating, prioritizing and monitoring ICT projects, enabling resource allocation, and effective execution of projects that deliver the intended benefits.

17. UNFCCC had abolished the ICT Governance Committee during the organizational restructuring which started in 2018 and did not establish any other mechanism to replace it since then. Furthermore, the Chief of the ICT sub-division was not a member of the other governing bodies in UNFCCC such as the Management Committee and Finance Committee, because only division heads were represented in these committees. ICT was indirectly represented in these meetings through the Director of AS/HR/ICT. OIOS' review of the meeting minutes of these committees showed that ICT risks or ICT strategic objectives were not a regular agenda item in these meetings. The only governance mechanism that existed was at the project board level for large projects.

18. The absence of an ICT Governance Committee was a significant gap in UNFCCC's ability to align its ICT resources with its objectives, with appropriate ICT investment at an enterprise level. For instance, the ICT project portfolio which encompassed new projects, enhancements and services requested by various business divisions or identified by the ICT department, contained 157 initiatives that were either in "red" health status or "pending assessment" due to resource conflicts that caused these initiatives to encounter delays. Establishing an ICT Governance Committee comprising senior management, business managers and ICT experts can help align ICT with UNFCCC's priorities and address risks related to aging systems, unsupported systems, data silos and ICT security at the enterprise level.

19. UNFCCC also did not have an ICT Technical Committee composed of ICT focal points of various divisions to facilitate cross-functional collaboration and knowledge-sharing among various divisions. Such a committee could reduce redundancy and promote the development of common standards and approaches for ICT-related matters, leading to cost savings and more streamlined ICT operations.

(2) UNFCCC should establish an ICT Governance Committee and ICT Technical Committee, and document their detailed terms of reference.

UNFCCC accepted recommendation 2 and stated that ICT is represented at the Management Committee by the ICT Manager and Director AS/HR/ICT for governance. The ICT Technical Committee and terms of reference will be developed and established in 2024. Other relevant actions for this recommendation will be completed by the end of 2025.

Need for an effective ICT service delivery model

20. The UNFCCC restructuring process initiated in 2018 and completed in 2020 significantly impacted the capacity and positioning of the ICT function. Prior to restructuring, the ICT function was a division with 61 staff members composed of three sub-divisions (ICT Governance, ICT Application Delivery, ICT Operations) and held a direct representation in the Management Committee and Finance Committee that operated under the guidance of an ICT Governance Committee. During the restructuring, major ICT positions including the Director, three P-5s and various other roles were abolished, and ICT was downgraded into a sub-division with 35 staff. This change did not align with the recommendations made by the consulting company which had been engaged to guide the restructuring. It also did not align with the results of the assessment of a previous consultancy service provided by another vendor, which had concluded that the structure and size of the ICT function were adequate in 2015. After the restructuring, the ICT sub-division was placed under AS/HR/ICT.

21. ICT requirements of UNFCCC have been increasing consistently following the restructuring due to the need to implement new mandates that depend on ICT solutions. One of the immediate consequences of the restructuring was the necessity to outsource core activities of the ICT sub-division such as management of critical ICT projects, implementation of systems and applications, analysis and documentation of business requirements, ICT security operations and ICT security management.

22. OIOS' review showed that the current capacity of the ICT sub-division was inadequate to meet the growing ICT requirements and risks across various business divisions of UNFCCC which resulted in slow response to support requests and project requirements. Additionally, the risks associated with various critical and aging applications were not addressed in a timely manner. OIOS noted the following:

(a) Excessive dependency on outsourcing resulted in delays and inefficiencies. Before restructuring, two dedicated ICT units (Rapid Application Services Unit and Requirements Engineering Unit) with eight staff were responsible for handling small-size projects and requirements of UNFCCC. However, following the restructuring, these units were disbanded with the result that there were delays in addressing important projects due to a lack of internal capacity. UNFCCC stated that challenges in finding a vendor willing to implement these small-size projects, along with additional time required for procurement activities, contributed to the delays in meeting the emerging needs of various divisions. For example, the Conference Affairs Division had to hire the services of a United Nations agency to implement data analytics services resulting in a 3-month delay. Additionally, some large projects such as ETF depended highly on external consultants for a long time for support activities such as business analysts and testers. This increased the risk of lack of continuity and institutional knowledge which hindered the ability of UNFCCC to capitalize on the experience gained for use in future projects.

(b) Changing priorities within ICT impacted the delivery of critical projects. For example, the Digital Platform for Climate Change Events **(**DPCCE) project which aimed to develop an enterprise solution for conference and event management by replacing obsolete systems had started as a $5.8 million project. Due to emerging priorities, the project's focus shifted to the delivery of interim solutions for the approaching COP conferences rather than implementing a long-term solution addressing the risks of aging systems. In another case, the Paperless (GrandReserva) project was initiated, with scope defined and funds provided. After the work was initiated, the project was frozen due to reprioritization of its resources to other activities.

(c) Individual user requests and reported incidents were not addressed in a timely manner. As a test, OIOS created a help desk request during the audit by reporting an incident. No response was received several days after the request was made.

23. Inadequate resourcing of ICT needs to be addressed to ensure that UNFCCC's mandates are achieved efficiently and effectively.

(3) UNFCCC should: (a) consider the two previous external studies on the size and placement of its ICT function and establish an effective ICT service delivery model; (b) assess the risks and costs of excessive dependency on external parties for project management, business analysis, testing, quality assessment and ICT security; and (c) identify its short and long term ICT staffing requirements to effectively address current bottlenecks in responding to business needs.

UNFCCC accepted recommendation 3 and stated that the review and decisions on ICT staffing approach, costs and management of business needs are part of the collective responsibilities of management that has direct or indirect oversight of ICT. Eventual actions based on management approval and budgetary availability on this recommendation will be implemented during the biennium 2024-2025.

Need to enhance ICT risk management

24. The Enterprise Risk Management (ERM) process requires a comprehensive framework for identifying, assessing and mitigating risks across an organization. UNFCCC was in the process of developing ERM policies and procedures. UNFCCC had not conducted an ICT risk assessment to identify and mitigate potential risks that may hinder the achievement of its strategic and operational objectives. The ERM risk register did not capture the entire ICT risk landscape such as cybersecurity risks, continuity and privacy risks. The lack of adequate ICT risk management may weaken UNFCCC's ability to protect its assets and detect, respond to, and prevent cybersecurity incidents.

(4) UNFCCC should establish an ICT risk assessment process integrating ICT risks into its Enterprise Risk Management covering its entire ICT landscape (including ICT services, systems, projects, cybersecurity and data privacy) with appropriate risk response plans.

UNFCCC accepted recommendation 4 and stated that the ICT sub-division will participate in the establishment of an ERM programme, as part of an overall UNFCCC ERM led by the Organizational Development and Oversight Unit.

Need to establish a data governance and data privacy programme

25. The Secretary-General's data strategy proposed a comprehensive framework to support accelerated data-driven transformation of members of the United Nations family through better use of data as a strategic asset. In 2018, the High-Level Committee on Management of the Chief Executives Board for Coordination adopted the Principles on Personal Data Protection and Privacy.

26. The data collected and generated by UNFCCC was scattered across multiple divisional databases and managed in silos by various units, leading to duplication and a lack of awareness about existing data sources. In 2017 and 2019, a team comprising UNFCCC staff from various divisions collaborated to establish data catalogs and document a draft data governance framework to enhance organizational

efficiency. However, these efforts did not progress into a data governance framework approved by management.

27. As of September 2023, roles and responsibilities for data management (e.g., data custodians, data stewards, data owners), data governance and data privacy were not defined. There was no governance mechanism or body, organizational structure or individual tasked with coordinating and monitoring data governance and data privacy issues. Additionally, several ICT systems lacked adequate controls to classify and protect sensitive personal data of conference attendees including visa, passport, telephone and address information. Also, the acquisition of technological solutions did not undergo a formal legal or technical review to ensure that data privacy requirements were embedded or considered during their acquisition and development.

(5) UNFCCC should: (a) establish a data governance and management framework with procedures, roles and responsibilities; and (b) implement data privacy procedures including protection of sensitive personal information stored in its ICT systems.

UNFCCC accepted recommendation 5 and stated that the Organizational Development and Oversight Unit will coordinate the implementation in close consultation with the Operations Coordination Department. The relevant activities will be completed by the end of 2024.

B. Security

Obsolete and aging technology risks need to be mitigated

28. There was a rise in outdated technologies at UNFCCC. As many as 52 applications were running on legacy platforms and obsolete authentication systems (such as old versions of SharePoint, Active Directory, content management systems and Windows 2012 operating system) without vendor support or a clear upgrade plan. Additionally, several legacy applications were accessible by only application layer authentication methods, instead of Active Directory-integrated authentication and authorization. These outdated technologies pose ICT security risks to UNFCCC.

29. Furthermore, UNFCCC's website was running on an unsupported content management system with no plans for migration or upgrade. During the audit, the ICT sub-division proposed a transition to Drupal 10 for improved security, performance and accessibility. However, there was no formal roadmap with management commitment to address the risks. Additionally, there were still some unsolved issues and technical backlogs in the areas of recovery and automation, performance, security, setup and tuning, migration of old websites, and new features from the previous revisions done in 2017.

Business continuity and disaster recovery plans need to be documented

30. Effective business continuity and disaster recovery planning is crucial for continuity of business operations and data protection in the event of a potential adverse incident. UNFCCC divisions had not documented their business continuity plans and had not determined the recovery time and recovery point objectives of the ICT systems that their processes depended on. Over 190 systems serving UNFCCC and its stakeholders lacked disaster recovery plans, leading to unaccounted dependencies and unpreparedness for disruptions. Defining these objectives would help the ICT sub-division to plan, resource and deliver the required resilience requirements and contingency plans to minimize the impact of disruptions.

(6) UNFCCC should: (a) implement a roadmap to modernize its aging infrastructure running out of vendor support and applications using obsolete authentication systems; (b)

document business continuity plans with expected recovery time and recovery point objectives; and (c) document and test the disaster recovery plans for all its applications.

UNFCCC accepted recommendation 6 and stated that it will modernize its outdated infrastructures and decommission legacy applications in support of the proposed ICT strategy and roadmap. The relevant activities will be completed by the end of 2025.

Need to improve management's commitment in managing ICT security risks

31. International standards for information security management emphasize that senior management is expected to demonstrate leadership and commitment to the establishment, implementation, maintenance and continual improvement of information security to prevent the organization from falling victim to cybersecurity threats and vulnerabilities.

32. Identification of vulnerabilities and applying patches are crucial to keep the network and systems safe from known threats. UNFCCC did not have a consistent process to run vulnerability scans and implement measures to mitigate the existing risks to its systems (such as applying patches). The last penetration test was conducted in 2020 but UNFCCC was yet to complete remedial action to fix all high and medium vulnerabilities. Additionally, UNFCCC had 144 web-based applications of which 31 were mission-critical and were not consistently being scanned for vulnerabilities. During the audit, a few sampled systems, related load balancers, database servers, web servers, and application servers were scanned. The results indicated 56 vulnerabilities with varied severity. UNFCCC explained that the on-premises security audit planned in 2023 was deprioritized due to lack of resources for the exercise.

33. A United Nations agency hired by UNFCCC to conduct a cyber resilience maturity assessment in August 2022 made recommendations for Information Security Management System upliftment. This included establishment of a cybersecurity programme, integration of information security risks in UNFCCC's ERM, and improvement of existing security controls. UNFCCC was yet to implement these recommendations. Additionally, UNFCCC migrated most of its systems to a cloud environment in 2019, but did not define how its cloud security posture aligned with its enterprise risk appetite. Also, there was no mechanism to review and track security configuration settings.

(7) UNFCCC should: (a) establish an ICT security roadmap that is approved by management, with appropriate resources assigned; and (b) document procedures for periodic vulnerability assessment and patch management.

UNFCCC accepted recommendation 7 and stated that the establishment of an ICT security roadmap will require dedicated resources and management approval. Pending these decisions, ICT will develop and ICT security roadmap. The relevant activities will be completed by the end of 2024.

[redacted]

34. [redacted]

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

(f) [redacted].

(8) [redacted]

[redacted]

35. [redacted]

36. [redacted]

37. [redacted]

(9) [redacted]

C. Operations

An ICT service catalog needs to be established with clear service rates

38. The ICT sub-division provided services to UNFCCC divisions based on the signed FDA for each division. Funds collected through the FDA contributed to 25 per cent of the ICT budget for the 2022-2023 biennium, excluding programme support costs. OIOS noted the following:

(a) UNFCCC's ICT service catalog did not adequately reflect all the services provided by the ICT sub-division. There was no clear methodology or cost breakdown to calculate the total cost of ownership of ICT services provided to client divisions. For example, the service catalog did not contain service rates for professional services that could be determined by the daily cost of certain skilled professionals (mostly outsourced). The majority of the services covered in FDAs were in this category (such as application support, application maintenance, project management, project support and system monitoring). As a result, it was not transparent to the client divisions how the service charges in the FDAs were calculated. In some cases, rates updated in the service catalog were not reflected in the FDAs.

(b) The ICT sub-division provided bi-annual financial statements to reconcile actual costs with the budgeted cost recorded in each FDA. But there was no procedure describing how overpayments/ overcharges would be handled.

(10) UNFCCC should: (a) update its ICT service catalog with all services provided, including professional services; and (b) determine service rates using a transparent methodology.

UNFCCC accepted recommendation 10 and stated that it will update its ICT Service Catalog, include service rates, and publish them accordingly. The update will be completed in 2024.

Service quality and service level monitoring needs to be improved

39. FDAs were annexed with a service level agreement (SLA) that provided targets for incident response and resolution based on priority level and holiday/conference period. The ICT sub-division was not able to satisfy the defined service levels in the SLAs, and the help desk response time was reported as a systemic issue. While the target incident response and resolution times based on priority levels, 1, 2 and 3 during service hours were defined as within one hour, within 2 hours, and same day, respectively, there was no indication that the ICT sub-division provided regular performance monitoring reports on its FDA SLA to its client community. Additionally, some divisions provided 1st tier support for some of their applications resulting in a lack of a single point of contact and centralized repository to track requests and incidents. OIOS identified the following issues regarding service monitoring:

(a) The ICT sub-division did not produce help desk activity reports to support regular performance reviews for service improvement.

(b) During COP27, three ICT help desks were established across the international convention centre to support the COP. However, help desk performance and service support tickets from the COP service desks had not been analyzed.

(c) Client satisfaction surveys of the user community had not been conducted to assess the effectiveness of service provision within UNFCCC. Feedback from users could inform the ICT strategy and roadmap.

(11) UNFCCC should: (a) establish a service monitoring process; (b) conduct periodic client satisfaction surveys; and (c) take action to close the gap between expected service levels and ICT capacity.

UNFCCC accepted recommendation 11 and stated that ICT will determine ways to improve satisfaction through surveys and other mechanisms as part of ongoing processes throughout 2024-2025.

Need to enhance configuration, incident and change management

40. Best practices recommend the establishment of a supporting tool and central repository of all relevant information on hardware and software as well as virtual assets (i.e., configuration items) to track their configuration, along with monitoring and recording of all incidents and changes pertaining to them.

41. The ICT sub-division had deployed ServiceNow to support the configuration, incident and change management processes. However, implementation of the system was yet to be completed. At the time of the audit, the following activities were pending: (a) consolidation of all configuration items managed under various systems into a centralized configuration management database; (b) definition of dependencies between services, applications and their components; and (c) incorporating the location, warranty expiration, versions, vendor, serial numbers and IP addresses of network hosts into the system.

42. Further, there was no incident management procedure guiding how security incidents will be identified, reported, categorized, prioritized, escalated and handled. Also, the roles and responsibilities of users, UNFCCC ICT teams and third-party service providers were not clear. There was no centralized repository for capturing all security incidents across its systems. This impeded incident analysis, reporting and resolution of incidents.

43. UNFCCC had a change advisory board that evaluated and approved changes, but the change management procedure was still in draft and not consistently applied. As a result, changes were tracked in multiple systems such as Footprint, JIRA, MS Teams, emails and other third-party provider change management tools. OIOS' review of the list of implemented changes indicated lack of clarity as to whether change requests were being systematically evaluated for their impact. Also, the final decision on change requests (approval or rejection) was not being tracked. The absence of an adequate change management process could lead to unauthorized changes, inconsistent assessment of risks, and potential adverse impact of changes on applications and systems.

(12) UNFCCC should: (a) fully implement the configuration management system; (b) establish procedures for configuration management, security incident response and change management; and (c) capture all incidents and changes in central repositories.

UNFCCC accepted recommendation 12 and stated that the ICT sub-division will complete the deployment of approved ServiceNow tools and modules. The relevant procedures for configuration management, security incident response and change management will be revised in newly developed Standard Operating Procedures. Relevant actions will be completed by the end of 2024.

D. Project implementation

44. UNFCCC had documented a comprehensive project portfolio management framework in 2016 which included detailed procedures for demand and portfolio management, project start-up, project execution and project closure, as well as roles and responsibilities of various key players in these processes.

However, following the organizational restructuring that significantly impacted ICT resources, these procedures were not revisited and aligned with the new structure. This condition, combined with a lack of effective ICT governance, caused cost inefficiencies and delays in delivering the intended outcomes of various projects, as explained below.

(a) The Digital Platform for Climate Change Events (DPCCE) project

Project planning, governance and execution was inadequate

45. The DPCCE project, with an initial estimated budget of EUR 5.8 million for three years (2021-2023), was initially planned for completion by the end of 2023. It included major deliverables to replace legacy registration and meeting management systems with a new event and stakeholder relationship management solution, simplifying meeting management, event access and venue navigation that is integrated with the UNFCCC website.

46. Portions of the project budget were used to deliver interim tools and solutions that were implemented as proofs of concept to facilitate conferences in 2021, 2022 and 2023, rather than focusing on complete delivery of project requirements identified at the beginning. The interim/temporary solutions did not fully meet project requirements and the planned outcomes. Consequently, the project was put on hold, and a new proposal was developed in 2023 to achieve the same outputs with an estimated budget of EUR 8.6 million spanning from 2023 to 2026. The new draft project plan (2023-2026) included only high-level deliverables without details and clear dependencies. It also lacked detailed justification and breakdown of its estimated budget and required staffing resources, as well as an approved business case and project plan.

(13) UNFCCC should: (a) document a detailed breakdown of the cost of the new project replacing the Digital Platform for Climate Change Events; (b) approve the business case and project plan; and (c) document a procurement plan to implement the project.

UNFCCC accepted recommendation 13 and stated that the project scope was expanded to include the revamp of conferencing systems and not just the digital platform. The Conference Affairs as the business owner of the project will determine the necessary actions related to this organizational initiative by the end of 2025.

(b) The Enhanced Transparency Framework (ETF) Reporting Tools Project

User stories need to be detailed in a timely manner to facilitate advance planning

47. UNFCCC applied the Agile software development methodology for the ETF Reporting Tools project. Agile projects prioritize customer collaboration, responsiveness to change and incremental development. They typically focus on ongoing adjustments to the project based on changing priorities and feedback. Therefore, Agile methodology requires additional controls to minimize the risk of delayed implementation and budget overrun. Early identification and prioritization of key requirements (user stories and user journeys) in the interim deliverables is required to ensure that essential features are implemented even if budget constraints arise later. Additionally, the Project Board should monitor the project deliverables and cost performance based on relevant key performance indicators (KPIs).

48. OIOS noted the following:

(a) The Project Initiation Document did not include a clear estimated project budget with a breakdown of all cost components such as internal cost, implementing vendor cost, external consultancy cost for project management and support activities, and infrastructure cost.

(b) The Project Board did not determine KPIs to monitor project cost and performance.

(c) The scope and cost of each increment was determined just before implementation, and the remaining user stories of future increments were not detailed in a timely manner. At the beginning of the project, there were 559 user stories which increased to 665 by September 2023. The project was expected to reach a total of 1,339 user stories by its conclusion. Similarly, the complexity of the user stories also increased by 44 per cent during the first five increments which increased the risks of cost increase and delayed delivery of a complete solution. Adequate and timely detailing of each user story and user journey by business owners, and a roadmap that addresses dependencies and priorities, are essential.

(d) The delivered user stories were individually tested at the end of each increment according to documented test procedures. However, end-to-end user journeys (narratives that outline the steps and experiences a user goes through when interacting with the system) were not tested as effectively at the end of each increment. This may lead to unexpected issues and additional work at later stages, potentially requiring redesign and redevelopment of some functionalities leading to cost increases and delays.

(14) UNFCCC should: (a) complete the comprehensive detailing of all remaining user stories for the Enhanced Transparency Framework Reporting Tools project taking into account their integration, flow (user journeys) and dependencies; (b) establish a realistic time and cost schedule for delivery of the remaining user stories; and (c) strengthen project management by defining and monitoring key performance indicators.

UNFCCC accepted recommendation 14 and stated that in conjunction with the ETF Project Board recommendations, ICT will incorporate relevant actions for project delivery improvements. Activities will be completed by December 2025.

Suboptimal design of the contract

49. At the outset, UNFCCC documented the requirements of the ETF Reporting Tools project and based on requirements, the contract's Not-To-Exceed (NTE) amount was agreed to be $8.7 million with a completion date of December 2024. Although the project had a well-defined scope and requirements outlined in the Request for Proposal (RFP) with expectation of delivery in ten increments by December 2024, UNFCCC did not structure the contract to provide a turnkey solution that could have facilitated project delivery with a fixed cost. The contract only determined the cost per day for various services. UNFCCC stated that the contract was designed as a framework agreement because user requirements were planned to be detailed during implementation using Agile methodology. OIOS is of the view that framework agreements are suitable for continuous services with a unit price (cost per day) model for recurring professional services, but not for projects. As a consequence of this contractual structure, UNFCCC bore the risk of cost escalation for the solution. At the time of the audit, the estimated cost had already reached $9.3 million.

50. OIOS also observed procurement irregularities related to the contract. For example, the contract of $8.7 million was signed in January 2023 without the required review by the Headquarters Committee on Contracts. As of 13 November 2023, the contract had still not been reviewed by the Committee on ex post facto basis. The vendor had commenced work three months before contract signature, and purchase orders were issued after delivery of work. Delegation of authority thresholds for purchase orders were exceeded in all cases.

51. Based on OIOS' review of this and other contracts, the need for strengthening procurement planning and oversight was highlighted in a previous OIOS audit of the Transparency Division at UNFCCC (Report No. 2023/035). The related recommendation was still under implementation.

IV. ACKNOWLEDGEMENT

52. 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.

Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change

Rec. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	UNFCCC should: (a) establish an ICT strategy aligned with its business objectives; (b) approve strategic and tactical plans to ensure effective implementation of the ICT strategy; and (c) establish priorities to implement an enterprise architecture thereby reducing fragmentation of systems and eliminating silos	Important	O	Receipt of evidence of: (a) an ICT strategy aligned with business objectives; (b) approved strategic and tactical plans; and (c) established priorities to implement an enterprise architecture.	31 December 2025
2	UNFCCC should establish an ICT Governance Committee and ICT Technical Committee, and document their detailed terms of reference.	Important	O	Receipt of evidence of established ICT committees with detailed terms of reference.	31 December 2025
3	UNFCCC should: (a) consider the two previous external studies on the size and placement of its ICT function and establish an effective ICT service delivery model; (b) assess the risks and costs of excessive dependency on external parties for project management, business analysis, testing, quality assessment and ICT security; and (c) identify its short and long term ICT staffing requirements to effectively address current bottlenecks in responding to business needs.	Important	O	Receipt of evidence that: (a) the two previous external studies have been considered and an effective ICT service delivery model has been established; (b) risks and related costs of excessive dependency on external parties for project management, business analysis, testing, quality assessment and ICT security have been assessed; and (c) short and long term ICT staffing requirements have been identified.	31 December 2025
4	UNFCCC should establish an ICT risk assessment process integrating ICT risks into its Enterprise Risk Management covering its entire ICT landscape (including ICT services, systems, projects, cybersecurity and data privacy) with appropriate risk response plans.	Important	O	Receipt of evidence that an ICT risk assessment process has been established and integrated with ERM covering the entire ICT landscape of UNFCCC, with appropriate risk response plans.	31 December 2024
5	UNFCCC should: (a) establish a data governance and management framework with procedures, roles and responsibilities; and (b) implement data privacy procedures including protection of sensitive personal information stored in its ICT systems.	Important	O	Receipt of evidence of the establishment of a data governance and management framework and implementation of data privacy procedures.	31 December 2024
6	UNFCCC should: (a) implement a roadmap to modernize its aging infrastructure running out of	Important	O	Receipt of evidence that: (a) a roadmap to modernize the aging infrastructure has been	31 December 2025

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change

	vendor support and applications using obsolete authentication systems; (b) document business continuity plans with expected recovery time and recovery point objectives; and (c) document and test the disaster recovery plans for all its applications.			implemented; (b) business continuity plans has been documented; and (c) disaster recovery plans for all applications has been documented and tested.	
7	UNFCCC should: (a) establish an ICT security roadmap that is approved by management, with appropriate resources assigned; and (b) document procedures for periodic vulnerability assessment and patch management.	Important	O	Receipt of evidence of: (a) the establishment of an ICT security roadmap approved by management with appropriate resources assigned; and (b) documentation of procedures for periodic vulnerability assessments and patch management.	31 December 2024
8	[redacted]	Important	O	[redacted]	31 December 2025
9	[redacted]	Important	O	[redacted]	31 December 2024
10	UNFCCC should: (a) update its ICT service catalog with all services provided, including professional services; and (b) determine service rates using a transparent methodology.	Important	O	Receipt of evidence that: (a) the service catalog including professional services provided has been updated; and (b) a transparent methodology has been established for service rate calculation.	31 December 2024

[2] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.
[3] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.
[4] Please note the value C denotes closed recommendations whereas O refers to open recommendations.
[5] Date provided by UNFCCC in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations, security and project implementation at the United Nations Framework Convention on Climate Change

11	UNFCCC should: (a) establish a service monitoring process; (b) conduct periodic client satisfaction surveys; and (c) take action to close the gap between expected service levels and ICT capacity.	Important	O	Receipt of evidence that: (a) service management and monitoring processes have been established; (b) client satisfaction surveys are conducted; and (c) action is taken to close the gap between expected service levels and ICT capacity.	31 December 2025
12	UNFCCC should: (a) fully implement the configuration management system; (b) establish procedures for configuration management, security incident response and change management; and (c) capture all incidents and changes in central repositories.	Important	O	Receipt of evidence of: (a) implementation of a configuration management system; (b) establishment of procedures for configuration management, security incident response and change management; and (c) capture of all incidents and changes in central repositories.	31 December 2024
13	UNFCCC should: (a) document a detailed breakdown of the cost of the new project replacing the Digital Platform for Climate Change Events; (b) approve the business case and project plan; and (c) document a procurement plan to implement the project.	Important	O	Receipt of evidence of: (a) detailed breakdown of the cost of the new project replacing DPCCE; (b) approved business case and project plan; and (c) the procurement plan to implement the project.	31 December 2025
14	UNFCCC should: (a) complete the comprehensive detailing of all remaining user stories for the Enhanced Transparency Framework Reporting Tools project taking into account their integration, flow (user journeys) and dependencies; (b) establish a realistic time and cost schedule for delivery of the remaining user stories; and (c) strengthen project management by defining and monitoring key performance indicators.	Important	O	Receipt of evidence of: (a) completeness of the remaining user stories; (b) establishment of a realistic time and cost schedule for delivery of the remaining user stories; and (c) strengthening of project management through KPIs.	31 December 2025

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of information and communications technology governance, operations, security and project implementation 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: (a) establish an ICT strategy aligned with its business objectives; (b) approve strategic and tactical plans to ensure effective implementation of the ICT strategy; and (c) establish priorities to implement an enterprise architecture thereby reducing fragmentation of systems and eliminating silos.	Important	Yes	Manager, ICT subdivision	December 2025	The UNFCCC accepts this recommendation. The UNFCCC is in the process of establishing a new ICT strategy. Subject to the endorsement of the strategy, the ICT subdivision will take appropriate measures for its implementation. Within its processes, ICT will continue to seek out opportunities for efficiency in services and modes of operations. Relevant actions will be completed by the end of 2025.
2	UNFCCC should establish an ICT Governance Committee and ICT Technical Committee, and document their detailed terms of reference.	Important	Yes	Manager, ICT subdivision	December 2025	The UNFCCC accepts this recommendation. ICT is represented at the Management Committee by ICT Manager and Director AS/HR/ICT for governance. ICT Technical Committee and terms of reference will be developed and established in 2024. Other relevant actions for this recommendation will be completed by the end of 2025.
3	UNFCCC should: (a) consider the two previous external studies on the size and	Important	Yes	Director AS/HR/ICT	December 2025	The UNFCCC accepts this recommendation. The review and

[1] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

[2] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

APPENDIX I

Management Response

Audit of information and communications technology governance, operations, security and project implementation 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
	placement of its ICT function and establish an effective ICT service delivery model; (b) assess the risks and costs of excessive dependency on external parties for project management, business analysis, testing, quality assessment and ICT security; and (c) identify its short and long term ICT staffing requirements to effectively address current bottlenecks in responding to business needs.					decisions on ICT staffing approach, costs and management of business needs are part of the collective responsibilities of management that has direct or indirect oversight of ICT. Eventual actions based on management approval and budgetary availability on this recommendation will be implemented during the biennium 2024-2025.
4	UNFCCC should establish an ICT risk assessment process integrating ICT risks into its Enterprise Risk Management covering its entire ICT landscape (including ICT services, systems, projects, cybersecurity and data privacy) with appropriate risk response plans.	Important	Yes	Manager, ODO	December 2024	The UNFCCC accepts the recommendation. The ICT subdivision will participate in the establishment of an enterprise risk management program, as part of an overall UNFCCC Enterprise Risk Management led by the Organizational Development and Oversight Unit. Required activities will be implemented during the biennium 2024-2025.
5	UNFCCC should: (a) establish a data governance and management framework with procedures, roles and responsibilities; and (b) implement data privacy procedures including protection of sensitive personal information stored in its ICT systems.	Important	Yes	Manager, ODO	December 2024	The UNFCCC accepts this recommendation. The Organizational Deveopment and Oversight Unit (ODO) will coordinate the implementation in close consultation with the Operations Coordination Department. The relevant activities for this recommendation will be completed by the end of 2024.

APPENDIX I

Management Response

Audit of information and communications technology governance, operations, security and project implementation 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
6	UNFCCC should: (a) implement a roadmap to modernize its aging infrastructure running out of vendor support and applications using obsolete authentication systems; (b) document business continuity plans with expected recovery time and recovery point objectives; and (c) document and test the disaster recovery plans for all its applications.	Important	Yes	Manager, ICT subdivision	December 2025	The UNFCCC accepts this recommendation. ICT will continue its activities to modernize outdated infrastructures and decommission legacy applications in support of the proposed ICT strategy and roadmap. The relevant activities for this recommendation will be completed by the end of 2025.
7	UNFCCC should: (a) establish an ICT security roadmap that is approved by management, with appropriate resources assigned; and (b) document procedures for periodic vulnerability assessment and patch management.	Important	Yes	Manager, ICT subdivision	December 2024	The UNFCCC accepts this recommendation. The establishment of an ICT security roadmap will require dedicated resources, and management approval. Pending these decisions, ICT will develop an ICT security roadmap. The relevant activities for this recommendation will be completed by the end of 2024.
8	[redacted]	Important	Yes	Manager, ICT subdivision	December 2025	[redacted]

APPENDIX I

Management Response

Audit of information and communications technology governance, operations, security and project implementation 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
						[redacted]
9	[redacted]	Important	Yes	Manager, ICT subdivision	December 2024	[redacted]
10	UNFCCC should: (a) update its ICT service catalog with all services provided, including professional services; and (b) determine service rates using a transparent methodology.	Important	Yes	Manager, ICT subdivision	December 2024	The UNFCCC accepts the recommendation. The ICT subdivision will update its Service Catalog, include service rates, and publish them accordingly. The update will be completed in 2024.
11	UNFCCC should: (a) establish a service monitoring process; (b) conduct periodic client satisfaction surveys; and (c) take action to close the gap between expected service levels and ICT capacity.	Important	Yes	Manager, ICT subdivision	December 2025	The UNFCCC accepts this recommendation. ICT will continue to implement Service Now and related modules for improved service. As part of the improvements to service delivery, ICT will determine ways to improve satisfaction through surveys and other mechanisms as part of ongoing processes throughout 2024-2025.
12	UNFCCC should: (a) fully implement the configuration management system; (b) establish procedures for configuration management, security incident response and change management; and (c) capture	Important	Yes	Manager, ICT subdivision	December 2024	The UNFCCC accepts this recommendation. The ICT subdivision will complete the deployment of approved ServiceNow tools and modules. The relevant procedures for configuration

APPENDIX I

Management Response

Audit of information and communications technology governance, operations, security and project implementation 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
	all incidents and changes in central repositories.					management, security incident response, change management will be revised in newly developed SOP's. Relevant actions will be completed by the end of 2024.
13	UNFCCC should: (a) document a detailed breakdown of the cost of the new project replacing the Digital Platform for Climate Change Events; (b) approve the business case and project plan; and (c) document a procurement plan to implement the project.	Important	Yes	Director, Conference Affairs Division	December 2025	The UNFCCC accepts this recommendation. Past progress – scope expanded to include the revamp of conferencing systems and not just the digital platform. In addition, in 2022, a review of market software was undertaken to determine that the leading software would only be viable with customization and/or changes in the business process. The UNFCCC, with Conference Affairs as the Business Owner of the project will determine the necessary actions related to this organizational initiative by the end of 2025.
14	UNFCCC should: (a) complete the comprehensive detailing of all remaining user stories for the Enhanced Transparency Framework Reporting Tools project taking into account their integration, flow (user journeys) and dependencies; (b) establish a realistic time and cost schedule for delivery of the remaining user stories; and (c) strengthen project management by defining	Important	Yes	Director, Transparency Division	December 2025	The UNFCCC accepts this recommendation. In conjunction with ETF Project Board recommendations, ICT will incorporate relevant actions for project delivery improvements. Activities will be completed by September 2025.

APPENDIX I

Management Response

Audit of information and communications technology governance, operations, security and project implementation 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
	and monitoring key performance indicators.					