Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2018/064

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

Control enhancements and improvements were required for the governance, operations and security of information and communications technology

21 June 2018
Assignment No. AT2017/241/01

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

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of governance, operations and security of information and communications technology (ICT) at the United Nations Framework Convention on Climate Change (UNFCCC). The objective of the audit was to assess the adequacy and effectiveness of internal controls over governance, operations and security of ICT at UNFCCC. The audit covered the period from January 2015 to December 2017 and included a review of risk areas relating to: risk management and strategic planning; performance monitoring indicators and mechanisms; and management of ICT support systems.

The audit showed that control enhancements and improvements were required in the areas of governance, operations and security of ICT at UNFCCC.

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

- Define the roles and responsibilities for information management, including data classification and records management.
- Ensure that its ICT risk management framework is aligned with its enterprise risk management framework, and consider environmental threats as part of its risk management process.
- Review and institute a sustainable funding model for ICT in alignment with the policy instructions of the Controller.
- Implement control mechanisms to ensure that the Information and Communications Technology Services does not commit the Organization to financial liabilities without adequate funding and approval.
- Develop a service management framework with documented criteria, standards and performance indicators for ICT service delivery; review its service catalogue and rate cards to ensure that they provide a complete description of services and costs; and enable the automated user satisfaction survey functionality of the service desk system to facilitate periodic user surveys.
- Implement procedures for systematic monitoring of its entire ICT infrastructure and define a baseline with metrics to manage the risk of service disruptions and/or performance degradation.
- Migrate all data related to ICT serialized assets and update Umoja with data relating to recently acquired ICT assets; accelerate the transition to network printers; and speed up the disposal of written-off ICT assets.
- Document procedures for configuration management; update the configuration management database with all relevant configuration items including their attributes and inter-dependencies; and establish a mechanism to monitor changes against the defined repository and baseline.
- Enhance its information security policies and procedures by: (i) deploying resources to effectively manage the information security risk assessment programme; and (ii) ensuring that roles and responsibilities for all ICT security-related tasks are appropriately assigned.
- Define appropriate baseline measures and response systems; plan and conduct periodic vulnerability assessments of risks and threats to its ICT infrastructure; deploy appropriate tools for periodic review of critical applications and systems; 'harden' all critical hardware and software; and assess and patch or isolate obsolete software from its network.

- Document and execute a plan for timely implementation of all critical recommendations made by the third-party consulting firm relating to the vulnerability test **(Critical)**.
- Develop and deliver periodic training to promote information security awareness among its user community.
- Develop and implement a comprehensive user account management policy which: (i) ensures that incompatible roles are not assigned; (ii) defines the criteria for granting and controlling user, remote and privileged access; and (iii) implements password management procedures including periodic review of inactive user and administrator access particularly for critical systems.
- Conduct a business impact assessment of its activities and document a business continuity plan to inform the ICT continuity plan; and conduct periodic tests of the ICT continuity plan.
- Strengthen the physical controls at its ICT installations by: (i) coordinating with campus security to conduct a risk assessment to define its physical security requirements; (ii) installing additional close-circuit television cameras as necessary; and (iii) maintaining a log of access to the data rooms.

UNFCCC accepted the recommendations but was yet to initiate action to implement them.

CONTENTS

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

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of governance, operations and security of information and communications technology (ICT) 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 which advise the COP/CMP, and the COP/CMP Bureau which deals mainly with procedural and organizational issues arising from the COP/CMP.

3. The Information and Communications Technology Services (ICTS) programme of UNFCCC is the central service provider for ICT infrastructure and user support services, as well as for information systems development, maintenance and application support within UNFCCC. By 2016, UNFCCC had transitioned from a decentralized ICT service delivery model to a centralized model.

4. ICTS was structured into three operations: Management and Coordination; Information Systems Delivery; and Information Technology Service Management and Monitoring. The programme employed approximately 60 staff members. These resources were augmented with consultants and contractors, as needed. As of December 2016, ICTS supported 427 users and had service level agreements (SLAs) to provide ICT services to three United Nations agencies and funds co-located in the Bonn complex.

5. The core operations of UNFCCC were funded from contributions of the Parties. ICTS was funded from the core budget and seven other funding sources. The total ICT funding for the 2016-2017 biennium was Euro 21.8 million as shown in Table 1.

Table 1: UNFCCC ICT budget for the 2016-2017 biennium by funding source

Funding Source	Euro	Percentage
Core budget	5,433,013	24.91
International Transaction Log Trust Fund	4,740,716	21.74
Project support Costs (Overhead funds)	322,000	1.48
Framework Programme Agreements	4,295,965	19.70
Per Capita Costs	4,533,628	20.79
Contribution from Governments	378,352	1.73
Bonn Fund	322,000	1.48
Other Supplementary funded projects	1,783,407	8.18
Total	**21,809,081**	**100**

6. Comments provided by UNFCCC are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

7. The objective of the audit was to assess the adequacy and effectiveness of internal controls over governance, operations and security of ICT at UNFCCC.

8. This audit was included in the 2017 risk-based work plan of OIOS due to the risks associated with the provision of ICT services at UNFCCC which could potentially affect the achievement of the Convention's objectives.

9. OIOS conducted the audit from December 2017 to January 2018. The audit covered the period from January 2015 to December 2017. Based on an activity-level risk assessment, the audit covered risk areas in ICT which included: risk management and strategic planning; project management capacity; performance monitoring; and management of ICT support systems.

10. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data; (d) tests of transactions and systems; (e) physical verification of data rooms and ICT assets; and (f) survey of the ICT user community.

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

III. AUDIT RESULTS

A. Risk management and strategic planning

<u>The ICT governance framework needed to be strengthened</u>

12. The professional standards "Control Objectives for Information and Related Technology" (COBIT) recommend that the organization should create a strategic plan that defines, in cooperation with relevant stakeholders, how ICT goals will contribute to the organization's strategic objectives and how ICT will support ICT-enabled programmes, ICT services and ICT assets. The ICT strategy should be complemented by a governance framework that defines the distribution of the decision-making rights and responsibilities among different offices in the organization, procedures to obtain formal sign-off from stakeholders, and procedures and mechanisms for implementing and monitoring strategic decisions.

13. UNFCCC's ICT environment was governed by a framework based on an ICT strategy, standard operating procedures, and the Management Sub-committee for ICT with the primary role of providing oversight, analysis, advice and recommendations on strategic ICT issues.

14. The overall ICT strategic direction and main goals driving the ICTS programme had been defined and endorsed by the Management Sub-committee for ICT. However, the ICT governance framework did not adequately reflect the strategic alignment with programme objectives, value delivery, resource management and performance measures. In this regard, the following gaps were observed:

(a) The ICT decision model for UNFCCC was based on a RACI model[1] annexed to the terms of reference of the Management Sub-committee for ICT. This document assigned roles and responsibilities for ICT decisions, including the roles and responsibilities of the Management Sub-committee for ICT, operational programmes and ICTS. However, the Convention's operational programmes expressed concern that the centralized nature of ICT service delivery limited their strategic priorities and operational requirements from being adequately represented and considered. Programmes felt that ICTS imposed solutions on them and they were restricted from conducting their own cost-benefit analysis on the various

[1] RACI is a matrix used to define the roles and responsibilities of tasks within a defined process. R- Responsible, A-Accountable, C-Consulted, I- Informed

options available, as this role was performed by ICTS. *UNFCCC stated that the ICT strategy, the ICT strategic priorities and the ICT service catalogue were all reviewed and aligned with programmes through the Management Sub-committee for ICT. Client/operational programmes have visibility and can influence ICT strategic decisions through the management sub-committee for ICT and through the framework programme agreements.*

(b) The roles and responsibilities for information management were yet to be determined. This included responsibility for data classification and records management. UNFCCC needs to address this matter to ensure that sensitive data is handled appropriately.

(1) UNFCCC should define the roles and responsibilities for information management, including data classification and records management.

UNFCCC accepted recommendation 1 and stated that it will discuss with relevant stakeholders including Administrative Services, Knowledge Management and ICTS for deciding on data classification and record management and will document the decisions accordingly. Recommendation 1 remains open pending receipt of evidence that the roles and responsibilities for information management, including data classification and records management, have been defined.

The ICT risk management process needed to be aligned to UNFCCC's risk management framework

15. The ICT risk and control framework should be aligned with the Organization's enterprise risk management (ERM) framework and should consider the Organization's risk tolerance. It should also ensure timely identification and assessment of risks, and implementation of mitigating controls.

16. UNFCCC had established an ERM framework modeled on the ERM framework of the United Nations Secretariat. ICTS had also documented an ICT risk management framework. However, the ICTS risk register was not aligned to UNFCCC's ERM framework. For instance, the ERM framework had a risk definition stating that "ICT strategies, including system development and infrastructure within different programmes, were not aligned with the overall strategic and operational objectives of the Organization, nor appropriately coordinated". But there was no corresponding entry and risk response plan in the ICT risk register. The two documents did not use similar risk classification principles. Additionally, neither the UNFCCC ERM nor the ICT risk register considered the risk of flooding, given that the Convention's facilities are located on the banks of the River Rhine. The lack of a robust ICT risk assessment framework may lead to inadequate risk response and potentially affect the achievement of UNFCCC's objectives.

(2) UNFCCC should: (i) ensure that its ICT risk management framework is aligned with its ERM framework; and (ii) consider environmental threats as part of its risk management process.

UNFCCC accepted recommendation 2 and stated that it will review existing ERM and align the ICT framework to it. ICTS will identify and assess environmental threats and include them as part of its risk management process. Recommendation 2 remains open pending receipt of evidence that the ERM and ICT risk management frameworks have been aligned and environmental threats are considered as part of the risk management framework.

Need to reassess and redefine the ICT service funding and cost recovery model

17. COBIT recommends that organizations should identify all ICT costs and map them to ICT services to support a transparent cost model. ICT services should also be linked to business processes such that the business can identify the associated service billing levels.

18. In June 2012, the Controller issued a policy for service costs and cost recovery in the United Nations Secretariat. The basic principle underlying this policy was that "All United Nations administrative services must understand the cost of providing services. Where they charge for these services, they must calculate service costs and attribute these to specific and clearly defined service activities irrespective of the sources of funding from which these services or activities are financed. They must also of course be directly attributable to users. Accurately establishing the costs of producing something is a useful exercise in managing and controlling those costs and identifying inefficiencies, which in turn can lead to improved use of scarce resources. The services to which service costs charges apply must be transparent and clearly defined. Once defined, the full cost of each type or category of service should be measured realistically and objectively".

19. In the 2014-2015 biennium, UNFCCC contracted an external consulting firm to recommend a sustainable funding model that ensures a higher degree of transparency in ICT-related spending and a more rigorous matching of funding sources with the nature of ICT services provided. UNFCCC used the recommendations of the consulting firm as a baseline for the funding and cost recovery model for its ICT services. The proposed model was endorsed by the Management Sub-committee for ICT in October 2015. OIOS noted the following gaps in this regard:

(a) Relevance of the benchmarking exercise to the United Nations operational context: The service delivery and funding model proposed by the external consulting firm was mainly based on a benchmarking with what the firm called "comparable peers". Except for the reference to a 2014 survey done by a consulting firm comparing the UNFCCC Secretariat with government entities with a budget allocation of less than $250 million, the firm did not define as to who the "comparable peers" were, and whether they included any United Nations agencies. As such, the exercise did not adequately take into consideration the United Nations environment to serve as a reliable basis for the funding model.

(b) Alignment of the model with the United Nations Secretariat rules and regulations: The model proposed the allocation of cost categories by type of services and cost recovery means (i.e., direct, variable, indirect and fixed indirect). However, the cost of services was not clearly attributable to specific and clearly defined service activities. Therefore, there was no assurance that the recommended funding model suited the financial and operational requirements of the United Nations Secretariat in accordance with the policy and instructions issued by the Controller.

(c) Concerns of stakeholders in embracing the model: Before implementing the model, UNFCCC did not get the advice of its Finance Section and substantive programmes to confirm its adequacy, appropriateness, and potential impact on their budgets. Also, the Management Sub-Committee for Finance expressed concern with regard to cash flow implications of the model and recommended that the Management Sub-committee for ICT review the business processes of the funding model after the first year of implementation. In addition, the Convention's substantive programmes did not buy into this model and expressed concern that: (i) the methodology used for costing was not transparent enough and clearly defined; (ii) there was no alignment between the services provided and their cost; and (iii) the services provided were expensive and not competitive.

(d) Sustainability of the model: The resources providing basic, long term services – i.e., total cost of ownership (TCO) per capita rates – were funded through short term means. This resulted in a shortfall of cash to meet commitments and constrained ICTS to enter into unauthorized financial commitments (without recording the obligation in Umoja) due to lack of funds or delayed funding. Consequently, at the end of 2016, ICT invoices amounting to $550,000 remained unpaid to a contractor and there were unauthorized financial commitments pending in the amount of $240,287 for 2017.

(e) High overhead-related activities: The Framework Programme Agreements (FPAs) between ICTS and other programmes of UNFCCC require the charging of costs to the respective services/projects. OIOS review of the hours charged to projects by four staff members selected randomly indicated that a large component of costs charged were overhead-related activities ('indirect' hours). In some instances, 'indirect' hours and 'other' hours were charged to projects which included non-project activities such as attending general meetings and non-project administrative tasks, as shown in Table 2. The Secretariat explained that a task force was scheduled to review the costs of overhead-related activities in 2018.

Table 2: Time charged by staff to overhead-related activities

Staff	Direct hours	Indirect hours	Others	Total hours
A	294.25	18.25	215.50	528.00
B	374.00	87.00	51.00	512.00
C	13.50	151.00	360.50	525.00
D	9.00	295.00	208.00	512.00
Total	**690.75**	**551.25**	**835.00**	**2,077.00**
Percentage	**33**	**27**	**40**	**100**

(f) Unclear directives: The Secretariat's Finance Section had prepared a draft term of reference in 2006 describing the various types of costs to be covered by the TCO but this was not formalized or updated. The document defined TCO services to include: (a) ICT services; (b) hardware, software and computer support required for staff and consultants; and (c) system support to operate specialized information systems on the network and related external internet connectivity. However, there were inconsistencies in the application and use of the TCO funding source by ICTS: the staffing costs associated with non-ICT support posts such as lead requirements engineer, project manager and quality assurance officer were also charged to TCO. An inadequate funding/cost recovery model that does not meet the policy requirements stipulated by the Controller poses significant risks to the effective management of ICT resources.

(3) UNFCCC should review and institute a sustainable funding model for ICT in alignment with the policy instructions of the Controller.

UNFCCC accepted recommendation 3 and stated that it will review and define a sustainable funding model for ICT according to United Nation regulations. Recommendation 3 remains open pending receipt of evidence that a sustainable funding model for ICT has been implemented.

(4) UNFCCC should implement control mechanisms to ensure that ICTS does not commit the Organization to financial liabilities without adequate funding and approval.

UNFCCC accepted recommendation 4 and stated that implementation is subject to having a sustainable funding model. UNFCCC will implement control mechanisms to ensure that ICTS does not commit the Organization to financial liabilities without adequate funding and approval. Recommendation 4 remains open pending receipt of evidence that control mechanisms have been implemented to prevent incurring financial liabilities without adequate funding/approval.

B. Performance monitoring

Need to standardize and enhance ICT service management and service delivery procedures

20. The Information Technology Infrastructure Library (ITIL) recommends that ICT service management procedures should enhance operational effectiveness by defining, monitoring and measuring ICT services. ITIL also recommends the development of ICT service catalogues documenting standard

services and deliverables, and SLAs defining expectations and metrics for measuring performance indicators to ensure that service/operational level agreements and underpinning contracts are appropriate for the agreed level of service contracts.

21. SLAs should be based on clear terms of reference defining the level of service expected by client organizations from their service provider (i.e., ICTS in the present case). These terms should include standard definitions and conditions for: (i) creating service requirements, delivery agreements and guides; (ii) monitoring, assessing and aligning clients' requirements and services provided; and (iii) complementing the standard service catalogue with details about the organizational structure designed by the service provider (i.e., ICTS).

22. ICTS provided services to internal UNFCCC clients and three United Nations entities co-located in the Bonn complex. ICTS had documented an ICT service catalogue, an ICT rate card, FPAs, proforma invoices, and SLAs. However, none of these documents were based on a clear framework for service management and an organized process for creating service requirements, service definitions, and quantitative and qualitative service metrics expected by client organizations from ICTS.

23. OIOS' comparison of the ICT service catalogue for 2017-18 vis-à-vis the signed FPA for 2017 and SLAs with external clients showed that ICTS offered and billed baseline services which were not quoted or categorized in the ICT service catalogue. There were also discrepancies between prices published in the ICT service catalogue and rates charged to clients. For instance, the ICT service catalogue quoted a rate of Euro 500 for local area network access (switches, cabling), whereas the SLA with a United Nations entity quoted Euro 6,000 for the same service.

24. In addition, the documents did not define and clarify how costs would be assigned and charged. For example, the layout and information communicated through the FPA did not provide clients with the detailed breakdown of services to be provided, the associated cost structure and the methodology for arriving at costs.

25. To monitor the quality of services it provided, ICTS had established a system of maintaining a log of service requests received, and defined some key performance indicators (KPIs) for services it provided to users. However, performance metrics and monitoring mechanisms were not consistently defined and applied. For example, the metrics provided in 2016-2017 budget document differed from the KPI metrics provided to OIOS. In some cases, there were no metrics for certain services. There was no indication that ICTS provided regular performance monitoring reports on its KPIs to its client community.

26. OIOS reviewed the adequacy of controls over monitoring of ICT services through interviews with various users, both internal and external, and the results of a survey of the ICT user community in Bonn. OIOS received responses from 143 users out of a total of 423 users surveyed (a response rate of 34 per cent). The interviews and survey results indicated the following:

(a) KPIs were not specific and consistent. For example, the KPI for providing the ICT service desk was defined as "95 per cent of all calls are responded to within five hours" whereas the ICT work programme for 2015-2016 for this parameter defined it as "the proportion of information technology service requests responded to and completed within 90 days".

(b) ICTS did not meet the KPI of responding to all calls within the stipulated five hours during the period under review. For example, the service desk log indicated that only 20,880 requests (32 per cent) out of a total of 65,535 requests were addressed between one to 530 days.

(c) The survey's responses to the question "How do you rate the quality of help desk services?" were as follows: Good - 39.4 per cent; Very Good - 14.5 per cent; and Fair to Very Poor - 46.1 per cent. This was much below UNFCCC's standard of 70 per cent positive feedback.

(d) Although reported to have been planned, ICTS did not undertake an assessment of the quality of services provided during the period under review. Therefore, it missed the opportunity to learn lessons, if any, to improve the quality of services provided.

(e) ICTS did not conduct periodic user satisfaction surveys of its service management processes and did not activate the automated user satisfaction survey functionality in its service desk system.

27. The Umoja system has a module for managing service delivery and cost recovery. ICTS did not use this functionality but instead used a system outside Umoja (a time management system for logging efforts and recovery). There was no interface between Umoja and the time management system which required extensive manual effort to reconcile the financials with Umoja.

28. Inadequately defined ICT service catalogues and the absence of metrics, baselines and periodic surveys may prevent ICTS from effectively monitoring its service performance and meeting user expectations.

(5) UNFCCC should: (i) develop a service management framework with documented criteria, standards and performance indicators for ICT service delivery; (ii) review its service catalogue and rate cards to ensure that they provide a complete description of services and costs; and (iii) enable the automated user satisfaction survey functionality of the service desk system to facilitate periodic user surveys.

UNFCCC accepted recommendation 5 stating that upon completion of its data centre migration project, it will develop a complete service management framework, review its service catalogue and rate card, and enable automated user satisfaction surveys as a way of facilitating periodic user surveys. Recommendation 5 remains open pending receipt of evidence that: (i) a service management framework has been developed; (ii) service catalogue and rate cards reflect a complete description of services and costs; and (iii) the automated user satisfaction survey has been enabled and used to monitor service performance.

Need to strengthen monitoring of the ICT infrastructure

29. The use of ICT resources and assets should be monitored, and projections of future capacity requirements should be made to ensure the required system performance.

30. ICTS had tools for performance and capacity monitoring of its infrastructure and operations. However, it did not establish a procedure for systematic performance monitoring of its entire infrastructure including continuous review of service capacity and performance, assessment of data regarding capacity, and resolution of identified events/issues.

31. Inconsistent performance monitoring and assessment of ICT infrastructure may result in unidentified and unattended events/issues which could potentially cause service disruptions and/or performance degradation.

(6) UNFCCC should implement procedures for systematic monitoring of its entire ICT infrastructure and define a baseline with metrics to manage the risk of service disruptions and/or performance degradation.

UNFCCC accepted recommendation 6 and stated that upon completion of its data centre migration project, it will develop a procedure for systematic monitoring of its entire ICT infrastructure, and define a baseline with metrics to monitor performance of services. Recommendation 6 remains open pending receipt of evidence of implementation of procedures for systematic monitoring of ICT infrastructure and a baseline with metrics to manage the risk of service disruptions and/or performance degradation.

C. Management of ICT support systems

ICT asset management procedures needed to be strengthened

32. The international ICT security management standard (ISO/IEC 27001) recommends the creation of an inventory of assets associated with information processing systems. Assets and their inventory should be maintained to reduce their exposure to environmental threats, hazards, and unauthorized access.

33. ICTS had an aging infrastructure and planned to outsource a large part of its infrastructure to a third-party provider. However, ICTS still retained the management of end user assets and a smaller sized data centre within the premises. OIOS noted the following with regard to management of ICT assets:

(a) Data related to serialized equipment was not migrated to Umoja. Also, the data for recently procured ICT assets had not been enriched in Umoja. ICTS stated that it would discuss with the Finance Section on how to proceed with updating Umoja with the required information.

(b) Printer rationalization is a United Nations project which improves the security of information and reduces the cost of supporting and maintaining dedicated printers. Although ICTS had a campaign to remove dedicated printers, it had only managed to obtain agreement to remove 15 out of 47 dedicated printers in use.

(c) ICTS had a process for disposing of ICT assets with recorded data (hard drives and other removable media). However, OIOS observed that 656 ICT assets were locked in a disposal room since April 2017 waiting for disposal.

(7) UNFCCC should: (i) migrate all data related to ICT serialized assets and update Umoja with data relating to recently acquired ICT assets; (ii) accelerate the transition to network printers; and (iii) speed up the disposal of written-off ICT assets.

UNFCCC accepted recommendation 7 and stated that it will complete the migration of all required assets into Umoja, complete the transition to network printers and improve its assets disposal process with a view to speed up the disposal of written-off assets. Recommendation 7 remains open pending receipt of evidence that: (i) all data related to ICT assets has been migrated to and/or updated in Umoja; and (ii) the transition to network printers has been completed; and (iii) written-off ICT assets stored in the warehouse have been disposed of.

Need to define and enhance configuration management procedures

34. COBIT recommends the establishment of a supporting tool and a central repository to contain all relevant information on configuration items, monitor and record all assets and changes to assets, and maintain a baseline of configuration items for every system to serve as a checkpoint to which to return after changes.

35. ICTS had deployed an integrated ICT service and asset management software which had a Configuration Management Database module (CMDB). The CMDB module should be used to track assets and their configuration information such as model, assignee, vendor and financial information. However, ICTS did not document configuration management procedures that defined the baselines for configuration information and mechanisms to monitor changes against the defined baselines. This gap caused the following:

(a) The CMDB database was not complete with a record of all configuration items (hardware, software and other components) across all service areas. The database only included hardware. Therefore, reliance could not be placed on the system for the identification of all configuration assets.

(b) Not all attributes of configuration information such as location, warranty expiration, versions, vendor, serial numbers and financial information were captured, including the Internet Protocol addresses of network hosts, network devices and a complete network diagram for UNFCCC. Therefore, there was insufficient baseline configuration information captured for reverting to baseline configuration when required.

(c) Inter-dependencies between attributes of configuration information were not captured. There was inadequate visibility of processes and relationships between parts, subsystems and systems for effective control of the entire ICT infrastructure. For instance, there was no visibility of security vulnerabilities across the virtual and physical ICT infrastructure.

36. Inadequacies in configuration management procedures could lead to security breaches and provision of outdated information on the Convention's ICT infrastructure.

(8) UNFCCC should: (i) document procedures for configuration management; (ii) update the configuration management database with all relevant configuration items including their attributes and inter-dependencies; and (iii) establish a mechanism to monitor changes against the defined repository and baseline.

UNFCCC accepted recommendation 8 and stated that it will prepare a configuration management procedure, update the configuration management database, and establish a mechanism to monitor changes against the defined repository and baseline. Recommendation 8 remains open pending receipt of: (i) documentation on configuration management procedures; (ii) evidence that the configuration management database has been updated; and (iii) evidence that a monitoring mechanism has been established.

Need to strengthen procedures for assessing and monitoring the general security of ICT operations

37. Organizations should define information security policies and procedures and assign specific responsibilities for their operations, monitoring, and compliance.

38. ICTS implemented several initiatives to address the ICT security risks, including: (i) appointment of a dedicated information security officer with defined role and responsibilities for risk management and information security; (ii) documentation of an electronic security governance programme; (iii) a RACI matrix which was used to assign roles and responsibilities for ICT security related policies and procedures; and (d) contracting a third party to conduct a penetration test of its infrastructure.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(9) UNFCCC should enhance its information security policies and procedures by: (i) deploying resources to effectively manage the information security risk assessment programme; and (ii) ensuring that roles and responsibilities for all ICT security-related tasks are appropriately assigned.

UNFCCC accepted recommendation 9 and stated that it will review and improve its information security policies and procedures accordingly. Recommendation 9 remains open pending receipt of enhanced information security policies and evidence that roles and responsibilities for ICT security-related tasks have been appropriately assigned.

(10) UNFCCC should: (i) define appropriate baseline measures and response systems; (ii) plan and conduct periodic vulnerability assessments of risks and threats to its ICT infrastructure; (iii) deploy appropriate tools for periodic review of critical applications and systems; (iv) 'harden' all critical hardware and software; and (v) assess and patch or isolate obsolete software from its network.

UNFCCC accepted recommendation 10 and stated that it will define baseline measures and response systems, plan and conduct periodic vulnerability assessments of risks and threats to its ICT infrastructure, deploy appropriate tools for periodic review of critical applications and systems, 'harden' all critical hardware and software; and assess and patch or isolate obsolete software from its network. Recommendation 10 remains open pending receipt of evidence demonstrating implementation.

(11) UNFCCC should document and execute a plan for timely implementation of all critical recommendations made by the third-party consulting firm relating to the vulnerability test.

UNFCCC accepted recommendation 11 and stated that it will have the plan fully prepared by mid-2019 and will start executing it immediately after. The execution of the plan will be completed by end of 2020. Recommendation 11 remains open pending receipt of evidence that a plan has been documented and executed to implement all critical recommendations made by the third-party consulting firm.

Need for training in ICT security awareness

42. Organizations should develop and deliver a security awareness programme to educate all employees on: (i) the impact on the organization and its employees if security requirements are not met; (ii) ethical use of ICT resources and facilities; (iii) how security incidents should be handled and escalated; and (iv) employees' responsibilities for information security.

43. UNFCCC had not developed training to educate its user community on the threats and risks relating to information security. Also, there was no evidence of ongoing efforts to promote information security awareness among the ICT user community. Inadequate ICT security awareness among the user community may have an adverse impact on information security and potentially cause security breaches.

(12) UNFCCC should develop and deliver periodic training to promote information security awareness among its user community.

UNFCCC accepted recommendation 12 and stated that it will deliver periodic training about information security awareness among its user community. Recommendation 12 remains open pending the development and delivery of ICT security awareness training in UNFCCC.

Need to strengthen user access management

44. User access to all systems and applications should be regulated by policies and procedures to control and manage system and application rights and privileges according to the organization's security policies, and for the periodic assessment of system and application access.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(13) UNFCCC should develop and implement a comprehensive user account management policy which: (i) ensures that incompatible roles are not assigned; (ii) defines the criteria for granting and controlling user, remote and privileged access; and (iii) implements password management procedures including periodic review of inactive user and administrator access particularly for critical systems.

UNFCCC accepted recommendation 13 and stated that it will develop and implement a comprehensive user account management policy accordingly. Recommendation 13 remains open pending receipt of evidence that a comprehensive user account management policy has been implemented.

Need for a comprehensive business continuity and disaster recovery plan

47. A business continuity plan defines how an organization will continue operating in response to adverse events. The plan should include instructions defining the actions required by all parties responsible for ensuring the continuation of operations under adverse conditions. The ICT disaster recovery plan should be developed in conjunction with the business continuity plan (BCP) and provide recovery strategies to meet the objectives of the BCP.

48. While ICTS had developed an ICT continuity plan, it was not aligned to a BCP. UNFCCC had not conducted a business impact assessment to identify the risks and impact of various disaster scenarios on business processes and critical ICT systems, and thereby inform a BCP. Also, ICTS had not tested its ICT continuity plan and there was no off-site fail-over for the data centres maintained within the premises. The absence of adequate business continuity and disaster recovery arrangements could lead to failure in timely recovery of ICT systems/applications and unavailability of communication systems.

(14) UNFCCC should: (i) conduct a business impact assessment of its activities and document a business continuity plan to inform the ICT continuity plan; and (ii) conduct periodic tests of the ICT continuity plan.

UNFCCC accepted recommendation 14 and stated that upon completion of the secretariat-wide structure review and the development of a strategic plan, it will conduct a high-level business impact *assessment of its activities and document a high-level business continuity plan to inform the ICT continuity plan. UNFCCC will conduct periodic tests of the ICT continuity plan, afterwards.* Recommendation 14 remains open pending receipt of evidence that a business impact assessment has been documented to inform the ICT continuity plan, and the ICT continuity plan has been tested.

<u>Need to strengthen physical security of ICT resources and assets</u>

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

50. The physical security at UNFCCC was provided under a cost-sharing agreement administered by United Nations Volunteers. Discussions with campus security indicated that UNFCCC had not provided specific security requirements to protect its ICT assets.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

52. Inadequate physical and environmental controls exposed UNFCCC's ICT assets to a number of risks including loss of equipment, loss of information, and unauthorized access to information systems and resources.

(15) UNFCCC should strengthen the physical controls at its ICT installations by: (i) coordinating with campus security to conduct a risk assessment to define its physical security requirements; (ii) installing additional CCTV cameras as necessary; and (iii) maintaining a log of access to the data rooms.

UNFCCC accepted recommendation 15 and stated that it will strengthen the physical controls at its ICT installations. Recommendation 15 remains open pending receipt of evidence that the physical security controls at ICT installations have been strengthened.

IV. ACKNOWLEDGEMENT

53. 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*) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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 define the roles and responsibilities for information management, including data classification and records management.	Important	O	Receipt of evidence that the roles and responsibilities for information management, including data classification and records management have been defined.	31 December 2019
2	UNFCCC should: (i) ensure that its ICT risk management framework is aligned with its ERM framework; and (ii) consider environmental threats as part of its risk management process.	Important	O	Receipt of evidence the ERM and ICT risk management frameworks have been aligned and environmental threats are considered as part of the risk management framework.	30 June 2019
3	UNFCCC should review and institute a sustainable funding model for ICT in alignment with the policy instructions of the Controller.	Important	O	Receipt of evidence that a sustainable funding model for ICT has been implemented.	31 December 2020
4	UNFCCC should implement control mechanisms to ensure that ICTS does not commit the Organization to financial liabilities without adequate funding and approval.	Important	O	Receipt of evidence that control mechanisms have been implemented to prevent incurring financial liabilities without adequate funding and approval.	31 December 2019
5	UNFCCC should: (i) develop a service management framework with documented criteria, standards and performance indicators for ICT service delivery; (ii) review its service catalogue and rate cards to ensure that they provide a complete description of services and costs; and (iii) enable the automated user satisfaction survey functionality of the service desk system to facilitate periodic user surveys.	Important	O	Receipt of evidence that: (i) a service management framework has been developed; (ii) service catalogue and rate cards reflect a complete description of services and costs; and (iii) the automated user satisfaction survey has been enabled and used to monitor service performance.	31 December 2019
6	UNFCCC should implement procedures for systematic monitoring of its entire ICT infrastructure	Important	O	Receipt of evidence of implementation of procedures for systematic monitoring of ICT	31 December 2019

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

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

[4] C = closed, O = open

[5] Date provided by UNFCCC in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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]
	and define a baseline with metrics to manage the risk of service disruptions and/or performance degradation.			infrastructure and a baseline with metrics to manage the risk of service disruptions and/or performance degradation.	
7	UNFCCC should: (i) migrate all data related to ICT serialized assets and update Umoja with data relating to recently acquired ICT assets; (ii) accelerate the transition to network printers; and (iii) speed up the disposal of written-off ICT assets.	Important	O	Receipt of evidence that: (i) all data related to ICT assets has been migrated to and/or updated in Umoja; and (ii) the transition to network printers has been completed; and (iii) written-off ICT assets stored in the warehouse have been disposed of.	30 June 2019
8	UNFCCC should: (i) document procedures for configuration management; (ii) update the configuration management database with all relevant configuration items including their attributes and inter-dependencies; and (iii) establish a mechanism to monitor changes against the defined repository and baseline.	Important	O	Receipt of: (i) documentation on configuration management procedures; (ii) evidence that the configuration management database has been updated; and (iii) evidence that a monitoring mechanism has been established.	31 December 2018
9	UNFCCC should enhance its information security policies and procedures by: (i) deploying resources to effectively manage the information security risk assessment programme; and (ii) ensuring that roles and responsibilities for all ICT security-related tasks are appropriately assigned.	Important	O	Receipt of evidence demonstrating the implementation of enhanced information security policies and evidence that roles and responsibilities for ICT security-related tasks have been appropriately assigned.	30 June 2019
10	UNFCCC should: (i) define appropriate baseline measures and response systems; (ii) plan and conduct periodic vulnerability assessments of risks and threats to its ICT infrastructure; (iii) deploy appropriate tools for periodic review of critical applications and systems; (iv) 'harden' all critical hardware and software; and (v) assess and patch or isolate obsolete software from its network.	Important	O	Receipt of evidence that: (i) appropriate baseline measures and response systems have been defined; (ii) periodic vulnerability assessments have been scheduled and conducted; (iii) tools have been deployed for periodic review of critical applications and systems; (iv) all critical hardware and software have been 'hardened'; and (v) obsolete software has been patched and/or isolated from the network.	31 December 2019
11	UNFCCC should document and execute a plan for timely implementation of all critical	Critical	O	Receipt of evidence that a plan has been documented and executed to implement all	31 December 2020

STATUS OF AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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]
	recommendations made by the third-party consulting firm relating to the vulnerability test.			critical recommendations made by the third-party consulting firm.	
12	UNFCCC should develop and deliver periodic training to promote information security awareness among its user community.	Important	O	The development and delivery of ICT security awareness training in UNFCCC.	31 December 2019
13	UNFCCC should develop and implement a comprehensive user account management policy which: (i) ensures that incompatible roles are not assigned; (ii) defines the criteria for granting and controlling user, remote and privileged access; and (iii) implements password management procedures including periodic review of inactive user and administrator access particularly for critical systems.	Important	O	Receipt of evidence that a comprehensive user account management policy has been implemented.	31 December 2018
14	UNFCCC should: (i) conduct a business impact assessment of its activities and document a business continuity plan to inform the ICT continuity plan; and (ii) conduct periodic tests of the ICT continuity plan.	Important	O	Receipt of evidence that a business impact assessment has been documented to inform the ICT continuity plan, and the ICT continuity plan has been tested.	31 December 2020
15	UNFCCC should strengthen the physical controls at its ICT installations by: (i) coordinating with campus security to conduct a risk assessment to define its physical security requirements; (ii) installing additional CCTV cameras as necessary; and (iii) maintaining a log of access to the data rooms.	Important	O	Receipt of evidence that the physical security controls at ICT installations have been strengthened.	30 June 2019

APPENDIX I

Management Response

APPENDIX I

AUDIT RECOMMENDATIONS

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

The UNFCCC secretariat is currently undergoing a secretariat-wide structure review, development of a strategic plan, as well strengthening resource mobilization function. Furthermore, the UNFCCC secretariat is facing a critical funding situation for the operations in addition to the overall political environment in which it operates. In view of these critical factors, the audit recommendations will be implemented taking into consideration the availability of staffing, financial resources and other competing priorities.

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNFCCC should define the roles and responsibilities for information management, including data classification and records management.	Important	Yes	ICT Director	End of 2019	UNFCCC will discuss with relevant stakeholders including AS, KM and ICT for deciding on data classification and record management and will document the decisions accordingly. Implementation date is subject to availability of staff, funds, and competing priorities.
2	UNFCCC should: (i) ensure that its ICT risk management framework is aligned with its ERM framework; and (ii) consider environmental threats as part of its risk management process.	Important	Yes	Team Lead, ICT Project and Service Management Office	End of June 2019	UNFCCC will review existing ERM and align ICT framework to it. ICT will identify and assess environmental threats and include them as part of its risk management process. Implementation date is subject to availability of staff, funds, and competing priorities.
3	UNFCCC should review and institute a sustainable funding model for ICT in alignment with the policy instructions of the Controller.	Important	Yes	ICT Director	End of 2020	While UNFCCC accepts the recommendation, the note below "note on recommendation #3" provides the secretariat's understanding of paragraph 19, a), c), e), f).

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

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

APPENDIX I

AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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
						UNFCCC will review and define a sustainable funding model for ICT according to UN regulations. Implementation date is subject to availability of staff, funds, and competing priorities.
4	UNFCCC should implement control mechanisms to ensure that ICTS does not commit the Organization to financial liabilities without adequate funding and approval.	Important	Yes	ICT Director	End of 2019	UNFCCC accepts the recommendation however wants to highlight that it is subject to having a sustainable funding model. UNFCCC will implement control mechanisms to ensure that ICTS does not commit the Organization to financial liabilities without adequate funding and approval. Implementation date is subject to availability of staff, funds, and competing priorities.
5	UNFCCC should: (i) develop a service management framework with documented criteria, standards and performance indicators for ICT service delivery; (ii) review its service catalogue and rate cards to ensure that they provide a complete description of services and costs; and (iii) enable the automated user satisfaction survey functionality of the service desk system to facilitate periodic user surveys.	Important	Yes	ICT Director	End of 2019	Upon completion of its datacenter migration (DCCP project), UNFCCC will develop a complete service management framework, review its service catalogue and rate card, and enable automated user satisfaction surveys as a way of facilitating periodic user surveys. Implementation date is subject to availability of staff, funds, and competing priorities.
6	UNFCCC should implement procedures for systematic monitoring of its entire ICT infrastructure and define a baseline with metrics to manage the risk of service	Important	Yes	ICT Director	End of 2019	Upon completion of its datacenter migration (DCCP project), UNFCCC will develop a procedure for systematic monitoring of its entire ICT

APPENDIX I

AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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
	disruptions and/or performance degradation.					infrastructure, and define a baseline with metrics to monitor performance of services. Implementation date is subject to availability of staff, funds, and competing priorities.
7	UNFCCC should: (i) migrate all data related to ICT serialized assets and update Umoja with data relating to recently acquired ICT assets; (ii) accelerate the transition to network printers; and (iii) speed up the disposal of written-off ICT assets.	Important	Yes	ICT Director	End of June 2019	UNFCCC will complete the migration of all required assets into Umoja, complete the transition to network printers and improve its assets disposal process with a view to speed up the disposal of written-off assets. Implementation date is subject to availability of staff, funds, and competing priorities.
8	UNFCCC should: (i) document procedures for configuration management; (ii) update the configuration management database with all relevant configuration items including their attributes and inter-dependencies; and (iii) establish a mechanism to monitor changes against the defined repository and baseline.	Important	Yes	ICT Director	End of 2018	UNFCCC will prepare a configuration management procedure, update the configuration management database, and establish a mechanism to monitor changes against the defined repository and baseline. Implementation date is subject to availability of staff, funds, and competing priorities.
9	UNFCCC should enhance its information security policies and procedures by: (i) deploying resources to effectively manage the information security risk assessment programme; and (ii) ensuring that roles and responsibilities for all ICT security-related tasks are appropriately assigned.	Important	Yes	ICT Security Officer	June 2019	UNFCCC will review and improve its information security policies and procedures accordingly. Implementation date is subject to availability of staff, funds, and competing priorities.
10	UNFCCC should: (i) define appropriate baseline measures and response systems;	Important	Yes	ICT Security Officer	End of 2019	UNFCCC will define baseline measures and response systems, plan and conduct

AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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
	(ii) plan and conduct periodic vulnerability assessments of risks and threats to its ICT infrastructure; (iii) deploy appropriate tools for periodic review of critical applications and systems; (iv) 'harden' all critical hardware and software; and (v) assess and patch or isolate obsolete software from its network.					periodic vulnerability assessments of risks and threats to its ICT infrastructure (as funding permits), deploy appropriate tools for periodic review of critical applications and systems, 'harden' all critical hardware and software; and assess and patch or isolate obsolete software from its network. Implementation date is subject to availability of staff, funds, and competing priorities.
11	UNFCCC should document and execute a plan for timely implementation of all critical recommendations made by the third-party consulting firm relating to the vulnerability test.	Critical	Yes	ICT Security Officer	End of 2020	UNFCCC will have the plan fully prepared by mid of 2019 and will start executing it immediately after. The execution of the plan will be completed by end of 2020. Implementation date is subject to availability of staff, funds, and competing priorities.
12	UNFCCC should develop and deliver periodic training to promote information security awareness among its user community.	Important	Yes	ICT Security Officer	End of 2019	UNFCCC will deliver periodic training about information security awareness among its user community. Implementation date is subject to availability of staff, funds, and competing priorities.
13	UNFCCC should develop and implement a comprehensive user account management policy which: (i) ensures that incompatible roles are not assigned; (ii) defines the criteria for granting and controlling user, remote and privileged access; and (iii) implements password management procedures including periodic review of	Important	Yes	ICT Security Officer	End of 2018	UNFCCC will develop and implement a comprehensive user account management policy accordingly. Implementation date is subject to availability of staff, funds, and competing priorities.

AUDIT RECOMMENDATIONS

Audit of governance, operations and security of information and communications technology 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
	inactive user and administrator access particularly for critical systems.					
14	UNFCCC should: (i) conduct a business impact assessment of its activities and document a business continuity plan to inform the ICT continuity plan; and (ii) conduct periodic tests of the ICT continuity plan.	Important	Yes	Team Lead ICT Project and Service Management Office	End of 2020	Upon completion of the secretariat-wide structure review and the development of a strategic plan, UNFCCC will conduct a high-level business impact assessment of its activities and document a high-level business continuity plan to inform the ICT continuity plan. UNFCCC will conduct periodic tests of the ICT continuity plan, afterwards. Implementation date is subject to availability of staff, funds, and competing priorities.
15	UNFCCC should strengthen the physical controls at its ICT installations by: (i) coordinating with campus security to conduct a risk assessment to define its physical security requirements; (ii) installing additional CCTV cameras as necessary; and (iii) maintaining a log of access to the data rooms.	Important	Yes	ICT Director	End of June 2019	UNFCCC will strengthen the physical controls at its ICT installations. Implementation date is subject to availability of staff, funds, and competing priorities.

APPENDIX I

AUDIT RECOMMENDATIONS

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

Notes on recommendation #3

The UNFCCC secretariat accepts all the audit recommendations and however wishes to put on record its understanding of the findings by the Audit as relates to the following paragraphs;

Paragraph and sub-paragraph	Client comments
19) a)	The benchmarks used by the consulting firm were not the basis for the service delivery and funding model. The benchmark was a cost benchmark for ICT size and ICT budget irrespective of the funding and the services delivery models. The service delivery model and funding model were defined according to industry best practices including COBIT. With regards to benchmarks for ICT size and budget, we would like to emphasize the savings ICT has been able to achieve since 2016 as shared with MT SC for ICT.
19) c)	We would like to draw attention to the fact that relevant stakeholders, including substantive programmes, are part of the MT-SC for ICT. The MT-SC for ICT has the mandate (as per its function #3 in its TOR) to monitor and review the ICT budget. Therefore, the ICT budget was reviewed by the MT-SC for ICT. We direct attention to the following: the members of the MT-SC include: AS, MDA and SDM. • The Administrative Services (AS) Director (as per the MT-SC for ICT TOR), who oversees the finance, HR, procurement and knowledge management functions in the secretariat; • Representatives of MDA and SDM as the biggest FPA clients of ICT in the secretariat, who played an active role in reviewing and approving the budget for ICT; • Representatives of SDM and AS as the biggest users of TCO (indirect) services, who also played a role in reviewing the ICT budget and made interventions such as changing the proposed ICT budget (e.g. in 2016 and 2017 – after the inception of the new funding model). • On an annual basis, all programme directors are informed by the Deputy Executive Secretary of any changes to the funding model and are requested to review them and provide input. • The MT-SC for ICT then reviews and endorses the funding model changes. • All MT-SC chairs provide regular updates to the MT on their respective subcommittee. The TCO MT-SC for ICT is no exception.
19) c) i)	The methodology for the calculation of TCO per capita is based on the actual cost of delivering the TCO services (as defined in the service catalogue) divided by the number of

	non-core funded personnel; please see the TCO budget tables in the TCO budget approved by the MT-SC for ICT. The efficiencies introduced in ICT produced ICT operation cost as highlighted in the ICT funding model that was presented to the MT-SC for ICT in 2016 and 2017. These reductions brought down the total cost of ICT services by more than 40%.
19) c) ii)	The cost of services is clearly itemized in the Service Catalogue approved by the MT-SC for ICT, the detailed FPAs for the specific services provided to client programmes and the quarterly FPA reports. Please consider as evidence the following: • The cost of TCO services as per the ICT service catalogue and the TCO budget approved by the MT-SC for ICT is not tied to the source of funding from secretariat programmes. Please note that since ICT services for supplementary staff are analogous to ICT services for core staff, the cost of the TCO services for supplementary staff is based on a complete set of services, same as for core staff. • FPA service cost is mostly based on person–hours spent on ICT activities agreed in FPA agreements and reported in FPA reports. FPA services are clearly described and costed in the FPA with each client programme and reported quarterly to all client programmes. • For other UN organizations in Bonn, which don't need all the TCO services, the details and the cost of services offered are well documented in the agreements signed with those organizations.
19) c) iii)	ICT services are aligned with the cost of the services. The ICT hourly rate card (comparative cost shown in document "Comparison of internal ICT costs with market costs") demonstrates that ICT service cost is competitive compared with the service cost of external vendors (sourced through a competitive procurement process), which include both nearshore and Germany-based vendors. Additionally, the effectiveness of ICT staff is higher owing to their thorough knowledge of UNFCCC, its programmes, its operations and its systems, eliminating the learning curve witnessed in external vendor arrangements. All ICT costs are attributed to the services described in the service catalogue and approved by the MT-SC for ICT. The efficiencies introduced in ICT produced ICT operation cost as highlighted in the ICT funding model that was presented to the MT-SC for ICT in 2016 and 2017. These reductions brought down the total cost of ICT services by more than 40%.
19) e)	Only project-related activities are charged to the project as described in the timesheet management process (see the file "Time Tracking and FPA process"). The table mentioned illustrates how personnel have assigned time (irrespective of the funding source) to direct activities (projects, services; column "Direct"), indirect activities (i.e. audit; column "Indirect") or overhead (annual sick leave, training, etc.). Only the hours in the column

	"Direct" are charged to client programmes.
19) f)	The Service Catalogue as approved by the MT-SC for ICT clearly describes that the work of the project management office, quality assurance, etc., are indirect costs ("Indirect for common services"). The approved funding model includes key services covered by indirect funding (core, TCO, etc.) – indirect services – which includes the following: management of requirements (ensuring institutional knowledge is kept within the secretariat), project governance (PMO) and quality assurance. Furthermore, the referenced project manager in governance (P-3) is a post that is part of the PMO, provides overview of the management of all ICT projects and is not directly tied to a specific project. PMO services are typically shared services and covered under cost recovery funds, such as core/TCO. The funding source of this post is now aligned with the funding source and category of his supervisor, the Lead Project and Services Management (P-4). His supervisor is currently funded under ICT/TCO. Quality assurance, P-3, provides services related to managing the quality assurance process and standards for all of the secretariat's ICT projects and is not directly tied to a specific project. As a shared and indirect service, it should be covered under ICT/TCO. Lead of requirements engineering, P-3, provides services related to managing the requirements process and standards for all of the secretariat's ICT projects including the preparation of project offers and discussing possible solutions with client programmes (i.e. demand management). These services are typically shared indirect services and covered under TCO.

(*) The related supporting evidence has been provided already as part of our response to the detailed audit results.