United Nations Population Fund

Delivering a world where every pregnancy is wanted,
every childbirth is safe and
every young person's potential is fulfilled

OFFICE OF AUDIT AND INVESTIGATION SERVICES

AUDIT
OF ICT GOVERNANCE AT UNFPA

FINAL REPORT
Nº IA/2025-32

31 December 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

1. The Office of Audit and Investigation Services (OAIS) conducted an audit of ICT Governance at UNFPA. The audit fieldwork took place from 13 October to 11 November 2025.

2. Information and Communication Technology (ICT) Governance refers to the structures, processes, and mechanisms through which an organization ensures that ICT enables and supports the achievement of its strategies and objectives, delivers value, manages risks, optimizes resources, and measures performance. Recognized frameworks such as COBIT[1] and ISO/IEC 38500[2] define ICT governance as a fundamental component of corporate governance, emphasizing accountability, transparency, value delivery, and efficient use of ICT resources.

3. Effective ICT Governance is essential to UNFPA due to the Organisation's firm reliance on digital systems to execute programmatic, operational, and administrative mandates across more than 150 Country Offices and 6 Regional Offices. ICT governance directly influences the Organization's ability to deliver high-quality programmes, support field operations, maintain operational continuity, safeguard information assets, and ensure cost-effective use of financial and technological resources.

4. ICT governance at UNFPA is overseen by the Information Technology Solutions Office (ITSO), which is responsible for ICT strategy development, digital transformation, enterprise architecture, cybersecurity management, ICT project delivery, service management, and overall stewardship of corporate information systems.

5. UNFPA has established a multilayered governance structure to oversee ICT strategy, investments, and operations. Key bodies in the structure include: (a) the ICT Board, (b) the ICT Portfolio Committee; (c) the Enterprise Resource Planning (ERP)/Customer Relationship Management (CRM) Sub-Committee; and (d) a Change Advisory Board.

6. The above governance structure, supported by formal Terms of Reference and consistent meeting documentation, provides a solid foundation for ICT oversight.

7. UNFPA operates in a hybrid environment where several major ICT components (i.e., Quantum,[3] CRM, QuantumPlus,[4] and other productivity and collaboration tools) are delivered through external providers. As a result, ICT governance encompasses internal processes and collaboration with third-party vendors under Long-Term Agreements for infrastructure, cybersecurity, managed services, development, and cloud platforms.

8. ITSO finalized the UNFPA ICT Strategy 2023–2025 in 2023 that identified three strategic themes: (a) mainstreaming of artificial intelligence; (b) increased use of data; and (c) leveraging and scaling innovation initiatives. The strategy aimed to enhance digital capability, modernize systems, and streamline operations. It established thematic objectives but did not prescribe a benefits-realization framework or measurable performance indicators.

[1] Control Objectives for Information and Related Technologies – an IT governance framework by ISACA to help organizations effectively manage and govern their information and technology with business objectives, manage risks, ensure compliance, and optimize resources for digital transformation.
[2] The international standard for the corporate governance of information technology that provides guiding principles, a model, and a framework for governing bodies on effective, efficient, and acceptable use of information technology.
[3] UNFPA's enterprise resource planning system.
[4] QuantumPlus is the Integrated Results and Resources Management platform, linked to Quantum (the UNFPA ERP system) for bidirectional real-time data exchange.

Audit objectives

9. The overall objective of the audit was to assess whether UNFPA's ICT governance framework, policies, practices, and resource management effectively support organizational objectives, with adequate controls and capabilities to sustain digital transformation, ensure efficient use of IT resources, manage risks, and ensure compliance with relevant internal policies and external standards. Specifically, the audit aimed at examining:

a) The design and implementation of the ICT governance framework, including roles, responsibilities, decision-making structures, and alignment with corporate objectives;
b) Risk management practices related to ICT planning, performance monitoring, cybersecurity, and service delivery;
c) The effectiveness of resource management, including budgeting, staffing, and sourcing; and
d) Compliance with applicable UNFPA policies and internationally recognized best practices such as COBIT, ISO/IEC 38500, and other relevant standards, as determined during the audit planning phase.

Methodology and scope

10. The audit was conducted in conformance with the Global Internal Audit Standards promulgated by the Institute of Internal Auditors (The IIA), with reference to recognized ICT governance frameworks, including COBIT and ISO/IEC 38500.

11. The audit adopted a risk-based approach, where objectives were defined, risks identified and ranked, controls evaluated, and tests conducted. The extent of testing was based on an engagement-level risk assessment, with tests of detail conducted on processes assessed to present high or medium risk. A multi-faceted approach was used, including: (a) review of documents provided by ITSO and the ICT governance bodies; (b) analyses of terms of reference and minutes of the ICT Board, ICT Portfolio Committee, ERP/CRM Sub-Committee, and the Change Advisory Board; and (c) review of ICT strategies, investment portfolios, dashboards, risk registers, disaster recovery test results, and vendor contracts.

12. The audit did not include technical testing of ICT systems but focused on governance, oversight, risk management, performance monitoring, and resource stewardship supporting ICT functions.

13. The period covered was from 1 January 2024 to 31 August 2025. Audit tests covering other periods were also conducted, as appropriate.

Overall audit rating

14. OAIS issued an overall audit rating of **"Satisfactory"**, which means that the assessed governance arrangements, risk management practices, and controls were adequately designed and operating effectively to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issues and improvement opportunities identified, if any, did not affect the achievement of the audited entity or area's objectives.

15. The audit provided recommendations to address the following issues: (a) The effectiveness of ICT Board oversight could benefit from additional expertise; (b) absence of a framework to measure the realization of ICT project benefits; and (c) key-person dependencies in critical ICT functions.

16. Ratings by key audit area are summarized in the following table.

Audit ratings by key audit area		
Strategic Alignment		**Satisfactory**
Risk Management		**Satisfactory**
Value Delivery		**Some improvement needed**
Performance Measurement		**Satisfactory**
Resource Management		**Some improvement needed**

Good practices identified

17. UNFPA established a solid foundation for ICT governance, supported by formal structures, documented processes, active engagement of its governance bodies, formal terms of reference for the governance bodies, a documented ICT strategy, and well-established change management and oversight mechanisms. Additionally, ITSO has, in recent years, strengthened ICT governance documentation, producing clearer policies, prioritization matrices, and risk registers. At the time of the audit fieldwork, ITSO was updating the ICT Strategy for 2026–2029 to align with the Organization's strategic planning cycle and ensure that future ICT priorities more fully reflect evolving organizational needs. These good practices are incorporated in the relevant issues noted in this report, as appropriate, and summarized here.

Key recommendations Total = **3**, High priority = **0**

18. No high priority recommendation was identified in this audit.

Implementation status of previous OAIS recommendations

19. ICT governance at UNFPA has not previously been audited by OAIS.

Management comments and action plan

20. The Director, ITSO, accepted all four recommendations in this report and is already implementing them. Comments and additional information provided have been incorporated in the report, where appropriate.

21. Management appreciates the collaboration with OAIS throughout this audit and the overall finding that ICT governance at UNFPA is at a satisfactory level. Management asserts that the current governance processes are effective and represent a good balance between governance overheads and benefits achieved through governance. Management highlights that while there are always opportunities for strengthening governance, additional governance overheads may not bring benefits that warrant the costs. Management would have welcomed a benefits calculation indicating that the suggested recommendations would be a net positive for the organization.

Acknowledgement

22. The OAIS team hereby thanks the Management and personnel of ITSO, members of the ICT governance bodies who contributed to the audit, and staff of various other Headquarter units and field offices[5] for their cooperation and assistance throughout the audit.

[5] Field offices include Country, Regional, Sub-Regional, and Liaison Offices.

Signed by:
50458A3AFD0C4EF...

Moncef Ghrib
Director
Office of Audit and Investigation Services

I. AUDIT BACKGROUND

1. Information and Communication Technology (ICT) Governance refers to the structures, processes, and mechanisms through which an organization ensures that ICT enables and supports the achievement of its strategies and objectives, delivers value, manages risks, optimizes resources, and measures performance. Recognized frameworks such as COBIT[6] and ISO/IEC 38500[7] define ICT governance as a fundamental component of corporate governance, emphasizing accountability, transparency, value delivery, and efficient use of ICT resources.

2. Effective ICT Governance is essential to UNFPA due to the Organization's firm reliance on digital systems to execute programmatic, operational, and administrative mandates across more than 150 Country Offices and 6 Regional Offices. ICT governance directly influences the Organization's ability to deliver high-quality programmes, support field operations, maintain operational continuity, safeguard information assets, and ensure cost-effective use of financial and technological resources.

3. The core ICT Governance practices at UNFPA include:

a) Strategic alignment of ICT investments with the UNFPA Strategic Plan, transformative results, and digital transformation efforts;

b) Risk management, including ICT risks documented in ITSO registries and business risks reflected in the enterprise risk Management (ERM) system;

c) Value delivery through prioritization, approval, and monitoring of ICT initiatives via structured decision-making bodies;

d) Performance measurement through operational dashboards and periodic reporting to governance bodies; and

e) Resource management, including workforce planning, vendor management, and oversight of ICT procurement activities.

4. ICT governance at UNFPA is overseen by the Information Technology Solutions Office (ITSO), which is responsible for ICT strategy development, digital transformation, enterprise architecture, cybersecurity management, ICT project delivery, service management, and overall stewardship of corporate information systems.

5. UNFPA has established a multilayered governance structure to oversee ICT strategy, investments, and operations. Key bodies in the structure include the following:

a) An ICT Board chaired at the senior-most level by the Assistant Secretary General/Deputy Executive Director (Management), which serves as the Organization's central decision-making body for ICT priorities and investments;

b) An ICT Portfolio Committee that provides recommendations to the ICT Board for decision making, and reviews ICT investment proposals and prioritization matrices, and supports annual planning cycles;

c) An Enterprise Resource Planning (ERP)/Customer Relationship Management (CRM) Sub-Committee, responsible for oversight of enterprise system enhancements and roadmap prioritization; and

[6] Control Objectives for Information and Related Technologies – an IT governance framework by ISACA to help organizations effectively manage and govern their information and technology with business objectives, manage risks, ensure compliance, and optimize resources for digital transformation.

[7] The international standard for the corporate governance of information technology that provides guiding principles, a model, and a framework for governing bodies on effective, efficient, and acceptable use of information technology.

d) A Change Advisory Board that oversees Information Technology (IT) changes and approves the release of the changes to the IT production environment.

6. The above governance structure, supported by formal Terms of Reference and consistent meeting documentation, provides a documented foundation for ICT oversight.

7. UNFPA operates in a hybrid environment where several major ICT components (i.e., Quantum,[8] CRM, QuantumPlus,[9] and other productivity and collaboration tools) are delivered through external providers. As a result, ICT governance encompasses internal processes and collaboration with third-party vendors under Long-Term Agreements (LTA) for infrastructure, cybersecurity, managed services, development, and cloud platforms.

8. ITSO finalised the UNFPA ICT Strategy 2023–2025 in 2023 that outlines three strategic themes: (a) mainstreaming of artificial intelligence; (b) increased use of data; and (c) leveraging and scaling innovation initiatives. The strategy aims to enhance digital capability, modernize systems, and streamline operations. It establishes thematic objectives but does not prescribe a benefits-realization framework or measurable performance indicators.

9. The Organization has strengthened its ICT governance documentation to include the following:

a) The ICT Governance Policy;
b) Third-Party ICT Risk Management Policy;
c) Risk registers and mitigation plans;
d) Disaster recovery plans and the related periodic testing reports; and
e) Project briefs, prioritization matrices, lesson-learned documents, and investment portfolios.

Audit objectives, Methodology, and Scope

10. As set out in the 2025 Annual Work Plan, an audit of ICT Governance at UNFPA was initiated was conducted in in conformance with the Global Internal Audit Standards promulgated by the Institute of Internal Auditors (The IIA), with reference to recognised ICT governance frameworks, including COBIT[1] and ISO/IEC 38500.[2]

11. The overall objective of the audit was to assess whether UNFPA's ICT governance framework, policies, practices, and resource management effectively support organizational objectives, with adequate controls and capabilities to sustain digital transformation, ensure efficient use of IT resources, manage risks, and ensure compliance with relevant internal policies and external standards. Specifically, the audit aimed at examining:

a) The design and implementation of the ICT governance framework, including roles, responsibilities, decision-making structures, and alignment with corporate objectives;
b) Risk management practices related to ICT planning, performance monitoring, cybersecurity, and service delivery;
c) The effectiveness of resource management, including budgeting, staffing, and sourcing; and
d) Compliance with applicable UNFPA policies and internationally recognized best practices such as COBIT, ISO/IEC 38500, and other relevant standards, as determined during the audit planning phase.

12. The audit adopted a risk-based approach, where objectives were defined, risks identified and ranked, controls evaluated, and tests conducted. The extent of testing was based on an engagement-level

[8] UNFPA's enterprise resource planning system.
[9] QuantumPlus is the Integrated Results and Resources Management platform, linked to Quantum (the UNFPA ERP system) for bidirectional real-time data exchange.

risk assessment, with tests of detail conducted on processes assessed to present high or medium risk. A multi-faceted approach was used, including:

a) Review of over 200 documents provided by ITSO and the ICT governance bodies;
b) Analyses of terms of reference and minutes of the ICT Board, ICT Portfolio Committee, ERP/CRM Sub-Committee, and the Change Advisory Board;
c) Review of ICT strategies, investment portfolios, dashboards, risk registers, disaster recovery test results, and vendor contracts;
d) Interviews with ITSO Management and functional focal points; and
e) Interviews with members of the ICT Board, including Regional Directors and Headquarters divisional leaders.

13. The audit did not include technical testing of ICT systems but focused on governance, oversight, risk management, performance monitoring, and resource stewardship supporting ICT functions.

14. The period covered was from 1 January 2024 to 31 August 2025. Audit tests covering other periods were also conducted, as appropriate.

15. The audit fieldwork took place from 13 October to 11 November 2025.

II. AUDIT RESULTS

16. The audit results are presented below, by audit area.

A. STRATEGIC ALIGNMENT	SATISFACTORY

Issue 1: The effectiveness of ICT Board oversight could benefit from additional expertise

17. Effective IT governance requires structured meetings of governance bodies to allow deeper discussions, informed decision-making, and availability of all relevant data to decision makers. According to COBIT 2019, the governance framework must ensure that ICT-related processes are effectively and transparently overseen, and that ICT Board decisions are based on a thorough understanding of the proposed investment and its implications for achieving UNFPA's strategy.

18. While the ICT Board received substantial information packages ahead of its meetings, the Board members expressed a lack of the necessary ICT expertise to fully utilize the information for informed oversight. Specifically, the information provided to the Board was seen as:

a) Having a qualitative bias – the information presented was predominantly qualitative rather than quantitative, lacking sufficient metrics and evidence-based analyses for strategic decision-making, particularly when addressing large-scale initiatives such as artificial intelligence (AI) implementation or adoption of IT collaboration environments and tools (e.g., Google Workspace). ITSO Management explained that the use of quantitative information in ICT initiatives was often highly technical; and

b) Being overly technical in focus – Board discussions often retained a high technical focus, making it challenging for non-specialist members to contribute meaningfully or to use the meeting contents to make informed decisions.

19. ITSO Management indicated that in-depth technical analysis was the responsibility of the ICT Portfolio Committee, not the ICT Board. However, the practice does not ensure that complex technical submissions consistently translate into strategically relevant, quantitative information for ICT Board deliberations. Management further indicated that a review of ICT Board meeting recordings and minutes did not identify instances where Board members explicitly stated that they lacked adequate information to make decisions. Notwithstanding the ITSO Management explanations, some ICT Board members interviewed indicated that they experienced challenges in interpreting highly technical or qualitative information, suggesting that opportunities remain to further enhance the clarity and strategic focus of information provided to support effective ICT governance at the Board level.

ROOT CAUSE	*Guidance: Inadequate oversight by Headquarters (failure to ensure that the ICT Portfolio Committee effectively bridges technical expertise gaps before passing information to the Board for deliberation and decision-making).*
IMPACT	*The ICT Board's ability to consistently carry out informed oversight and decision-making is diminished.*
CATEGORY	*Strategic*

Recommendation 1	**Priority: Medium**
Strengthen decision-support arrangements for the ICT Board to ensure that members can effectively interpret, challenge, and use technical information for governance and investment decision-making.	

This should be achieved by: a) providing concise, decision-oriented summaries that translate technical matters into business, risk, and strategic implications for the ICT Board's consideration. b) clearly articulating the key ICT risks, trade-offs, and dependencies in Board papers; and c) periodically assessing whether existing governance arrangements, information flows, and supporting committees adequately enable informed ICT Board oversight.
Manager Responsible for Implementation: Director, ITSO.
Status: *Agree.*
Management action plan: In line with the ICT Strategy 2026-2029, Management will review the ICT Portfolio Committee's terms of reference and update its membership.
Estimated completion date: *July 2026.*

B. RISK MANAGEMENT — SATISFACTORY

20. Audit work performed in this area focused on assessing whether ICT risks were appropriately identified, assessed, reflected in the ERM system, and communicated to relevant stakeholders.

21. The audit examined ICT risk registers, ERM entries for ICT-related risks, disaster recovery testing results, ICT governance minutes where risk matters were discussed, and the process for communicating risk during project initiation, change management, and release management activities.

22. No reportable matters were identified based on the audit work performed.

C. VALUE DELIVERY — SOME IMPROVEMENT NEEDED

Issue 2: Absence of a framework to measure the realization of ICT project benefits

23. According to COBIT 2019 (EDM02 – Ensure Benefits Delivery) and ISO/IEC 38500 (Principle 3: Strategy), ICT governance bodies should ensure that ICT investments are supported by: (a) clearly defined and measurable expected benefits; (b) assigned benefit owners; (c) mechanisms to track performance against planned outcomes; (d) post-implementation reviews assessing achievement of intended value; and (e) visibility into whether digital investments contribute to organizational strategies.

24. Several positive elements that support value delivery were noted in the ICT governance arrangements. The Organization had a structured process for initiating and prioritizing ICT initiatives through the ICT Board, the ERP/CRM Sub-Committee, and the ICT Portfolio Committee - each operating under formal terms of reference and meeting regularly, as anticipated. A standardized project prioritisation matrix was used to support transparent investment decisions, and ITSO provided the ICT governance bodies with comprehensive documentation on project proposals, system roadmaps, and progress updates. These practices demonstrated a strong foundation for planning and decision-making around ICT investments.

25. The above arrangements did not include a structured, organization-wide framework for measuring, tracking, and reporting the realization of ICT project benefits.

26. A review of project briefs, prioritization matrices, ICT Board minutes, and annual workplans confirmed that the governance bodies primarily tracked project initiation and delivery milestones but did not systematically monitor post-implementation results or verify whether the intended benefits were achieved. There were no corporate templates or indicators to quantify the expected outcomes (e.g., productivity gains, process efficiency, cost savings, user adoption, programme effectiveness). ICT Board members acknowledged that reporting remained qualitative and narrative, making it challenging to assess realized value or alignment with the ICT strategy.

27. As a result of the foregoing, the Organization could not reliably determine the extent to which ICT investments delivered measurable value, supported the objectives of the ICT strategy, or contributed to the broader outcomes of the UNFPA Strategic Plan.

28. Further, the audit identified two contextual factors that further weakened value delivery across the ICT governance environment. These are:

a) Limited linkage between ICT priorities and field operational needs. Regional Directors reported that prioritization processes were largely Headquarters-driven and did not consistently incorporate structured inputs from the Regional or Country Offices. This weakened alignment with operational realities and limited the adoption or perceived usefulness of corporate digital solutions. OAIS hereby notes that the development process for the upcoming ICT Strategy 2026–2029 includes strengthened mechanisms to capture field needs, which, once implemented, are expected to improve alignment with operational realities;

b) Duplication of local digital initiatives and limited visibility of field-developed tools. In several cases, field offices[10] independently developed or procured small-scale digital solutions outside the corporate oversight channels, contributing to shadow IT, inconsistent data governance, and potential duplication of effort. UNFPA did not maintain a consolidated inventory or governance mechanism for these solutions.

29. ITSO Management indicated that, as members as the ICT Board, Regional Directors were directly involved in prioritization and nominated members (one for each region) to the ICT Portfolio Committee - giving the regions a majority in both governance bodies. Management also highlighted that it maintained an inventory of all IT solutions that had undergone ICT governance processes, as well as any solutions subsequently disclosed. Further, Management indicated that the audit observations did not constitute a material issue, noting that (a) most ICT resources were devoted to operations rather than investments; (b) benefits measurement was inherently challenging for small projects; and (c) no new initiatives were launched locally during the audit period.

30. While Management's point of view is noted, the audit concludes that having a structured benefits-realization framework is an established good practice and its absence at UNFPA reduces transparency and limits the ability of governance bodies to assess whether ICT initiatives deliver measurable value aligned with UNFPA's strategy.

ROOT CAUSE	*Guidelines: Lack of or inadequate corporate policies or procedures (absence of a formal, organization-wide methodology for defining, tracking, and reporting ICT project benefits and no structured mechanism to systematically incorporate field needs into ICT prioritization.)*
IMPACT	*It is difficult to demonstrate whether ICT investments achieve their intended outcomes or contribute to organizational efficiency, effectiveness, and strategic objectives, creating the risk of limited value realization, duplication of digital effort, misalignment with operational needs, and reduced accountability for ICT decisions.*

[10] Field offices include Country, Regional, Sub-Regional, and Liaison Offices.

CATEGORY *Strategic*

Recommendation 2	**Priority: Medium**
Formalize a benefits definition and follow-up process for ICT initiatives to include: a) a concise benefits-definition template to accompany all project proposals submitted to the ICT Board and its sub-committees; b) preparation, for ITSO-led initiatives, of benefits definitions and submission of post-implementation updates to the ICT Board to assess benefits realization; and c) provision, for business-led initiatives, of templates and guidance to business owners and the establishment of a mechanism to monitor whether business owners submit the necessary post-implementation benefit updates to the ICT Board.	
Manager Responsible for Implementation: Director, ITSO.	
Status: *Agree.*	
Management action plan: Management notes the importance of ensuring that any additional governance measures remain proportionate and cost-effective and will develop a benefits review process and template.	
Estimated completion date: *November 2026.*	

D. PERFORMANCE MEASUREMENT — SATISFACTORY

31. Audit work performed in this area focused on assessing whether ICT performance information was sufficiently defined, monitored, and reported to support oversight and decision-making by ICT governance bodies.

32. The audit reviewed ICT performance reports and management information presented to the ICT Board, as well as relevant governance minutes, ICT strategy documents, and performance-related sections of project and operational reporting. Interviews were conducted with ITSO management and selected members of ICT governance bodies to understand how performance information was used in practice.

33. While opportunities were identified to further enhance the strategic focus and consistency of performance information, these were assessed as incremental improvements and did not indicate material weaknesses in the design or operation of ICT performance measurement practices. These have been reported in a separate memorandum as they were of low risk.

E. RESOURCE MANAGEMENT — SOME IMPROVEMENT NEEDED

Issue 3: Key-person dependencies in critical ICT functions

34. International good practice, including COBIT 2019 (APO07 – Manage Human Resources; APO10 – Manage Vendors; BAI09 – Manage Assets) and ISO/IEC 38500 (Principle 5: Performance), emphasize that ICT governance should ensure adequate redundancy for critical functions, structured cross-training, and accessible documentation to support continuity of operations.

35. Critical ICT functions at UNFPA remained dependent on a small number of highly specialized staff, particularly in areas such as cybersecurity, cloud and infrastructure management, and ERP/CRM support. Review of job descriptions, organograms, and interviews conducted indicated that, while alternates were designated for most key roles, the depth of cross-training and the consistency of documentation supporting handover varied across the teams. This condition was also identified in the 2025 Business Impact Analysis (BIA), which noted "*single point of failure in personnel*" risks and recommended strengthening cross-training, documenting key processes, and defining contingency arrangements for staff unavailability.

36. ITSO took several steps to mitigate the above risks. For instance: (a) the critical roles and alternates register provided visibility on primary and secondary role coverage; the 2025 incident response tabletop exercise incorporated scenarios involving staff absence to test decision-making continuity; and an agreement with the United Nations International Computing Centre (UNICC) for Google Cloud Platform-managed services represented a deliberate effort to reduce reliance on internal specialists for certain technical functions. These positive measures demonstrated ITSO's ongoing efforts to address capacity risks within the available resources.

37. ITSO Management expressed the view that the risks were managed within acceptable tolerances, noting stable staffing levels, successful recruitment efforts, and strategic use of LTAs and shared services. Management also emphasized the importance of ensuring that additional documentation requirements remained proportionate and did not divert resources from core ICT activities.

38. While taking into consideration the above Management views, the audit team concluded that residual risks remained due to the absence of a formal, consolidated workforce-resilience approach, particularly in relation to cross-training depth and structured documentation. The mitigation measures implemented were positive and addressed individual areas of exposure; however, they were not applied systematically across all critical ICT functions. Key-person dependency remained an area that could be further strengthened to enhance operational resilience.

ROOT CAUSE	*Guidelines: Inadequate planning (absence of a formal framework for capacity planning, documentation, succession mechanisms, and consistent routing of ICT-related procurements for technical review).*
IMPACT	*The risks of service disruption, delayed incident response, and reduced operational resilience are heightened.*
CATEGORY	*Operational.*

Recommendation 3	**Priority: Medium**
Formalize the structured continuity arrangements for critical ICT functions in line with the mitigation actions identified in the 2025 Business Impact Analysis (BIA). They should include: a) Cross-training arrangements for the most critical roles identified in the BIA, documented at team level and incorporated into regular operational planning; b) Documentation of key operational processes essential for continuity, stored in an accessible repository and reviewed at least annually; and c) Clear contingency and escalation arrangements to manage temporary unavailability of critical personnel, reflecting practices tested during the 2025 tabletop exercise. Implementation should be built on existing measures already in place (e.g., alternates, outsourcing arrangements, shared services, etc.) and remain proportional to available resources.	
Manager Responsible for Implementation: Director, ITSO.	
Status: *Agree.*	

Management action plan: Management will further document the measures in place, taking into account the available resources.
Estimated completion date: *November 2026.*

ANNEX I - DEFINITION OF AUDIT TERMS

A. AUDIT RATINGS

Audit rating definitions, adopted for use in reports for audit engagements initiated as of 1 January 2016[11], are explained below:

▪ **Satisfactory**	The assessed governance arrangements, risk management practices and controls were adequately designed and operating effectively to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issue(s) and improvement opportunities identified, if any, did not affect the achievement of the audited entity or area's objectives.
▪ **Partially Satisfactory with Some improvement needed**	The assessed governance arrangements, risk management practices and controls were adequately designed and operating effectively but needed some improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issue(s) and improvement opportunities identified did not significantly affect the achievement of the audited entity/area objectives. Management action is recommended to ensure that identified risks are adequately mitigated.
▪ **Partially Satisfactory with Major improvement needed**	The assessed governance arrangements, risk management practices, and controls were generally established and functioning but need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issues identified could significantly affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.
▪ **Unsatisfactory**	The assessed governance arrangements, risk management practices and controls were not adequately established or functioning to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issues identified could seriously compromise the achievement of the audited entity or area's objectives. Urgent management action is required to ensure that the identified risks are adequately mitigated.

B. CATEGORIES OF ROOT CAUSES AND AUDIT ISSUES

Guidelines: absence of written procedures to guide staff in performing their functions

- Lack of or inadequate corporate policies or procedures
- Lack of or inadequate Regional and/or Country Office policies or procedures
- Inadequate planning
- Inadequate risk management processes
- Inadequate management structure

Guidance: inadequate or lack of supervision by supervisors

- Lack of or inadequate guidance or supervision at the Headquarters and/or Regional and Country Office level
- Inadequate oversight by Headquarters

[11] Based on the proposal of the Working Group on harmonization of engagement-level audit ratings approved by the United Nations Representatives of Internal Audit Services (UN-RIAS) in September 2016.

Resources: insufficient resources (funds, skills, staff) to carry out an activity or function:

- Lack of or insufficient resources: financial, human, or technical resources
- Inadequate training

Human error: un-intentional mistakes committed by staff entrusted to perform assigned functions

Intentional: intentional overriding of internal controls.

Other: factors beyond the control of UNFPA.

C. PRIORITIES OF AGREED MANAGEMENT ACTIONS

Agreed management actions are categorized according to their priority as a further guide to Management in addressing the related issues in a timely manner. The following priority categories are used:

- **High** Prompt action is considered imperative to ensure that UNFPA is not exposed to high risks (that is, where failure to take action could result in critical or major consequences for the organization).
- **Medium** Action is considered necessary to avoid exposure to significant risks (that is, where failure to take action could result in significant consequences).
- **Low** Action is desirable and should result in enhanced control or better value for money. Low priority management actions, if any, are discussed by the audit team directly with the Management of the audited entity during the course of the audit or through a separate memorandum upon issued upon completion of fieldwork, and not included in the audit report.

D. CATEGORIES OF ACHIEVEMENT OF OBJECTIVES

These categories are based on the COSO framework and derived from the INTOSAI GOV-9100 Guide for Internal Control Framework in the Public Sector and INTOSAI GOV-9130 ERM in the Public Sector.

- **Strategic** High level goals, aligned with and supporting the entity's mission
- **Operational** Executing orderly, ethical, economical, efficient, and effective operations and safeguarding resources against loss, misuse, and damage
- **Reporting** Reliability of reporting, including fulfilling accountability obligation
- **Compliance** Compliance with prescribed UNFPA regulations, rules, and procedures, including acting in accordance with Government Body decisions, as well as agreement specific provisions

GLOSSARY

Acronym	Description
AI	Artificial Intelligence
BIA	Business Impact Analysis
COBIT	Control Objectives for Information and Related Technologies
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
ICT	Information and Communications Technology
IIA	Institute of Internal Auditors
IT	Information Technology
ITSO	Information Technology Solutions Office
LTA	Long-Term Agreement
OAIS	Office of Audit and Investigation Services
UNFPA	United Nations Population Fund