Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2024/041

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

Control processes relating to governance, operations and security need to be strengthened

6 September 2024
Assignment No. AT2023-812-01

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, operations and security at the United Nations Assistance Mission for Iraq (UNAMI). The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes for ICT governance, operations and security at UNAMI. The audit covered the period from January 2020 to October 2023 and included a review of: (a) ICT governance and risk management; (b) ICT project management; (c) ICT operations; (d) information security; (e) ICT access management; and (f) data governance and management.

The audit indicated that UNAMI needs to strengthen its control processes relating to ICT governance, operations and security.

OIOS made 9 recommendations. To address the issues identified in the audit, UNAMI needed to:

- Strengthen ICT governance by establishing a local ICT committee with formal terms of reference and representation from all relevant stakeholders;
- Strengthen its risk management procedures by conducting a risk assessment of its entire ICT and operational technology landscape and integrating the results into its entity-level risk register;
- Strengthen ICT project management by adhering to the requirements of the Secretariat's project management methodology and ST/AI/2005/10 on ICT initiatives;
- Reassess the funding and cost recovery model for ICT services provided to the United Nations Country Team by documenting the total cost of delivery of services and adopting cost recovery based on the number of users and/or ICT resource utilization;
- Strengthen the change and configuration procedures by establishing a change review board with terms of reference, tracking of change requests, and establishing a configuration management process;
- Ensure regular and comprehensive patch management for both Windows and non-Windows systems; ensure comprehensive and regular updates of firmware; conduct regular, comprehensive and authenticated vulnerability scans of its ICT infrastructure; establish secure configuration guidelines for all critical equipment; and address the vulnerabilities identified in the vulnerability scans;
- Strengthen operational resilience and recovery by conducting a business impact assessment of critical mission activities to define Recovery Point Objectives and Recovery Time Objectives and to inform the Disaster Recovery Plan;
- Strengthen its user access controls by implementing regular reviews of user accounts and access rights; and
- Strengthen data governance and management by assigning centralized archives and records management responsibilities, developing and implementing data retention policies, and fully implementing the Secretary-General's data strategy.

UNAMI accepted eight recommendations and has initiated action to implement them. Actions required to close the recommendations are indicated in Annex I. However, UNAMI did not accept the recommendation concerning the funding and cost recovery for ICT services. OIOS maintains that the current practices in UNAMI do not comply with the policy established by the Controller. This unaccepted recommendation has been closed without implementation, indicating management's acceptance of residual risks.

CONTENTS

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, operations and security at the United Nations Assistance Mission for Iraq (UNAMI).

2. UNAMI is a Special Political Mission established in 2003 by Security Council Resolution 1500 at the request of the Government of the Republic of Iraq. The mandate was revised by the Council's resolution 1770 (2007) and has since been extended on an annual basis.

3. The United Nations in Iraq comprises two field missions: UNAMI and the United Nations Investigative Team for Accountability of crimes committed by Da'esh/ Islamic State in Iraq and the Levant (UNITAD). The United Nations Country Team (UNCT) in Iraq comprises 24 United Nations agencies, funds and programmes including 19 resident and five non-resident agencies. UNAMI supports inter-agency coordination and liaison with United Nations agencies, funds and programmes, working at the community, governorate and national levels across the Republic of Iraq. Currently, there are approximately 648 personnel, 251 international staff and 397 national staff working for the Mission in Iraq. Also under the purview of UNAMI is the Kuwait Joint Support Office (KJSO) with 33 out of 41 positions funded by UNAMI and the Resident Coordinator's office in Kuwait.

4. The Operations and Resource Management pillar of UNAMI is responsible for the provision of general support and the management of operations and resources. The Chief of Operations and Resource Management, reporting to the Chief of Mission Support, oversees the Human Resources Section, the Financial Resourcing and Performance Unit, the Field Technology Section (FTS), and the regional offices in Erbil and Kirkuk. FTS provides ICT services to Country Team entities co-located within the Baghdad and Erbil campus, UNITAD, KJSO, and the Resident Coordinator's office in Kuwait. UNCT consists of 13 entities (funds and programmes) that are offered ICT support services on a cost recovery basis.

5. FTS operates under the policy framework of the United Nations Secretariat and works in close cooperation with the Office of Information and Communications Technology (OICT). Cybersecurity requirements are embedded within the ICT policies. UNAMI is responsible for operationalizing the policies at the local level and implementing additional measures to mitigate risks. FTS had 42 staff in total, comprising 13 international (inclusive of 2 Information Management Assistants) and 29 national staff.

6. Resources amounting to $2.8 million and $2.7 million were proposed in the budgets for 2022 and 2023, respectively (excluding staff costs) to provide ICT activities. In addition, the 2022 cost plan projected cost recoveries for UNAMI of $13.5 million.

7. Comments provided by UNAMI are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

8. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes for ICT governance, operations and security at UNAMI.

9. This audit was included in the 2023 OIOS risk-based work plan because of the high risks associated with ICT systems supporting UNAMI operations and the criticality of the ICT infrastructure in ensuring

that the Mission's mandate is accomplished. Further, due to the high prevalence of cybersecurity-related attacks, the audit scope also included cybersecurity preparedness.

10. OIOS conducted this audit from June to October 2023. The audit covered the period from January 2020 to October 2023. Based on an activity-level risk assessment, the audit covered risk areas in the ICT governance, operations and security which included: (a) ICT governance and risk management; (b) ICT project management; (c) ICT operations; (d) information security; (e) ICT access management; and (f) data governance and management.

11. The audit methodology included: (a) interview with key personnel; (b) review of relevant documentation; (c) analytical review of data; (d) testing of controls; and (e) vulnerability scanning of local ICT infrastructure.

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

III. AUDIT RESULTS

A. ICT governance and risk management

Need to strengthen ICT governance

13. ICT governance mechanisms should determine priorities for ICT investments, provide guidance for the management of ICT resources, define roles and responsibilities of stakeholders, and establish procedures for managing risks. UNAMI had developed standard operating procedures (SOP) and policies such as ICT services usage policy, SOP on provision of official mobile communication devices and services, and guidance on the use, access and safety of communication towers. Further, UNAMI had established a Working Group with representation from United Nations agencies that discussed connectivity and costing of FTS services.

14. ST/AI/2005/10 on ICT initiatives requires establishing an ICT committee to ensure that ICT initiatives are supported by a high-level business case, are updated in the ICT assets inventory, and comply with ICT standards while avoiding duplication of initiatives. Although the Special Representative of the Secretary-General (SRSG) of UNAMI is a rotating member of the global ICT Steering Committee, UNAMI did not have a local ICT Steering Committee. FTS had proposed to the Chief of Mission Support the need to establish a local ICT committee. UNAMI undertook several ICT projects such as i-Entry access control, Closed Circuit Television (CCTV), the United Nations Guard Unit meal management system, migration of local servers to the cloud, and repeater site replacement. The projects on Field Remote Infrastructure Monitoring (FRIM) and community applications were ongoing. Further, there were other operational and digitization projects within UNAMI (e.g., technology-enabled environment projects) that were not managed by FTS which also needed visibility and oversight.

15. Inadequate ICT governance mechanisms may expose UNAMI to the risk of inability to meet its ICT needs for effective and timely mandate implementation.

(1) UNAMI should strengthen ICT governance by establishing a local ICT committee with formal terms of reference and representation from all relevant stakeholders.

UNAMI accepted recommendation 1 and stated that it will continue to strengthen ICT governance by establishing a local ICT committee with formal terms of reference and representation from all relevant stakeholders.

Need to assess and embed ICT risks in the risk management process

16. Best practice recommends that since ICT comprises some of an organization's most valuable assets, cybersecurity-related risks that threaten these assets need to be integrated into the enterprise risk management so that senior management has a clear understanding of the entity's cybersecurity posture and facilitates informed and timely mitigation of the associated risks. Further, the Secretariat's enterprise risk management framework requires Secretariat entities to assess their risks, including information security and cybersecurity risks.

17. UNAMI had a mission-wide risk register, and FTS had a dedicated risk management role with staff that were trained in managing risks. The audit showed that roles and responsibilities for ICT security needed to be strengthened across all aspects of UNAMI's activities – not just technology – to ensure that cybersecurity risks are also considered as part of a holistic approach towards risk management. Also, there was no clarity in terms of responsibilities for identification of ICT security-related risks at the business level, and their upward flow to inform the enterprise risk register. While many of the business areas understood their business risks, their understanding of cybersecurity risks was limited; they believed this to be the responsibility of FTS. While FTS had implemented measures to address some of the risks – such as awareness training, resilience and redundancy mechanisms – ICT risk assessments were not conducted holistically to cover the entire UNAMI digital landscape. For instance, there were no operational risks or operational technology risks among the risks rated as very high, high, or medium in UNAMI's entity-level risk register, indicating a lack of integration of the ICT and operational technology risk assessment into the entity-level risk assessment process.

(2) UNAMI should strengthen its risk management procedures by conducting a risk assessment of its entire ICT and operational technology landscape and integrating the results into its entity-level risk register.

UNAMI accepted recommendation 2 and stated that it will conduct a thorough risk assessment of all relevant areas. The findings will then be systematically integrated into the entity-level risk register to ensure comprehensive tracking and management of identified risks.

Need to implement segregation of duties to prevent role conflicts

18. Best practice requires that ICT responsibilities are clearly defined and allocated. Further, conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Segregation of duties also provides controls to enhance the detection of errors and control failures such as security breaches, data theft, and bypassing of security controls.

19. OIOS observed the following role conflicts:

(a) The security and compliance team were assigned ICT compliance and assurance responsibilities, and the team reported to the Chief of the Innovation and Technology Unit in FTS. This arrangement gave rise to a conflict because this Unit was also responsible for other operational activities (such as network and server management) which should be independently reviewed for security compliance. The role should have visibility of all FTS functions and require collaboration with other units in UNAMI, with a direct reporting line to the Chief of FTS.

(b) In the Operations Management Unit, there was an administrator who had roles of system administrator, compliance and monitoring, and business user which could result in conflicts. Further, the administrator was the sole administrator of the system which is a service continuity risk.

(c) A network engineer was responsible for managing the local area network end-to-end, which included operations, enforcement and compliance. There network engineer also set network policies, conducted operations, and monitored compliance. The compliance role should appropriately be part of the functions of the Security and Compliance Unit. UNAMI explained that FTS and mission management formulate the network services policy with oversight provided by the ICT Compliance Unit, while the Network Operations Unit maintains a real-time monitoring station to swiftly apply mitigating measures where necessary and ensure uninterrupted service delivery.

20. UNAMI explained that unique operational contexts such as the mandated Rest and Recuperation schedule for internationally recruited staff every 28 days require the mapping of roles to additional tasks to ensure seamless business continuity during the absence of the designated staff member. Also, sensitive systems like CCTV and access control had limited roles, which was in line with the Department of Safety and Security's guidance that only limited staff should have access.

21. Role conflicts increase the risks of unauthorized activities, malicious or inadvertent breach of system security, data integrity, and potential disruption of normal business processes. *UNAMI stated that FTS operational organigram is designed to be dynamic and adaptable, ensuring alignment with mission objectives and maintaining thorough accountability and visibility of roles across all operational domains. Also, FTS operates under a segregation of duties framework, segregating roles where applicable. Contingent measures within the structure define distinct lead roles and tandems, customized to meet specific services within the FTS service portfolio. Due to human resource constraints, FTS strategically delegates supplementary roles and responsibilities to individuals or groups, maintaining clear boundaries among various functional teams. Additionally, the direct assignment of ICT security under the Chief FTS's purview enhances oversight and fortifies security protocols. Proactive measures have been undertaken to enhance the organigram's efficacy in risk mitigation. Further, the direct assignment of ICT security under the purview of the Chief FTS enhances oversight and fortifies security protocols.*

B. ICT project management

Need to strengthen project management

22. ST/AI/2005/10 requires that ICT initiatives estimated to cost more than $200,000 in combined monetary and staff resources over four years shall be reviewed by the Project Review Committee. Further, the administrative instruction requires departments and offices to submit approved high-level business cases for ICT initiatives in support of the relevant portions of their proposed budget requests and shall include references to approved high-level business cases for ICT initiatives when requesting the procurement of goods or services related to such initiatives. There is also a requirement in the project management framework to integrate information security into the project lifecycle.

23. In 2023, FTS had eight ongoing ICT projects with an assigned Project Manager role. However, it had not fully adopted the Secretariat's ICT project management methodology and technical standards. OIOS noted the following:

(a) While documentation on global projects such as Unite FRIM, Network Segmentation, and migration from local Active Directory to Azure was available, the project management documentation of

locally managed projects was unavailable or inadequate. For example, the documentation for i-Entry, CCTV (Erbil) replacement, the United Nations Guard Unit meal management system, and Community app for mission support services were limited and did not adequately describe the business case, options appraisal, and cost-benefit analysis together with detailed project plans with milestones, activities and interdependencies. The CCTV project brief was documented during the audit.

(b) OICT standards require entities to obtain approval from the Architecture Review Board (ARB) to use non-standard technologies. A proprietary access control management system (i-Entry) on the integrated campus and UNITAD was deployed in 2019 while it was not listed on the approved software standards. UNAMI applied for ARB review and approval in October 2023. Also, UNAMI did not request OICT for an application security risk assessment for i-Entry before deployment, as required by OICT standards.

(c) Purchase orders for i-Entry were raised as exceptions to Financial Rule 105.16 (a) (i) 3 on sole source basis. UNAMI explained that it had sought technical clearance and approval from the OICT support team to proceed with the procurement process. However, a Business Relationship Manager in OICT, who did not have the requisite authority, granted the technical approval whereas the approval should have been accorded by ARB. Consequently, ICT security standards were not complied with. For example, the cryptography standard set by OICT in its technical procedure is AES 256, while the project documents showed AES 128.

(d) While UNAMI stated that it had selected the vendor of i-Entry after finding the vendor to be the most suitable to fulfill the requirements, no options appraisal was documented indicating how such a conclusion was reached.

(e) UNAMI was unable to provide the functional/technical design and also describe the security features embedded in the design, considering that the system captures biometric data. The Digital Blue Helmet team of OICT had informed UNAMI of the risks associated with this system, considering that it uses Port 80 for communication which does not offer encryption services. The underlying mobile handheld access control computing device was not secure and was not hardened according to security best practices. Tests conducted by OIOS indicated that the access control device was directly accessible and open to the internet. It could be used to transfer data in and out, and data could be stored on Google drives. i-Entry used multifactor authentication through Google Authenticator whereas the Secretariat's standard authentication is through Azure. Further, there was no access control policy for i-Entry. For instance, there was a role called "users" with special privileges without clarity as to why the role was needed, and to whom it should be assigned. UNAMI subsequently addressed the risks associated with port 80 by implementing SSL (secure sockets layer) certificates on port 443.

24. There were no pre-defined metrics for monitoring project performance, costs and timelines. There was also no assessment of whether the projects were completed on time and within budget. Failure to follow best practices in project management exposes UNAMI to risks such as insecure applications and deployment of systems that do not meet its requirements.

(3) UNAMI should strengthen its ICT project management by implementing a project management process that adheres to the requirements of OICT's project management methodology and ST/AI/2005/10 on ICT initiatives.

UNAMI accepted recommendation 3 and stated that it will continue to strengthen its ICT project management.

C. ICT operations

ICT service management was adequate

25. Best practices recommend that ICT service management procedures should enhance operational effectiveness by defining, monitoring and measuring ICT services through the development of ICT service catalogs, documenting standard services and deliverables, and Service Level Agreements (SLA) that define the expectations and metrics for performance monitoring.

26. UNAMI conducted quarterly user satisfaction surveys which showed over 85 per cent of users were 'very satisfied' with the ICT services provided. OIOS interviews with various internal and external service recipients confirmed that they were generally satisfied with the ICT services delivered by UNAMI.

27. UNAMI did not have up-to-date SLAs for the ICT support services it provided to UNCT. The SLAs were signed in 2014 and had not been revised since. The rates in the service catalog were not aligned to those in SLAs. The roles, responsibilities and response times were also not defined. Since the financial obligations and terms were not formally updated, there was a risk of disputes. *UNAMI clarified that cost recovery notices are issued to participating entities as provided under the Memorandum of Understanding, 30 days before they take effect. The notification includes a clause that, should an objection not be received by UNAMI by a specified date, the new rates are considered accepted. UNAMI also sends out agreements to each of the entities to sign. However, most entities do not sign the agreements but make payments based on new rates, which implies a constructive agreement. SLAs for external service providers are included in the Statement of Requirement for contract establishment. Contract performance is monitored quarterly through the Contract Performance Review Tool managed by the United Nations Global Service Centre. Service management to UNCT is recorded and monitored in iNeed. In addition, UNAMI has taken the initiative to develop a community application that will include tracking mechanisms for service providers.*

The cost recovery model for ICT services needs to be reviewed

28. In 2022, the Controller issued a policy for service costs and cost recovery. The basic principle underlying this policy is 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, and they must also be directly attributable to users. Further, the services to which service costs 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. Additionally, a policy guide promulgated in 2021 stated that assessed resources should not subsidize non-assessed activities, and vice versa. Service providers should establish efficient and effective cost recovery mechanisms to ensure that costs are assigned to the appropriate funding source in line with approved mandates to avoid cross-subsidization.

29. UNAMI provided ICT services to UNCT entities on a cost-recovery basis, as defined in a service catalog and rate card. Rates were not changed unilaterally but were set in consultation with UNCT. OIOS noted the following:

(a) The best practice for ICT cost recovery is based on the number of users on and/or usage of ICT resources. However, the cost recovery modality for UNAMI ICT services was based on the space occupied by user entities, rather than the usage or number of users of ICT services. This was because other utilities provided by UNAMI were costed on the basis of space occupied. This is not optimal since an entity may have high utilization of ICT resources but occupy lesser physical space, which would result in the entity

paying less as compared to an entity with low ICT utilization but higher space occupancy. It may also result in surpluses or deficits in cost recovery.

(b) There was no clarity between the cost of ICT services provided and their recovery. The majority of FTS' cost recovery was bundled with space management revenue that included non-ICT services. Costs were not attributable to specific and clearly-defined service activities irrespective of their sources of funding, which was contrary to the policy and instructions issued by the Controller. The cost of services (except direct costs such as telephones) provided by UNAMI to UNCT entities using the space occupancy method recorded cost recovery in totality, including ICT and non-ICT services.

(c) There was no clarity as to how the rate cards for ICT services matched the costs recovered from the concerned entities. The "reconciliation" provided by UNAMI (see Figure 1 below) did not provide any explanation or comparison between the cost of ICT services according to the rate cards, and the actual recoveries made from the entities served.

Figure 1: Comparison of 2022 rate card and cost recovery documentation

2022 rate card	
PART I: ICTS RELATED SERVICES	Current Rates
Description	Amount (USD)
(a) Centralized Data Storage	$85.00
(b) Device Enterprise Applications	$310.00
(c) IT Services	$240.00
(d) Loan Satellite Phone Device	Actual Cost
(e) Support Service for Special Applications	$320.00
(f) Video Conference Extra	$685.50
(g) Video Conference	$72.50
(h) Telephone Extension	$25.00
(i) OICT Applications Support	$75.00
(j) Computer Installation / Relocation	$350.00
(k) Telephone Relocation	$50.00
(l) Telephone Installation, Equipment and License	Actual Cost
(m) Mobile Device Installation / Relocation	$62.50
(n) ECM FIL Vehicle Loading	$1,358.00
(o) ECM Vehicle Maintenance	$952.00
(p) High Resolution Satellite Imagery	$2,500.00
(q) Medium Resolution Satellite Imagery	$1,800.00
(r) Low Resolution Satellite Imagery	$300.00
(s) Acquisition of Raster Digital Maps	$100.00
(t) Acquisition of Vector Digital Maps	$300.00

≠

Cost recovery reconciliation provided by UNAMI

The amount of 2022 cost recovery related to FTS (ICTS services)	
	Actual
Security Cost Sharing	75,500.00
KJSO Operational Costs Sharing	80,988.00
Telephone and other direct recoveries	122,524.61
Space Management Related Costs	661,621.74
Total	$940,634.35

30. Therefore, it was not possible to establish whether there was a surplus or deficit in ICT cost recovery. For instance, the World Health Organization and other entities hosted infrastructure equipment on telecom rigs and rooftops of buildings in the integrated compound, but the cost of these services was not visible. Also, it was not clear whether the cost of service delivery and cost recovery included the cost of staff resources. From the service delivery cost plan provided by UNAMI, only 1 FTS post was attributed to service delivery. In OIOS' opinion, the total cost of service delivery should better describe the services provided and the corresponding cost to deliver the services, as required by the policy and instructions issued by the Controller.

(4) UNAMI should reassess the funding and cost recovery model for ICT services provided to the United Nations Country Team by documenting the total cost of delivery of services and adopting cost recovery based on the number of users and/or ICT resource utilization.

UNAMI did not accept recommendation 4 stating that implementation would require additional resources without providing significant benefits. The current procedure, which involves cost recovery based on space utilization, is fundamental to the Mission's shared services model. While implementing a per-user or bandwidth utilization model might appear impractical within this framework, it's crucial to emphasize that the existing process is the agreed-upon practice between UNAMI and UNCT. The Mission firmly believes that this approach serves the best interests of both parties. OIOS reiterates that UNAMI's current practices do not comply with the 2022 policy for service costs and cost recovery as issued by the Controller. The current practices also do not provide any transparency or reconciliation of actual costs and recoveries for ICT services. Recommendation 4 has been closed without implementation, indicating management's acceptance of residual risk.

Need to strengthen change and configuration management

31. Formal change management procedures facilitate a standardized approach to handling all requests for changes to applications, procedures, processes, system service parameters and the underlying platforms. A supporting tool and central repository should be established to log all relevant information on configuration items (i.e., ICT assets and resources) and maintain a baseline of configuration items for every system to serve as a checkpoint to which to return after changes are made.

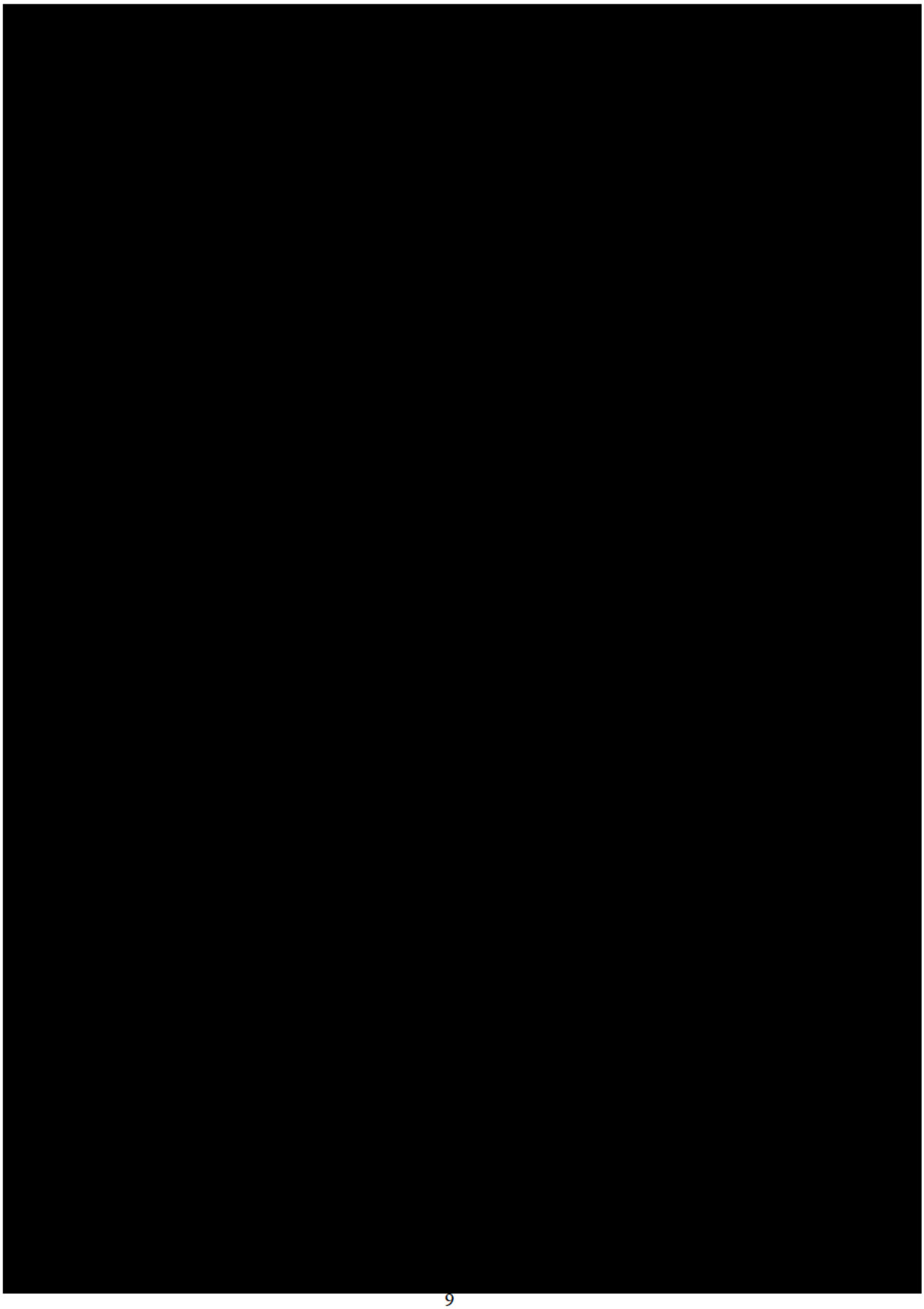
32. UNAMI had a draft change management guideline which was not fully implemented. OIOS' review of 15 scheduled change proposals showed that UNAMI had not established a change review board as specified in the guidelines and had not established mechanisms for change tracking and post-implementation review. Also, configuration changes at the network level were done without following the change management process. Configuration procedures were absent, including a repository database for recording relevant information about configuration items and for maintaining a baseline of the Missions' systems for tracking and controlling changes to installed software and applications.

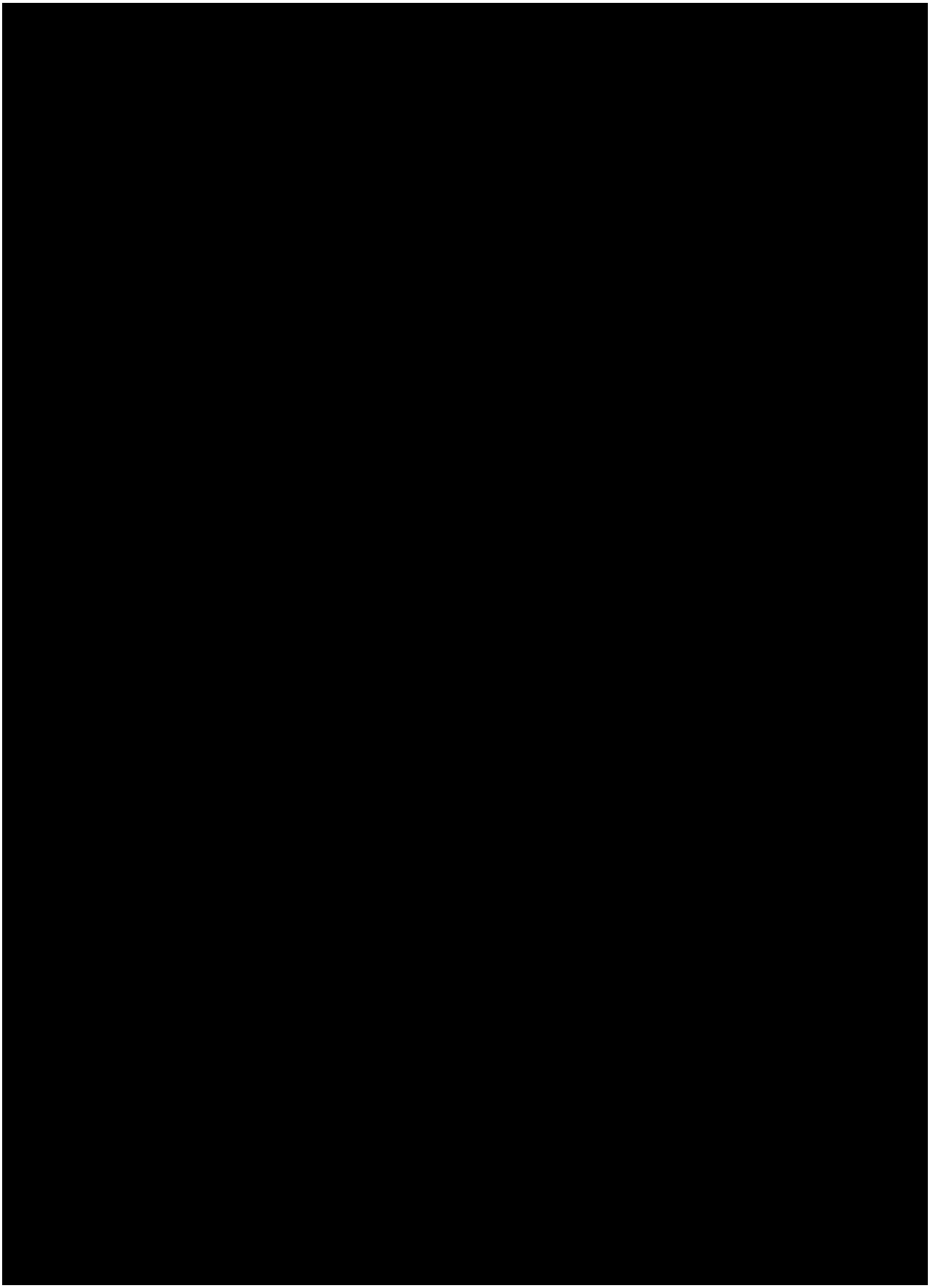
33. The lack of adequate change and configuration management mechanisms could have a significant negative impact on UNAMI's technology infrastructure and operations, because it increases the risk of downtime, security vulnerabilities, unauthorized changes and errors.

(5) UNAMI should strengthen its change and configuration procedures by: (a) establishing a change review board with terms of reference; (b) tracking of change requests; and (c) establishing a configuration management process including a tool for tracking configuration items.

UNAMI accepted recommendation 5 and stated that it will continue to strengthen change and configuration procedures.

[redacted]





E. ICT access management

Need to strengthen user access management

44. OICT's Technical Procedure on Access Control (SEC.02.PROC) emphasizes that effective security practices should prevent unauthorized access to systems and services. Users should only be provided with access to systems that they have been specifically authorized to use, and the allocation and use of privileged access rights should be restricted and controlled. Information owners should review the access privileges of user accounts periodically to determine if access rights are still commensurate with the user's job requirements. Documentation for such reviews should include information about who conducted the review, and what action (if any) was taken by the application owner. Such information should be kept according to the published retention schedule.

45. There was no evidence that FTS had a process for conducting logical access control reviews of all the critical ICT systems. For example, the Manage Engine AD Manager Plus had visibility of users in the Active Directory. However, there was no user reconciliation between systems and the Active Directory. Further, compliance monitoring of access control procedures had not been implemented.

46. The absence of regular reviews of user access accounts and their access rights may result in users having more access rights than required for their jobs, increased attack surface, and a weakened security posture due to stale accounts, privilege creep and compromised credentials.

(8) UNAMI should strengthen its user access controls by implementing regular reviews of user accounts and access rights.

UNAMI accepted recommendation 8.

F. Data governance and management

Need to strengthen data governance and management

47. In April 2020, the Secretary-General promulgated the data strategy for the United Nations to build an ecosystem that unlocks the full potential of data for effective governance by building capabilities in data management and analytics. The enablers for the Secretary-General's data strategy include people and culture, data governance, oversight, partnerships and the technology environment. Effective data governance and management structures are required to ensure success.

48. In a memorandum to all departments, the Chef de Cabinet outlined the action required for implementing the data strategy which included assigning a senior-level owner for the data strategy and a working level contact, ideally with existing data expertise. UNAMI was yet to assign specific roles and responsibilities for implementing the data strategy. OIOS noted the following:

(a) At the time of the audit, UNAMI did not have a Records Management Unit; the staff responsible for record management functions at the time of audit was away on temporary assignment without a backup. Each section/unit handled its own records, but there was no SOP for archiving of records. In 2023, a course on "Record and Information Management" was mandated for all Secretariat staff. At the time of the audit, 80 per cent of UNAMI staff had completed the course.

(b) UNAMI had not established a data inventory in accordance with the requirements of the data strategy to provide visibility over the data assets and mitigate the risks associated with the data assets.

(c) UNAMI had not established retention schedules as required by ST/SGB/2007/5 on record-keeping and the management of United Nations archives. Clarity is also needed about the retention policy of code cables after distribution.

(9) UNAMI should strengthen data governance and management by: (a) assigning centralized archives and records management responsibilities; (b) developing and implementing data retention policies; and (c) fully implementing the Secretary-General's data strategy.

UNAMI accepted recommendation 9 and stated that it will strengthen governance and management of archives and records data.

IV. ACKNOWLEDGEMENT

49. OIOS wishes to express its appreciation to the management and staff of UNAMI for the assistance and cooperation extended to the auditors during this assignment.

Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	UNAMI should strengthen ICT governance by establishing a local ICT committee with formal terms of reference and representation from all relevant stakeholders	Important	O	Receipt of evidence that a local ICT committee has been established.	31 December 2024
2	UNAMI should strengthen its risk management procedures by conducting a risk assessment of its entire ICT and operational technology landscape and integrating the results into its entity-level risk register.	Important	O	Receipt of evidence that risk management procedures have been strengthened by ensuring that the entire ICT and operational technology landscape is covered in the entity-wide risk assessment and integrated into the UNAMI risk register.	31 December 2024
3	UNAMI should strengthen its ICT project management by implementing a project management process that adheres to the requirements of the OICT project management methodology and ST/AI/2005/10 on ICT initiatives.	Important	O	Receipt of evidence of action taken to ensure the implementation of OICT's project management methodology and ST/AI/2005/10.	31 December 2024
4	UNAMI should reassess the funding and cost recovery model for ICT services provided to the United Nations Country Team by documenting the total cost of delivery of services and adopting cost recovery based on the number of users and/or ICT resource utilization.	Important	C	Closed without implementation based on management's acceptance of residual risk.	Not implemented
5	UNAMI should strengthen the change and configuration procedures by: (a) establishing a change review board with terms of reference; (b) tracking of change requests; and (c) establishing a configuration management process including a tool for tracking configuration items.	Important	O	Receipt of evidence of action taken to strengthen change and configuration management procedures.	31 December 2024
[redacted]					

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
[redacted]					
8	UNAMI should strengthen its user access controls by implementing regular reviews of user accounts and access rights.	Important	O	Receipt of evidence that regular reviews of user accounts and access rights have been performed.	31 December 2024
9	UNAMI should strengthen data governance and management by: (a) assigning centralized archives and records management responsibilities; (b) developing and implementing data retention policies; and (c) fully implementing the Secretary-General's data strategy.	Important	O	Receipt of evidence of action taken to strengthen data governance and management by assigning centralized archives and record management responsibilities, developing data retention policies, and implementing the Secretary-General's data strategy.	31 December 2024

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

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNAMI should strengthen ICT governance by establishing a local ICT committee with formal terms of reference and representation from all relevant stakeholders	Important	Yes	O/CMS	31 Dec 2024	UNAMI will continue to strengthen ICT governance by establishing a local ICT committee with formal terms of reference and representation from all relevant stakeholders.
2	UNAMI should strengthen its risk management procedures by conducting a risk assessment of its entire ICT and operational technology landscape and integrating the results into its entity-level risk register.	Important	Yes	O/CoS O/CMS	31 Dec 2024	The UNAMI Mission Support and Chief of Staff Offices will conduct a thorough risk assessment of all relevant areas. The findings will then be systematically integrated into the entity-level risk register to ensure comprehensive tracking and management of identified risks.
3	UNAMI should assess the conflicted roles and responsibilities within the Field Technology section and assign responsibilities to enforce checks and balances and minimize the opportunity for unauthorized activities.	Important	No			UNAMI did not accept this recommendation in response to the detailed audit report dated May 10, 2024 (Ref. CMS-024/011R, para #6 and Rec #3 of Annex 1). The relevant extract is attached.
4	UNAMI should strengthen its ICT project management by implementing a project management process that adheres to the requirements of the OICT project management methodology and ST/AI/2005/10 on ICT initiatives.	Important	Yes	Chief FTS	31 Dec 2024	UNAMI will continue to strengthen its ICT project management.

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

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

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
5	UNAMI should reassess the funding and cost recovery model for ICT services provided to the United Nations Country Team by documenting the total cost of delivery of services and adopting cost recovery based on the number of users and/or ICT resource utilization.	Important	No			UNAMI does not accept this recommendation due to its lack of added value. Implementation would require additional resources without providing significant benefits. For detailed reasoning, please refer to paragraphs 9-14 of our response to the detailed audit report dated May 10, 2024 (Ref. CMS-024/011R). The relevant extract is attached.
[redacted]						
8	UNAMI should strengthen operational resilience and recovery by conducting a	Important	Yes	O/CoS, O/CMS	31 Dec 2024	UNAMI will strengthen operational resilience and recovery by conducting

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the United Nations Assistance Mission for Iraq

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	business impact assessment of critical mission activities to define Recovery Point Objectives and Recovery Time Objectives and to inform the Disaster Recovery Plan.					a business impact assessment of critical mission activities to define Recovery Point Objectives and Recovery Time Objectives and to inform the Disaster Recovery Plan.
9	UNAMI should strengthen its user access controls by implementing regular reviews of user accounts and access rights.	Important	Yes	Chief FTS	31 Dec 2024	
10	UNAMI should strengthen data governance and management by: (a) assigning centralized archives and records management responsibilities; (b) developing and implementing data retention policies; and (c) fully implementing the Secretary-General's data strategy.	Important	Yes	Chief FTS	31 Dec 2024	UNAMI will strengthen the governance and management of archives and records data.