



INTERNAL AUDIT DIVISION

REPORT 2023/088

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

**There is need to strengthen network
infrastructure and access management,
besides security monitoring and vulnerability
assessments**

**22 December 2023
Assignment No. AT2023-800-01**

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of network access management in the Office of Investment Management (OIM) of the United Nations Joint Staff Pension Fund. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over network access management in OIM. The audit covered the period from January 2020 to September 2023 and included a review of: (a) governance; (b) network operations; (c) infrastructure management; (d) access management; (e) resilience and security monitoring; (f) vulnerability assessment; and (g) third-party service management.

The audit indicated the need for OIM to strengthen network infrastructure and access management, besides security monitoring and vulnerability assessments.

OIOS made 11 recommendations. To address the issues identified in the audit, OIM needed to:

- Document the critical path for completion of the infrastructure migration project, and the lessons learned from implementing this project to prevent recurrence in future;
- Deploy a configuration and change management tool for network operations and document procedures to manage and track emergency changes to the network;
- Explore the feasibility of using automated tools for network topology mapping; validate the network infrastructure periodically to identify inconsistencies or discrepancies; complete its network documentation including the Internet Protocol address allocation table and physical, logical and security diagrams; and establish a mechanism for preserving documentation required to be passed on to the new service provider;
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED];
- Assess the cost-benefit and risks associated with the co-existence of multiple domains vis-à-vis consolidation of these domains;
- Document a decommissioning plan with timelines for servers and the data centre maintained by the previous service provider following the migration of infrastructure services; finalize a plan for further utilization of the data centre managed by the previous service provider; and clean up the firewall rules in the servers being decommissioned, and ensure the deletion or destruction of the related sensitive data;
- Define the process for risk acceptance and document the risk owner and risk acceptance authority for its risk treatment plans;
- Develop a comprehensive plan for analysis and follow-up of identified network vulnerabilities; conduct an assessment of vulnerability scanning tools for its network; implement a solution to periodically scan iOS devices connected to its network; and establish a mechanism to ensure

compliance with training requirements for staff who responded negatively to the phishing campaign;
and

- Review and strengthen the provisions of the contract with the infrastructure service provider and clarify the responsibility of the provider regarding policy-setting activities; assess the conflicting roles assigned to the infrastructure service provider and ensure there is a clear delineation of roles and responsibilities; and establish service level agreements with defined key performance indicators for the infrastructure service provider.

OIM accepted the recommendations and has agreed to initiate action to implement them. Actions required to close the recommendations are indicated in Annex I.

CONTENTS

I. BACKGROUND	1
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	1-2
III. AUDIT RESULTS	2-10
A. Governance	2
B. Network operations	2-3
C. Infrastructure management	3-4
D. Access management	4-5
E. Resilience and security monitoring	6-8
F. Vulnerability assessments	8-9
G. Third-party service management	9-10
IV. ACKNOWLEDGEMENT	10
ANNEX I	Status of audit recommendations
APPENDIX I	Management response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of network access management in the Office of Investment Management (OIM) of the United Nations Joint Staff Pension Fund (UNJSPF).
2. UNJSPF was established in 1948 by the General Assembly to provide retirement benefits and social security protection for the staff of the United Nations and other organizations admitted to membership in the Fund. The Secretary-General is responsible for the investment of the assets of the UNJSPF. The Secretary-General delegated this responsibility to the Representative of the Secretary-General for the investment of the assets of UNJSPF (RSG). The RSG is assisted in this function by OIM which manages an investment portfolio worth \$84.4 billion as of 30 June 2023.
3. The Operations and Information Systems Section of OIM is responsible for providing, maintaining and securing information and communications technology (ICT) systems and network services. OIM had outsourced network infrastructure, network management and security to a United Nations agency and later to another third-party vendor (hereafter referred to as “infrastructure service provider”). At the time of the audit, migration of infrastructure services to the third-party vendor was ongoing.
4. OIM had also contracted a vendor specialized in ICT security to provide managed security services known as Security Operations Centre (SOC) which included threat and vulnerability identification, recommending remediation, security monitoring and alerts, intrusion protection, cyber surveillance, incident analysis, incident response and coordination. OIM had also implemented a Security Information and Event Management (SIEM) system with the support of the SOC service provider.
5. The majority of applications currently used by OIM were hosted in one or more of the following data centres and a server room: (i) North America data centre in New Jersey managed by the United Nations agency; (ii) data centre in Andover, Massachusetts managed by the infrastructure service provider; and (iii) the Dag Hammarskjöld Plaza server room managed by OIM.
6. The 2023 budget for ICT infrastructure and security in OIM is approximately \$1.7 million and \$0.6 million, respectively.
7. Comments provided by OIM 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 over network access management in OIM.
9. This audit was included in the 2022 risk-based work plan of OIOS due to the high risks associated with network access management.
10. OIOS conducted this audit from February to September 2023. The audit covered the period from January 2020 to September 2023. Based on an activity-level risk assessment, the audit covered risk areas in network access management which included: (a) governance; (b) network operations; (c) infrastructure

management; (d) access management; (e) resilience and security monitoring; (f) vulnerability assessment; and (g) third-party service management.

11. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data; (d) ICT security tests; (e) physical observation; and (e) walkthroughs.

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

III. AUDIT RESULTS

A. Governance

Delay in infrastructure migration project needs to be addressed

13. ICT project requirements define the criteria, necessary conditions and functions that must be met for a project to be considered complete. They also provide the basis for deliverables that form part of the planning process and the steps that must be taken to achieve them in a timely manner.

14. OIM initiated 'Infrastructure as a Service' provider project to migrate the on-premises ICT infrastructure to cloud-based provider. The project, which was initiated in March 2022 and projected to go live in January 2023, was still ongoing as of October 2023. OIM attributed the delay to the establishment of a leased line for site-to-site connectivity as well as a dedicated circuit with a financial services vendor which had not been earlier anticipated during the requirements and planning phase. Additional reasons for the delay were the long lead times of telecommunication vendors, and delay in the procurement process. However, the project risk register indicated that the reasons for delay were inadequate definition of project deliverables, requirements for information security and business continuity requirements, and scope creep. The slippage in the delivery schedules required project personnel to constantly keep revising their plans and allocation of resources.

(1) OIM should document: (a) the critical path for completion of the infrastructure migration project; and (b) the lessons learned from implementing this project to prevent recurrence in future.

OIM accepted recommendation 1.

B. Network operations

Need to strengthen configuration and change management

15. Configuration management is required for maintaining network devices and other components in an optimal state, to keep track of system changes and interrelated dependencies, and to prevent undocumented changes. A Configuration Management Database (CMDB) enables organizations to maintain a comprehensive and up-to-date repository of all network-related information from hardware and

software configurations to interdependencies among configuration items¹, services and their providers, as well as history of changes to each item and criticality of each configuration item.

16. An automated configuration management process facilitates the orderly management of system information and system changes. OIM had not deployed a CMDB tool but relied on Excel to manage configuration items, updates and dependencies. Automation of this process would enable OIM to effectively capture the interdependencies among service providers and services being provided. It would also enhance OIM's ability to use Dynamic Host Configuration Protocol (DHCP) logging² for automatic identification of all assets and resources connected to the network, including unauthorized assets for removal or remediation.

17. OIM used Excel for managing changes. Automation of change management would facilitate identification, logging, assessing, approving and deploying ICT-related changes, including emergency changes made to the network.

(2) OIM should: (a) deploy a configuration and change management tool for network operations; and (b) document procedures to manage and track emergency changes to the network.

OIM accepted recommendation 2 and stated that it is going live with the infrastructure service provider enabled deployment of configuration and change management tools for network operations. Also, Phase 2 of the information technology service management tool is expected to implement OIM-initiated change management, which also covers emergency changes.

C. Infrastructure management

Need to strengthen network infrastructure management

18. ICT best practices require network infrastructure management to implement and actively manage network devices to safeguard network services and access points. OIOS noted the following:

(a) Network security necessitates regular re-evaluation of architecture diagrams including network topology maps that provide a detailed blueprint of an organization's network infrastructure including architecture, configurations, interconnections, and layout for the correct placement of preventive and detective controls. OIM did not use an automated tool for network mapping that provides real-time detection of changes in the network. The use of automated tools for network mapping would minimize the potential risks of security breaches, unauthorized modification or exploitation of network weaknesses. OIM used a charting tool which was manually updated. This increased the risk of delays and errors, and the tool may not reflect the actual network architecture at a given point of time.

(b) While a well-documented diagram is crucial for understanding the network's architecture,

¹ A configuration item is any service component, infrastructure element or other item that needs to be managed to ensure the successful delivery of services, such as a router, a server, an application, a virtual machine, a container, or even a logical construct such as a portfolio.

² DHCP logging is a feature that dynamically updates assets by mapping internet protocol (IP) addresses to the unique Media Access Control addresses of the network resources and generates logs. DHCP logs should be reviewed to look for any anomalies, unauthorized devices, or simply devices missing from the inventory that need to be added.

ensuring that it accurately reflects the actual operational state is equally vital. Since networks are dynamic in nature, changes arising from device addition, configuration and maintenance can occur frequently. Regularly validating the operational status of the network against the diagram helps identify any inconsistencies or discrepancies. The data centre managed by the infrastructure service provider had only two exchange management console servers on the rack, without any firewalls attached to the servers. This configuration was a concern because without a firewall, exchange management console servers are potentially vulnerable to attacks, unauthorized access, data theft and network disruption. The existing network topology had not been updated to reflect the new architecture following the migration of the exchange servers. OIM stated that its infrastructure uses software-defined networking³, and is fully virtualized with no physical hardware besides the hypervisor that is owned by the infrastructure service provider. However, since the network topology had not been updated, this aspect could not be confirmed.

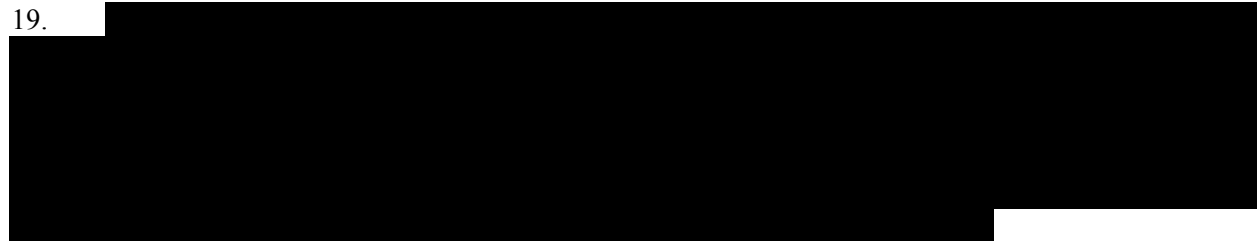
(c) Detailed and accurate documentation in the form of physical and logical network diagrams, security diagrams, configuration of devices and the Internet Protocol (IP) address allocation table should be maintained to preserve business continuity and optimally manage network operations, considering the transition of operations from one service provider to another. OIM had not defined a mechanism for preserving the information required to be passed on to the new service provider. Lack of documentation of network components and maintenance requirements may lead to an inability to identify problems and vulnerabilities in the network and minimize the impact of unavailability.

(3) OIM should: (a) explore the feasibility of using automated tools for network topology mapping; (b) validate the network infrastructure periodically to identify inconsistencies or discrepancies; (c) complete its network documentation including the Internet Protocol address allocation table and physical, logical and security diagrams; and (d) establish a mechanism for preserving documentation required to be passed on to the new service provider.

OIM accepted recommendation 3 and stated that it will explore the feasibility of using an automated tool for network topology mapping. OIM also stated that it conducts quarterly firewall review and bi-weekly change management review, quarterly configuration management database update review, and periodic assessment of network infrastructure.

D. Access management

Need to strengthen network access management

19. 

20. 

³ Software-defined networking is a solution that centralizes and simplifies network management through programmable, software-based controllers allowing dynamic, adaptable control over traffic without reliance on traditional hardware-based solutions.

(4) [Redacted]
[Redacted]

[Redacted]

21. [Redacted]

22. [Redacted]

(5) [Redacted]
[Redacted]

[Redacted]

23. [Redacted]

24. [Redacted]

(6) [Redacted]
[Redacted]

E. Resilience and security monitoring

[Redacted]

25.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(7) [Redacted]

Need to consolidate the several active domains

26. Best practices in the financial services industry require data security and privacy safeguards for enforcing data protection policies that restrict sensitive data from being exfiltrated. Data loss prevention

systems inspect all network traffic to detect or block confidential data from leaving an organization's network.

27. OIM had implemented a data loss prevention solution (O365 E5 licence) only for the domain 'unoim.org' accounts, whereas other domains such as 'un.org', 'unimd.org', or 'unims.org' remained as it is. To protect the Organization, the data loss prevention solution needs to be consistently implemented for all existing domains to minimize data loss.

28. Also, OIM had several active domains due to its evolution from previously being a Service to a Division ('unims.org', 'unimd.org') and later an Office ('unoim.org'), in addition to being part of the United Nations ('un.org'). These multiple domains continued to coexist and bring complexities in their management. There is need for a risk assessment and cost-benefit analysis to determine whether these domains should continue to be maintained.

(8) OIM should assess the cost-benefit and risks associated with the co-existence of multiple domains vis-à-vis consolidation of these domains.

OIM accepted recommendation 8 and stated that its ICT Steering Committee approved an initiative to consolidate multiple domains to single domain unoim.org. To that effect, OIM is already in the process of decommissioning unims.org and un.org. Based on the actions taken by OIM, recommendation 8 has been closed.

Need for a plan to decommission servers and data centre managed by the previous service provider

29. A decommissioning plan serves as a roadmap for systematically retiring the existing infrastructure and outlines the sequence of actions, responsible parties and timelines for server decommissioning, thereby ensuring that no critical data or assets are left behind. Although OIM documented a procedure for decommissioning the servers maintained by the outgoing service provider, it did not indicate timelines for their decommissioning. Delay in decommissioning the servers poses the following risks:

(a) Unless firewall rules are periodically cleaned up, any new system using the same IP address would inherit the old firewall rules and may allow security vulnerabilities into the network. Also, sensitive data stored on servers need to be considered for deletion or destruction to remove trails and avoid a potential attack. The service decommissioning procedure did not address the need to delete the firewall rules associated with the decommissioned servers and the data therein.

(b) The status of utilization/decommissioning of the data centre managed by the previous service provider to host network resources needs to be finalized. Due consideration should be given to the minimum base cost of maintaining the data centre by OIM after the migration of infrastructure services to the new service provider. OIM stated that the end state of the data centre managed by the previous service provider would be to decommission it. However, it was also considering a new service delivery agreement for better control and monitoring of the costs.

30. Timely decommissioning of servers and data centres, and clean-up of sensitive data stored in these resources are essential to strengthen OIM's information security.

(9) OIM should: (a) document a decommissioning plan with timelines for servers and the data centre maintained by the previous service provider following the migration of infrastructure services; (b) finalize a plan for further utilization of the data centre managed by the previous service provider; and (c) clean up the firewall rules in the servers being decommissioned, and ensure the deletion or destruction of the related sensitive data.

OIM accepted recommendation 9 and stated that the decommissioning plan was fully executed as of November 2023. All core infrastructure dependencies with the previous service provider have been removed. All services are fully migrated and managed by the new service provider.

F. Vulnerability assessments

ICT risk acceptance procedures need to be formalized

31. The ICT operational risk management process includes a risk response phase which requires risk owners and accountable managers to review the identified risk ratings and decide to accept, reduce or transfer the risks through a risk treatment plan. OIM stated that the Information Security group reviews the vulnerabilities following scans by the SOC and decides to mitigate or accept the risk. However, the process for risk acceptance was not well defined and needs to be documented with clearly defined risk acceptance authority. For example, the OIM ICT risk treatment and response plan defined the treatment strategy as risk acceptance, risk monitoring and control monitoring, but it does not mention who is responsible for risk acceptance. The lack of clarity on risk acceptance and absence of documentation on such decisions need to be addressed.

(10) OIM should define the process for risk acceptance and document the risk owner and risk acceptance authority for its risk treatment plans.

OIM accepted recommendation 10 and stated that its Enterprise Risk Committee is the governing body to authorize the acceptance of risks and treatment plans based on OIM's risk appetite.

Need for a well-coordinated vulnerability assessment mechanism

32. Best practice recommends that organizations should conduct continuous vulnerability assessments of their network infrastructure, applications and systems to proactively discover and remediate network security vulnerabilities that may expose the organization to data and cybersecurity related breaches.

33. The SOC service provider performed monthly vulnerability scans of OIM's infrastructure. OIOS noted the following:

(a) OIM relied on the threat intelligence information provided by the SOC service provider. Excel spreadsheets were used to record the identified vulnerabilities. However, there was no evidence that the vulnerabilities were prioritized for remediation or follow-up. There was also no evidence of correlation of vulnerabilities identified in various scans across different timeframes that were analyzed for identification of similarities or differences to provide input into incident management and threat-hunting.

(b) There is a need to validate that all OIM subnets are included in the monthly vulnerability scans conducted after the migration of infrastructure to the new service provider, thereby ensuring that potential vulnerabilities that may arise during or after migration are timely mitigated. Also, periodic vulnerability scan of the migrated infrastructure is required. OIOS could not validate that all OIM subnets were included in the monthly vulnerability scans because the migration was ongoing.

34. A credentialed scan (i.e., vulnerability scans performed with usernames and passwords for network assets) was not performed in OIM. Without a credentialed scan, the full extent of security vulnerabilities could not be identified, leading to unpatched network security vulnerabilities. OIM stated that the

Information Security unit is in the process of developing a vulnerability tool and agents for all endpoints for optimal configuration, as recommended by the vulnerability tool provider.

35. OIM was currently not able to scan Apple (iOS) devices connected to the network, which is a cause for concern. OIM explained that it was currently conducting a due diligence exercise for a solution.

36. Data pertaining to OIM's targeted phishing campaign conducted in December 2022 indicated that out of 162 user accounts, 15 (or 9 per cent) were compromised. However, 3 (out of 15) staff who had supplied their credentials during the simulated phishing exercise did not undertake the required training. OIM had not taken further action to ensure that these staff completed the training.

37. Inadequate vulnerability management processes may result in potential attacks on OIM's information assets.

(11) OIM should: (a) develop a comprehensive plan for analysis and follow-up of identified network vulnerabilities; (b) conduct an assessment of vulnerability scanning tools for its network; (c) implement a solution to periodically scan iOS devices connected to its network; and (d) establish a mechanism to ensure compliance with training requirements for staff who responded negatively to the phishing campaign.

OIM accepted recommendation 11 and stated that it has a plan in place based on the approved vulnerability assessment management policies. Also, OIM will initiate a business case to its ICT Steering Committee for approval to remediate the risk relating to iOS devices. Further, OIM will update the policy to ensure that training is mandatory for privileged users who click on a phishing campaign link. Upon approval of the policy, OIM will enforce the remedial training plan accordingly.

G. Third-party service management

Terms and conditions of the contract with the infrastructure service provider need to be improved

38. Best practices recommend that third-party services should be monitored, and any deviation from the agreed-upon standards should be noted. Further, organizations should not contract out policy-setting activities or decisions. This is to prevent the service provider from having complete control over all activities they render and decisions they make for the services they provide.

39. OIOS reviewed the terms and conditions of the contract with the infrastructure service provider and noted that there was no clarity in terms of potential conflicts in the application of policies regarding firewall management, incident management, emergency changes and retention policy. For example, the contract stated that '..... The infrastructure service provider reserves the right to review any OIM-requested firewall changes that allow unnecessary security vulnerabilities...', thereby giving the service provider the ability to question or not act on an OIM policy decision. OIM agreed to update the wording of the contract at the next contract review to safeguard its interests and promote a collaborative and secure working partnership.

40. There were role conflicts in the services provided by the infrastructure services provider. For instance, it performs network operation activities, ensures compliance with policies and monitors its own performance-related activities, which are incompatible functions. The service provider could potentially ignore negative outcomes which may impact OIM.

41. Annex B of the Service Schedule of the Contract between OIM and the infrastructure service provider did not include the key performance indicators (KPIs) expected of the service provider. OIM stated that after the first year of service, it will review the arrangement to get a better understanding of the services implemented and then determine, based on priorities, the relevant KPIs.

(12) OIM should: (a) review and strengthen the provisions of the contract with the infrastructure service provider and clarify the responsibility of the provider regarding policy-setting activities; (b) assess the conflicting roles assigned to the infrastructure service provider and ensure there is a clear delineation of roles and responsibilities; and (c) establish service level agreements with defined key performance indicators for the infrastructure service provider.

OIM accepted recommendation 12 and stated that contract terms will be enhanced at the next renewal cycle. However, more detailed terms can be enhanced during the review of the service guides which are being developed whereby the detailed roles and responsibilities will be streamlined while incorporating robust service level agreements and KPIs to meet business requirements.

IV. ACKNOWLEDGEMENT

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

Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical ⁴ / Important ⁵	C/ O ⁶	Actions needed to close recommendation	Implementation date ⁷
1	OIM should document: (a) the critical path for completion of the infrastructure migration project; and (b) the lessons learned from implementing this project to prevent recurrence in future.	Important	O	Receipt of evidence that OIM has documented: (a) the critical path for completion of the infrastructure migration project; and (b) the lessons learned from implementing this project to prevent recurrence in future.	31 March 2024
2	OIM should: (a) deploy a configuration and change management tool for network operations; and (b) document procedures to manage and track emergency changes to the network.	Important	O	Receipt of evidence that OIM has: (a) deployed a configuration and change management tool for network operations; and (b) documented procedures to manage and track emergency changes to the network.	30 September 2024
3	OIM should: (a) explore the feasibility of using automated tools for network topology mapping; (b) validate the network infrastructure periodically to identify inconsistencies or discrepancies; (c) complete its network documentation including the Internet Protocol address allocation table and physical, logical and security diagrams; and (d) establish a mechanism for preserving documentation required to be passed on to the new service provider.	Important	O	Receipt of evidence that OIM has: (a) explored the feasibility of using automated tools for network topology mapping; (b) validated the network infrastructure periodically to identify inconsistencies or discrepancies; (c) completed its network documentation including the IP address allocation table and physical, logical and security diagrams; and (d) established a mechanism for preserving documentation required to be passed on to the new service provider.	31 March 2024
4		Important	O		30 September 2024

⁴ 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.

⁵ 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.

⁶ Please note the value C denotes closed recommendations whereas O refers to open recommendations.

⁷ Date provided by OIM in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

5	[REDACTED]	Important	O	[REDACTED]	30 September 2024
6	[REDACTED]	Important	O	[REDACTED]	30 June 2024
7	[REDACTED]	Important	O	[REDACTED]	31 March 2024
8	OIM should assess the cost-benefit and risks associated with the co-existence of multiple domains vis-à-vis consolidation of these domains.	Important	C	Action completed.	Implemented
9	OIM should: (a) document a decommissioning plan with timelines for servers and the data centre maintained by the previous service provider following the migration of infrastructure services; (b) finalize a plan for further utilization of the data centre managed by the previous service provider; and (c) clean up the firewall rules in the servers being decommissioned, and ensure the deletion or destruction of the related sensitive data.	Important	O	Receipt of evidence that OIM has: (a) documented a decommissioning plan with timelines for servers and the data centre maintained by the previous service provider following the migration of infrastructure services; (b) finalized a plan for further utilization of the data centre managed by the previous service provider; and (c) cleaned up the firewall rules in the servers being decommissioned, and ensured the deletion or destruction of the related sensitive data.	31 March 2024
10	OIM should define the process for risk acceptance and document the risk owner and risk acceptance authority for its risk treatment plans.	Important	O	Receipt of evidence that OIM has defined the process for risk acceptance and documented the risk owner and risk acceptance authority for its risk treatment plans.	31 March 2024

STATUS OF AUDIT RECOMMENDATIONS

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

11	OIM should: (a) develop a comprehensive plan for analysis and follow-up of identified network vulnerabilities; (b) conduct an assessment of vulnerability scanning tools for its network; (c) implement a solution to periodically scan iOS devices connected to its network; and (d) establish a mechanism to ensure compliance with training requirements for staff who responded negatively to the phishing campaign.	Important	O	Receipt of evidence that OIM has: (a) developed a comprehensive plan for analysis and follow-up of identified network vulnerabilities; (b) conducted an assessment of vulnerability scanning tools for its network; (c) implemented a solution to periodically scan iOS devices connected to its network; and (d) established a mechanism to ensure compliance with training requirements for staff who responded negatively to the phishing campaign.	31 March 2024
12	OIM should: (a) review and strengthen the provisions of the contract with the infrastructure service provider and clarify the responsibility of the provider regarding policy-setting activities; (b) assess the conflicting roles assigned to the infrastructure service provider and ensure there is a clear delineation of roles and responsibilities; and (c) establish service level agreements with defined key performance indicators for the infrastructure service provider.	Important	O	Receipt of evidence that OIM has: (a) reviewed and strengthened the provisions of the contract with the infrastructure service provider and clarified the responsibility of the provider regarding policy-setting activities; (b) assessed the conflicting roles assigned to the infrastructure service provider and ensured there is a clear delineation of roles and responsibilities; and (c) established service level agreements with defined key performance indicators for the infrastructure service provider.	31 March 2025

APPENDIX I

Management Response



To: Fatoumata Ndiaye
Under Secretary General
Internal Oversight Services

DATE: December 19, 2023

Reference: OIOS-2023-02170

-and-

Byung-Kun Min, Director
Internal Audit Division, OIOS

FROM: Pedro Guazo
Representative of the Secretary-General
for the investment of UNJSPF assets


[Pedro Guazo \(Dec 19, 2023 12:44 EST\)](#)


-and-

José Antonio Nunez Poblete
Chief Risk and Compliance Officer
Office of Investment Management



-and-

Bill Wilkinson
Chief Operating Officer
Office of Investment Management


[William J Wilkinson \(Dec 21, 2023 11:54 EST\)](#)

SUBJECT: Draft report on an audit of Network Access Management in the Office of Investment Management of the United Nations Joint Staff Pension Fund (Assignment No. AT2022-801-01)

1. OIM acknowledges receipt of the draft report of an audit of Network Access Management in the Office of Investment Management of the United Nations Joint Staff Pension Fund (Assignment No. AT2022-801-01).
2. OIM would like to take this opportunity to thank the Office of Internal Oversight Services and staff for their comprehensive effort including the on-going collaboration during the thorough review and analysis, and the detailed findings, observations and recommendations.
3. OIM has attached the completed form provided (Appendix I) to the recommendations related to OIM with additional comments for your kind consideration prior to the final publication.

c.c. Mr. Rajiv Prabhakar, OIM
Ms. Maria Tsimboukis, OIM
Mr. Byung-Kun Min, OIOS
Mr. David Nyskohus, OIOS
Mr. Jeffrey Lin, OIOS

Management Response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

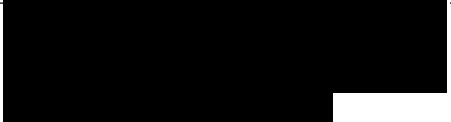
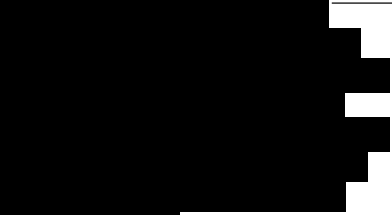

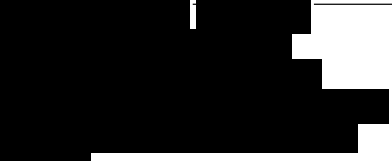
Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OIM should document: (a) the critical path for completion of the infrastructure migration project; and (b) the lessons learned from implementing this project to prevent recurrence in future.	Important	Yes	ICT Infrastructure Services Manager	March 31, 2024	Change closure document for CAB meeting in January 2024, will be provided along with any other updated documentation need to close this recommendation.
2	OIM should: (a) deploy a configuration and change management tool for network operations; and (b) document procedures to manage and track emergency changes to the network.	Important	Yes	Chief of IT	a) Q1 2024 b) Q3 2024	(a) Going live with Navisite enabled deployment of configuration and change management tool for network operations. This documented process within ServiceNow will be provided as evidence in Q1 2024 (b) Phase 2 of ServiceNow is expected to implement OIM initiated change managed which also covers emergency changes. Expected timeline is Q3, 2024
3	OIM should: (a) explore the feasibility of using automated tools for network topology mapping; (b) validate the network infrastructure periodically to identify inconsistencies or discrepancies; (c) complete its network documentation	Important	Yes	ICT Infrastructure Services Manager	Q1 2024	a) OIM will explore the feasibility of using an automated tool for network topology mapping. Since OIM does not have large network infrastructure the

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.

Management Response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	including the Internet Protocol address allocation table and physical, logical and security diagrams; and (d) establish a mechanism for preserving documentation required to be passed on to the new service provider.					cost/benefit analysis will help OIM determine the right solution. b) OIM conducts quarterly firewall review and bi-weekly change management review, quarterly CMDB update review and periodic assessment of network infrastructure. All updated evidence will be provided to OIOS in Q1 2024 c) All updated evidence will be provided to OIOS in Q1 2024 d) All updated evidence will be provided to OIOS in Q1 2024
4		Important	Yes	Chief of IT	Q3 2024	
5		Important	Yes	Chief Information Security Officer	Q3 2024	

Management Response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical/ Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
6	[REDACTED]	Important	Yes	Chief Information Security Officer	Q2 2024	[REDACTED]
7	[REDACTED]	Important	Yes	Chief of IT	Q1 2024	[REDACTED]
8	OIM should assess the cost-benefit and risks associated with the co-existence of multiple domains vis-à-vis consolidation of these domains.	Important	Yes	Chief of IT	Q3 2024	OIM ICT Steering Committee approved an initiative to consolidate multiple domains to single domain UNOIM.ORG. To that effect, OIM is already in the process of decommissioning of UNIMS.ORG and UN.ORG.

Management Response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical/ Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
9	OIM should: (a) document a decommissioning plan with timelines for servers and the data centre maintained by the previous service provider following the migration of infrastructure services; (b) finalize a plan for further utilization of the data centre managed by the previous service provider; and (c) clean up the firewall rules in the servers being decommissioned, and ensure the deletion or destruction of the related sensitive data.	Important	Yes	ICT Infrastructure Services Manager	Q1 2024	<ul style="list-style-type: none"> a) The decommissioning plan was fully executed as of Nov 2023. Documentation will be shared with OIOS. b) All core infrastructure dependency with the previous service provider have been removed. All services are fully migrated and managed by the new service provider. Updated evidence will be provided in Q1 2024. c) Clean up of firewall rules and server decommissioning policies are already provided to OIOS. Any physical equipment that belongs to Bloomberg has been shipped and updated evidence will be provided in Q1 2024.
10	OIM should define the process for risk acceptance and document the risk owner and risk acceptance authority for its risk treatment plans.	Important	Yes	Chief Risk & Compliance Officer, Chief of IT	Q1 2024	OIM Enterprise Risk Committee is the governing body to authorize the acceptance of the risks and the treatment plans based on OIM's risk appetite. Updated evidence will be provided in Q1 2024.
11	OIM should: (a) develop a comprehensive plan for analysis and follow-up of identified network vulnerabilities; (b) conduct an assessment of vulnerability scanning tools for its network; (c)	Important	Yes	Chief Information Security Officer	<ul style="list-style-type: none"> (a) Q1 2024 (b) Q1 2024 (c) Q4 2024 (d) Q1 2024 	<ul style="list-style-type: none"> a) OIM has a plan in place based on the approved vulnerabilities assessment management policies.

Management Response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical/ Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	implement a solution to periodically scan iOS devices connected to its network; and (d) establish a mechanism to ensure compliance with training requirements for staff who responded negatively to the phishing campaign.					<p>Updated evidence will be provided in Q1 2024.</p> <p>b) OIM does conduct monthly vulnerability assessment and bi-weekly meeting with the stakeholders to remediate the vulnerabilities. Updated evidence will be provided in Q1 2024.</p> <p>c) Infosec has highlighted this as a risk to OIM. Infosec will initiate a business case to OIM ICT Steering Committee for approval to remediate this risk.</p> <p>d) OIM will update the policy to ensure the training is mandatory for the privileged users who click on a phishing campaign link. Upon approval of the policy, we will enforce remedial training plan accordingly.</p>
12	OIM should: (a) review and strengthen the provisions of the contract with the infrastructure service provider and clarify the responsibility of the provider regarding policy-setting activities; (b) assess the conflicting roles assigned to the infrastructure service provider and ensure there is a clear delineation of roles and responsibilities; and (c) establish service	Important	Yes	Chief of IT	(a) Q1 2025 (b) & (c) Q2 2024	<p>(a) Contract terms will be enhanced at next renewal cycle. However, more detailed terms can be enhanced during the review of the service guides.</p> <p>(b)&(c) Service Guides are being developed where the detailed roles and responsibilities will be</p>

Management Response

Audit of network access management in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	level agreements with defined key performance indicators for the infrastructure service provider.					streamlined while incorporating robust SLAs and KPIs to meet business requirements.