INTERNAL AUDIT DIVISION

REPORT 2019/027

Audit of information and communications technology services provided by a United Nations agency to the Office of Investment Management of the United Nations Joint Staff Pension Fund

Controls over the management of services needed to be strengthened

26 April 2019
Assignment No. AT2017/801/01

Audit of information and communications technology services provided by a United Nations agency to 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 information and communications technology (ICT) services provided by a United Nations agency (hereafter referred to as “Agency”) to 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 the management of ICT services provided by the Agency to OIM. The audit covered the period from January 2015 to January 2019 and focused on risk areas relating to the provision of ICT services including: (a) strategy, budgeting and acquisition planning; (b) service and project management; and (c) ICT security.

The audit showed that controls over the management of services provided by the Agency needed to be strengthened. To address issues identified in the audit, OIM needed to:

- Present the updated business case and transition strategy to the ICT Steering Committee for review and approval to ensure that the costs and benefits are desirable, viable and in the best interest of OIM; and update its transition strategy in alignment with the completed business case.
- Review its actual usage of the services and use it as the basis to determine future service requirements and the related budgets.
- Periodically perform a verification of its physical and virtual assets hosted and managed by service providers; decommission and dispose of idle equipment; update the configuration management database to ensure correct billing; and improve the due-diligence process during preparation of contractual agreements by conducting a holistic review of existing ICT infrastructure and agreements.
- Ensure that project agreements describe the projects in sufficient detail and clearly link deliverables to project costs; document the project benefit realization plans; and ensure that closure reports are documented at the end of each project.
- Initiate periodic service monitoring and review meetings to communicate issues, delays, status of services/projects and status of accounts, invoices and credits; transfer recurring professional services to one-time services with clear deliverables and key performance indicators.
- Request the Agency to provide detailed breakdown for the credit notes of 2016-2017 and 2018 for each service; reconcile the advance payments against the unused services and recover the net overpayments; request quarterly credit notes rather than biennial; and strengthen the invoice certification process to ensure that payments are not approved for unused services.
- Communicate its change management requirements to the Agency to ensure that it is informed about the changes before their implementation.
- Periodically monitor the access logs of the file server to ensure that confidential information is not accessed by unauthorized parties; ascertain from the Agency the reasons for its delayed response to the ICT security incident of July 2018; implement mitigating controls in coordination with the Agency for the vulnerabilities communicated to it after the ethical hacking exercise; and communicate to the Agency the need to ensure redundancy of power supply to OIM equipment.

OIM accepted the recommendations and has initiated action to implement them.

CONTENTS

Audit of information and communications technology services provided by a United Nations agency to 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 information and communications technology (ICT) services provided by a United Nations agency (hereafter referred to as "the Agency") to the Office of Investment Management (OIM) of the United Nations Joint Staff Pension Fund (UNJSPF).

2. UNJSPF comprises of OIM which is responsible for investment of the Fund's assets, and the Fund Secretariat which is responsible for pension plan administration. The management of the Fund's investments is the fiduciary responsibility of the Secretary-General of the United Nations and this responsibility is delegated to the Representative of the Secretary-General (RSG), who heads OIM.

3. The Agency, which was established by a Memorandum of Understanding (MOU) between the United Nations, the United Nations Development Programme, and the World Health Organization, operates as a self-funding, not-for-profit inter-organization facility. According to its mandate, the Agency "provide[s] information technology services, including both operational services and training, to partner organizations and users by maximizing the sharing of its computing and communications infrastructure, the associated systems and software and its specialist skills, so that recipients of its services can benefit from economies of scale". The Agency's mandate also states that it must operate on a purely cost-recovery basis, with no core funding. The Agency is governed by a Management Committee, composed of one representative from each partner organization. The Management Committee's role is to provide broad policy guidelines and review the Agency's work programmes.

4. Each partner organization signs a MOU with the Agency that sets out the general terms under which the Agency conducts its business (including roles and responsibilities, payment terms and confidentiality). Service specifications provided by the Agency under the MOU are detailed in service delivery agreements (SDAs). SDAs may contain a one-time project component (also known as "project agreements"), and a recurring service component. Major changes to services are managed through business change requests (BCRs) that are contractual agreements agreed and signed by both parties. The mandate, MOU, SDAs, and BCRs constitute the contractual framework for specific service deliverables.

5. At the time of the audit, the services provided by the Agency to OIM were covered under three main SDAs, various BCRs and project agreements. The services included: (i) infrastructure services (i.e., servers and enterprise server support, storage on demand and management, enterprise backup); (ii) network services; (iii) email services; (iv) web services; (v) help desk support; and (v) consulting services. The cost of actual usage of the Agency services by OIM are shown in Table 1.

Table 1: Cost of the Agency's services used by OIM (in $)

Year	*Usage*
2015	1,197,466
2016	1,256,541
2017	1,130,169
2018	1,194,573

6. Comments provided by OIM are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

7. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the management of ICT services provided by the Agency to OIM.

8. This audit was included in the 2017 risk-based work plan of OIOS due to the risk that potential weaknesses in management of ICT services provided by the Agency could lead to sub-optimal utilization of resources and non-achievement of the intended objectives.

9. This audit was initiated in September 2017 but was suspended in January 2018 to give higher priority to the General Assembly's request for a comprehensive audit of the governance structure and related processes of the United Nations Joint Staff Pension Board, which OIOS completed in September 2018. OIOS resumed the present audit in October 2018 and completed the fieldwork in January 2019. The audit covered the period from January 2015 to January 2019. Based on an activity-level risk assessment, the audit focused on risk areas relating to the provision of ICT services by the Agency including: (a) strategy, budgeting and acquisition planning; (b) service and project management; and (c) ICT security.

10. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data; and (d) sample testing of performance documents, invoices, and usage reports related to the various services provided by the Agency per the SDAs, MOUs and BCRs.

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

III. AUDIT RESULTS

A. Strategy, budgeting and acquisition planning

Inadequate strategic planning and service transition

12. The OIM ICT Steering Committee was established and authorized by the RSG to oversee the alignment of the ICT strategy with OIM's investment strategy. OIM documented a target operating model with the assistance of a consulting firm that defined a "multi-year roadmap" of projects aimed to improve the systems, processes, organization and data needed to support OIM's goals.

13. One of the recommendations in the target operating model was to outsource OIM's infrastructure (servers, application support and networking) and review its existing supplier relationships to ensure an adequate level of support and pricing to match international trading requirements. As part of its effort to implement this recommendation, OIM planned to transfer the services provided by the Agency to other vendors. The plan included: (i) gathering requirements; (ii) developing a request for proposal for long-term infrastructure support to obtain a lower-cost solution; and (iii) migrating to the new infrastructure. Pending the conduct of a competitive bidding exercise, OIM reviewed its existing contractual agreements with the Agency and drafted a new one in November 2018 by consolidating the existing SDAs and BCRs which will be valid until transition of all services to the new vendor(s).

14. The draft SDA with the Agency included some new projects for the transition of certain applications and systems from the Agency to a cloud vendor. However, the decision to transfer the services from the Agency to a new service provider was made without preparing a business case to determine whether the transition to another vendor is desirable, viable and will achieve return on investment. As of February 2019, the draft business case was not complete and had not been presented to the ICT Steering

Committee. However, OIM entered into a new SDA (with project agreements) without prior evaluation of the business case, costs and benefits of transition to a new service provider.

15. Furthermore, the business case documented for the new projects did not include an accurate estimation of cost and benefits. For example, the total cost of ownership and return on investments were not properly calculated in the business case; the annual cost of maintaining the existing Enterprise Communication Services was shown as a cost saving of $162,000 whereas the correct figure was $66,912. In the absence of reliable benefit estimation and documentation, it was not clear how the benefits from the project will be measured, and when they will be realized.

(1) OIM should: (a) present the updated business case and transition strategy to the ICT Steering Committee for review and approval to ensure that the costs and benefits are desirable, viable and in the best interest of OIM; and (b) update its transition strategy in alignment with the completed business case.

OIM accepted recommendation 1 and stated that it will provide business case documents for each project under the project agreements, minutes of the ICT Steering Committee, business case and draft statement of work for the new infrastructure service provider. Recommendation 1 remains open pending receipt of evidence showing that it has been implemented.

OIM interests should be represented in the Management Committee of the Agency

16. The operations of the Agency are governed by a Management Committee composed of one representative from each partner organization. The Management Committee reviews and approves the business plan, programme budget, financial and technical reports, and provisional unit costs charged by the Agency for its services, establishes operational policies, and makes recommendations to the Director of the Agency for the effective functioning of the Agency.

17. Prior to l January 2015, the Agency provided services to OIM under an MOU that was between the Fund Secretariat and the Agency due to the common infrastructure of UNJSPF as a whole. As such, all changes, technical issues and financial matters were routed to the Agency through the Fund Secretariat, and all contractual agreements were signed by the Chief Executive Officer or Deputy Chief Executive Officer of the Fund Secretariat. In 2015, OIM and the Fund Secretariat separated their ICT infrastructure and fully transferred the management of their ICT infrastructure to the Agency under separate MOUs/agreements.

18. Even though OIM established separate MOU and agreements with the Agency, it was not represented on the Agency’s Management Committee which met twice a year to discuss overall strategy of the Agency, policy matters, work plans and other issues. The Fund Secretariat was represented in the Agency’s Management Committee by one member and an alternate member. The information presented to the Management Committee was not shared with OIM. Therefore, OIM had no role in the decisions made by the Committee and remained unaware of its activities.

19. In February 2019, OIM contacted the Agency and formally requested a member seat in the Agency’s Management Committee which was pending approval at the time of the audit. In view of the action taken by OIM, OIOS did not make a recommendation on this issue.

The methodology for estimating service and budget requirements needs to be strengthened

20. To assist it with its business planning process, the Agency’s mandate requires each partner organization to provide indications of changes in workload foreseen for services currently provided and the

likely dates of any changes, as well as indications of new work intended for the Agency. This requirement is defined in the funding estimates prepared by each partner organization to reflect the content of all services required from the Agency. The Agency raises invoices on a quarterly basis in advance for an amount corresponding to the funding estimates for the quarter covered by the invoice. At the end of every financial period, there was a reconciliation of the funding estimates and the actual expenditures incurred on providing the services.

21. OIM provided a detailed breakdown of the Agency's services (aggregating $3 million) in its budget proposal of the 2016-2017 biennium. According to the Agency's service usage reports, OIM used services valued at $2,386,711 during the 2016-2017 biennium. The difference between the budgeted amount and actual usage was $613,289. This underspending was caused by reduced/cancelled services which should have been reflected in the budget proposal for the following biennium.

22. OIM explained that the Agency reconciled the actual usage with the payments at the end of each biennium and issued a credit note to OIM. OIOS is of the view that not knowing the amount of credit until the end of biennium was not in the financial interest of OIM and did not facilitate a transparent budgeting process. During the audit, OIM decided to request quarterly credit notes from the Agency instead of biennial credit notes.

23. OIM's budget proposal for the 2018-2019 biennium did not clearly indicate the amount associated with the Agency's services. Instead, it provided a combined estimate for infrastructure services ($4,479,900) which included services provided by the Agency as well as the Office of Information and Communications Technology of the United Nations Secretariat. During the audit, OIM stated that the budget requested for the Agency's services during 2018-2019 was $4,255,008. OIOS review showed that: (a) the cost of various systems and services that were no longer used by OIM were included in the budgeted amount; (b) the cost of new projects planned to be implemented during the biennium were not included in the budget proposal; and (c) the credit note that would be received at the end-of biennium for unused services was not considered.

24. Table 2 shows the details of budgeted, actual and planned amounts required for the Agency's services. The requested budget was almost two times the required amount.

Table 2: OIM budget for the Agency's services versus actual and planned usage

Description	Amount ($)
Proposed budget for the Agency's services (2018-2019)	4,255,008
Credit received from the previous biennium	830,454
Actual usage during 2018	(1,194,573)
Expected usage during 2019	(1,279,524)
New projects in 2019-20	(640,651)
Net resource requirement for the Agency's services	**2,284,294**

(2) OIM should review its actual usage of the services provided by the United Nations agency and use it as the basis to determine future service requirements and the related budgets.

OIM accepted recommendation 2 and stated that it will provide detailed breakdown of 2018 actual usage, detailed breakdown of 2019 new SDA and draft 2020 budget related to the Agency's services. Recommendation 2 remains open pending receipt of evidence showing that it has been implemented.

B. Service and project management

Contract management, asset management and configuration management need to be strengthened

25. OIM managed its infrastructure and network (the majority of its physical or virtual assets) through two SDAs with the Agency, namely infrastructure services and network services. These agreements were signed in 2014 and 2015 respectively, reflecting the ICT environment at that time. Since then, OIM's ICT infrastructure went through various major changes such as separation of network infrastructure from the Fund Secretariat and decommissioning of various business applications. In addition, several servers were decommissioned or virtualized using new technologies. OIOS also noted the following:

(a) After major changes, the scope and cost of the existing SDAs were not updated. Changes that required additional cost were implemented through BCRs, but they did not trigger an update of the existing SDAs. Each new SDA, BCR or project agreement was independently prepared without considering the previous ones. This caused a misalignment between contractual agreements and actual services received.

(b) OIOS' review of the new draft SDA of November 2018, which was planned to consolidate all the existing SDAs and BCRs, showed that the scope of services contained obsolete information from previous SDAs. Table 3 shows examples of variation between actual requirements and the scope of services defined in the new consolidated SDA. During the audit, OIM took note of the highlighted issues and revised the draft SDA to reflect the actual ICT portfolio.

Table 3: Examples of variation between actual services and the scope of the new consolidated SDA

Description	Draft SDA of November 2018	Actual need
Number of physical server provisioning and hosting	5	3
Number of virtual server provisioning and hosting	40	29
Number of Enterprise Server Support	45	31
Additional Memory	300	220
Additional CPU	80	58
Number of Backup Nodes	45	31

Data source –Original and updated versions of the draft SDA

26. For effective management of ICT systems and services, it is imperative for organizations to have an up-to-date inventory of their ICT assets and accurate data for effective configuration management.

27. In two audits conducted by OIOS in 2014 and 2015, risk exposures related to lack of a configuration management process were highlighted to OIM and recommendations were made to improve the tracking of ICT services, assets (physical and virtual), and their dependencies. In 2017, OIM hired the Agency to conduct an assessment of its configuration and change management processes. OIM established its configuration management policy and procedure and implemented an Excel-based Configuration Management Database (CMDB).

28. OIOS noted during the current audit that the OIM configuration management policy and procedures were not effectively implemented and CMDB was not properly maintained. For example:

(a) Information on various servers maintained by OIM did not match the records kept by the Agency. According to OIM records, there should be 16 equipment (physical servers and network equipment) in the main data centre. The matching exercise showed that 12 OIM assets (server or network equipment) were missing from the Agency's records.

(b) Records of decommissioned servers were not complete and did not capture the date of decommissioning. Therefore, it was not possible to accurately determine when the Agency should stop charging for the decommissioned service.

(c) Serial numbers of some of the equipment in the Agency's records did not match OIM records.

(d) 12 Citrix XenApp servers (idle since October 2018) and 1 SWIFT server (idle since 2017) were shown as active and continued to be charged for, even though these had been replaced by new systems.

29. Weaknesses in management of changes in contract scope and controls over configuration and asset management resulted in: (a) misalignment of contractual agreements with the services actually received; (b) inaccurate budgeting; and (c) payment for unused services. During the audit, OIM initiated action to address these issues and requested a quarterly meeting with the Agency to keep track of its assets and verify the accuracy of the services charged for.

(3) OIM should: (a) periodically perform a verification of its physical and virtual assets hosted and managed by service providers; (b) identify, decommission and dispose of idle servers and network equipment; (c) update the configuration management database to ensure correct billing; and (d) improve the due-diligence process during preparation of contractual agreements by conducting a holistic review of existing ICT infrastructure and agreements.

OIM accepted recommendation 3 and stated that it will provide: terms of reference for the quarterly vendor performance review; report of the next review of assets performed in second quarter of 2019 by OIM as per the new SDA; updated list of active assets; evidence of request to decommission inactive assets; updated OIM CMDB; and updated SDA. Recommendation 3 remains open pending receipt of these documents and evidence of periodic review to ensure the alignment of contractual agreements with the existing ICT infrastructure.

Project management procedures need to be strengthened

30. Project agreements should be detailed enough to describe the requirements, deliverables, acceptance criteria, implementation timelines and cost of the project. Best practice requires that at the end of projects, all project deliverables are signed off and a closure report is produced detailing the final cost, time, and information on the achievement of objectives.

31. OIOS review of the various project documents showed a number of weaknesses detailed below.

(i) Project planning

32. At the time of the audit, OIM was in the process of finalizing a project agreement with the Agency. OIOS reviewed this agreement to assess project management controls and noted the following:

(a) Unrelated projects were consolidated under one project title without clear description of individual project activities and deliverables. For example, the projects on ISO-27001 implementation, implementation of network Intrusion Prevention System, and migration to Share Point were all described under one project name called Microsoft Cloud Migration Project.

(b) Costs were not associated with the project deliverables.

33. OIM took note of these issues and revised the project document during the audit. As a result of this revision, the project agreement was split into five separate projects with clear project description, deliverables and associated cost components to enable OIM to track the projects separately and facilitate their successful implementation.

(ii) Project closure

34. According to the Agency's business model, two types of project reports should be prepared for all projects: (i) quarterly "Project to date reports"; and (ii) "end of project report". The purpose of these reports was to summarize the status of project deliverables and show the project's budget compared to used resources. OIOS' analysis of the project documents showed that for most projects, no "end of project report" was prepared. Therefore, the completion date and actual expenditure of several projects were not known, including the following:

(a) Enterprise Communication Services;
(b) Web site development extension;
(c) Exchange (old-email system) and Active Directory Administration;
(d) Bit Locker;
(e) Managed hosting services for additional infrastructure; and
(f) IP Reconfiguration with Dynamic Host Configuration Protocol Implementation.

(4) OIM should: (a) ensure that project agreements describe the projects in sufficient detail and clearly link deliverables to project costs; (b) document the project benefit realization plans; and (c) ensure that closure reports are documented at the end of each project.

OIM accepted recommendation 4 and stated that it will provide: updated project agreements; project documents including bi-weekly progress reports; project closure reports; and description of OIM's Programme Management Office roles and responsibilities. Recommendation 4 remains open pending receipt of evidence showing that it has been implemented.

Service level monitoring needs to be strengthened

35. Best practices require that ICT services should be reviewed on a regular basis to maintain and improve service quality.

36. OIM and the Agency had periodically met to review the status of services and projects as well as invoices and statement of accounts until September 2016. However, no service review meetings were held since then, except for one formal meeting in November 2018. OIOS also noted the following:

(a) There were no coordinated communication mechanisms to address issues and questions raised by OIM. This resulted in concerns not been addressed in a timely manner (for example, the Agency did not provide a response to various follow-up emails from OIM regarding some open requests, which should have been escalated as an issue to service managers).

(b) No periodic service reports were provided except for Enterprise Communication Services. For example, for Help Desk support, the last service report provided by the Agency was in December 2017.

(c) Availability report (2018) for OIM services did not provide information for several months. For example, availability information for April 2018 and August 2018 was not included in the availability records of network services.

(d) Service level targets and achievements were listed in a high-level report that did not provide any detailed breakdown of service-specific targets and achievements.

(e) Some of the professional services (such as consultancy services) were included as recurring services in the new SDA without any key performance indicators or deliverables defined. In the absence of clear deliverables and tasks, it was not clear how OIM monitored the performance and effectiveness of these consultancy services.

(5) OIM, in coordination with the United Nations agency, should: (a) initiate periodic service monitoring and review meetings to communicate issues, delays, status of services/projects and status of accounts, invoices and credits; and (b) transfer recurring professional services to one-time services with clear deliverables and key performance indicators.

OIM accepted recommendation 5 and stated that it will provide minutes of the next quarterly meeting in 2nd quarter of 2019; service reports for all services; availability reports for all services; actual usage and credit note report; updated project agreements and SDA. Recommendation 5 remains open pending receipt of evidence showing that it has been implemented.

Weaknesses in invoice certification caused unnecessary advance payments for unused services

37. Invoices and payments should be relevant to the services rendered. The Agency's business model requires that invoices should be paid in advance for the services planned to be delivered in the next quarter. This meant that OIM should not pay for any service that would not be used in the next quarter. OIOS noted the following in this regard:

(i) Concurrent payments for old and new email systems

38. OIM transferred the management of its old email system to the Agency in December 2014 with a recurring cost of $476,760 per biennium. Following this transfer, a new project started in July 2015 for implementation of a new email system. The recurring service cost of the new email system was $133,824 per biennium. The project was completed in May 2016. In August 2016, OIM requested the Agency to decommission its old email system (11 servers).

39. OIOS noted that the Agency's usage reports for 2016 and 2017 did not reflect any usage charges for the old email system. However, the Agency continued to send invoices associated with the old system to OIM during the 2016-2017 biennium. OIM paid invoices amounting to $476,760 for the BCR "Exchange and Active Directory Administration Services" without review. At the end of 2016-2017 biennium, the Agency issued a credit note for unused services that were paid in advance by OIM. However, the breakdown of the credit note did not include a line item for the old email service. The Agency explained that recurring costs were charged to an account for Infrastructure Services instead of Exchange and Active Directory Administration Services (i.e., old email system) and the credit was applied to the former account.

40. By not reviewing service usage reports before authorizing recurring payments, OIM made advance payments to the Agency for services that it knew will not be utilized amounting to approximately $317,840 covering 16 months, from September 2016 to December 2017. Additionally, credit notes sent by the Agency at the end of each biennium did not include a detailed breakdown which made it difficult to reconcile with the service usage reports and verify the accuracy of the credited amount.

(ii) Overpayments for discontinued/unused services and inability to reconcile credit notes

41. On 18 December 2014, OIM sent a request (BCR) to the Agency, titled “BCR-Extension of Infrastructure Support for IMD”. The request included enterprise server support for nine servers that were located in the data centre in the Dag Hammarskjold Plaza (DHP) building. The recurring service cost was estimated as $77,016 per biennium. In May 2016, OIM decided to decommission some of these servers by archiving the data and virtualize and move some others to the main data centre. This was done through a new BCR titled “BCR-Managed hosting services for additional infrastructure”. There were no servers left in the DHP data centre after this BCR was implemented. The recurring cost of the new BCR was estimated as $326,136 per biennium although it caused decommissioning of several physical servers or replacement of them with virtual servers.

42. OIM continued to pay invoices amounting to $125,151 for “BCR-Extension of Infrastructure Support for IMD” until December 2018 for servers that did not exist since 2016. Similarly, OIM continued to pay in advance for unused services amounting to $475,870 for invoices charged against “BCR-Managed hosting services for additional infrastructure” until December 2018 (covering three years). According to the Agency’s service usage reports, OIM’s actual usage value that should be charged for these two BCRs were $6,612 for 2016 and $6,722 for 2017.

43. Lack of detailed credit notes and inadequate invoice certification caused unnecessary advance payments for unused services.

(6) OIM should: (a) request the United Nations agency to provide detailed breakdown for the credit notes of 2016-2017 and 2018 for each service; (b) reconcile the advance payments against the unused services and recover the net overpayments; (c) request the Agency to provide quarterly credit notes rather than biennial; and (d) strengthen the invoice certification process to ensure that payments are not approved for unused services.

OIM accepted recommendation 6 and stated that it will provide: detailed breakdown of past credit notes; reconciliation report comparing invoices vs actual usage and credit notes; quarterly credit note; new invoice certification process. Recommendation 6 remains open pending receipt of evidence showing that it has been implemented.

OIM was not informed about infrastructure changes made by the Agency

44. A service provider should inform its client about the changes done on the services especially if the change may impact the client operations.

45. OIOS reviewed a sample of 14 infrastructure or configuration changes that may have an impact on the availability of OIM services. OIM was notified of the changes on 3 occasions out of 14.

46. Additionally, during the audit, the Agency decommissioned and disposed of three physical servers (ESX servers) in December 2018. Until OIOS’ inquiry, OIM was not aware of the decommissioning of these servers which require an update of OIM inventory and will impact the verification of future invoices.

(7) OIM should communicate its change management requirements to the United Nations agency to ensure that it is informed about the changes before their implementation.

OIM accepted recommendation 7 and stated that it will provide: the memorandum communicating change management requirements to the Agency, including OIM’s Change Advisory Board’s terms *of reference; and list of change requests performed by the Agency and reviewed during the quarterly meeting in the second quarter of 2019.* Recommendation 7 remains open pending receipt of evidence showing that it has been implemented.

C. ICT security

Long delays in mitigating the reported security risks

47. The service provider should mitigate the ICT security risks communicated to it as a priority and audit logs on the critical servers containing confidential data should be enabled and monitored periodically.

48. OIOS noted the following in this regard:

(a) One of the OIM servers contained confidential information grouped under different drives and restricted to the users of specific OIM groups such as RSG's Office, Traders group, Operations, Compliance, Investments, and Backups. After an incident in July 2018, OIM requested the Agency to enable the access logs of the server into the centralized log repository. However, the Agency did not initiate any action on this request nor provide feedback despite several follow-ups from the ICT security officer of OIM. The work was finally completed on 21 February 2019, seven months after the incident. During the audit, OIM senior management was informed about the risk of unauthorized access to the information stored on the server.

(b) OIM established a quarterly monitoring mechanism to review users with 'administrative' access rights on OIM systems. The ICT security officer sends the list of administrators to the Agency every quarter to confirm their duties. During the last review in January 2019, there was a user with administrator privileges to OIM's systems who no longer worked for the Agency. The user account was deleted upon request of OIM during the audit.

(c) In July 2018, OIM hired a vendor to conduct an ethical hacking exercise on OIM systems. The vulnerabilities identified by the exercise were communicated to the Agency as a service request for implementation of mitigation actions. The service request was still in progress at the time of the audit.

(d) OIM's servers and network equipment are hosted in the Agency's data centre in New Jersey in a shared cage with other clients. The racks holding the equipment were not locked and the equipment was physically accessible by other clients of the Agency.

(e) In the data centre, even though redundant power sources were available in the racks to ensure continuity of services in the event of the primary power source becoming unavailable, one of the network devices (which supports redundant power supplies) was not connected to the redundant power source.

(8) OIM should: (i) periodically monitor the access logs of the file server to ensure that confidential information is not accessed by unauthorized parties; (ii) ascertain from the United Nations agency the reasons for its delayed response to the ICT security incident of July 2018; (iii) implement mitigating controls in coordination with the Agency for the vulnerabilities communicated to it after the ethical hacking exercise; and (iv) communicate to the Agency the need to ensure redundancy of power supply to OIM equipment.

OIM accepted recommendation 8 and stated that it will provide: evidence of OIM periodic log review process and controls; memo escalating the ICT security incident of July 2018; new ethical *hacking assessment ensuring that identified vulnerabilities have been addressed; and memorandum communicating to the Agency the need for redundancy of power supply and evidence of implementation in next review meeting.* Recommendation 8 remains open pending receipt of evidence showing that it has been implemented.

IV. ACKNOWLEDGEMENT

49. 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.

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

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology services provided by a United Nations agency to the Office of Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	OIM should: (a) present the updated business case and transition strategy to the ICT Steering Committee for review and approval to ensure that the costs and benefits are desirable, viable and in the best interest of OIM; and (b) update its transition strategy in alignment with the completed business case.	Important	O	Receipt of evidence showing that the recommendation has been implemented.	31 May 2019
2	OIM should review its actual usage of the services provided by the United Nations agency and use it as the basis to determine future service requirements and the related budgets.	Important	O	Receipt of evidence showing that the recommendation has been implemented	30 April 2019
3	OIM should: (a) periodically perform a verification of its physical and virtual assets hosted and managed by service providers; (b) identify, decommission and dispose of idle servers and network equipment; (c) update the configuration management database to ensure correct billing; and (d) improve the due-diligence process during preparation of contractual agreements by conducting a holistic review of existing ICT infrastructure and agreements.	Important	O	Receipt of documents and evidence of periodic review to ensure the alignment of contractual agreements with the existing ICT infrastructure.	31 May 2019
4	OIM should: (a) ensure that project agreements describe the projects in sufficient detail and clearly link deliverables to project costs; (b) document the project benefit realization plans; and (c) ensure that closure reports are documented at the end of each project.	Important	O	Receipt of evidence showing that the recommendation has been implemented.	30 September 2019
5	OIM, in coordination with the United Nations agency, should: (a) initiate periodic service monitoring and	Important	O	Receipt of evidence showing that the recommendation has been implemented.	31 May 2019

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

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

[3] C = closed, O = open

[4] Date provided by OIM in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology services provided by a United Nations agency to the Office of Investment Management of the United Nations Joint Staff Pension Fund

	review meetings to communicate issues, delays, status of services/projects and status of accounts, invoices and credits; and (b) transfer recurring professional services to one-time services with clear deliverables and key performance indicators.				
6	OIM should: (a) request the United Nations agency to provide detailed breakdown for the credit notes of 2016-2017 and 2018 for each service; (b) reconcile the advance payments against the unused services and recover the net overpayments; (c) request the agency to provide quarterly credit notes rather than biennial; and (d) strengthen the invoice certification process to ensure that payments are not approved for unused services.	Important	O	Receipt of evidence showing that the recommendation has been implemented.	31 May 2019
7	OIM should communicate its change management requirements to the United Nations agency to ensure that it is informed about the changes before their implementation.	Important	O	Receipt of evidence showing that the recommendation has been implemented.	15 May 2019
8	OIM should: (i) periodically monitor the access logs of the file server to ensure that confidential information is not accessed by unauthorized parties; (ii) ascertain from the United Nations agency the reasons for its delayed response to the ICT security incident of July 2018; (iii) implement mitigating controls in coordination with the Agency for the vulnerabilities communicated to it after the ethical hacking exercise; and (iv) communicate to the Agency the need to ensure redundancy of power supply to OIM equipment.	Important	O	Receipt of evidence showing that the recommendation has been implemented.	30 September 2019

APPENDIX I

Management Response

UNITED NATIONS **NATIONS UNIES**

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: A: Gurpur Kumar, Deputy Director
Internal Audit Division, OIOS

DATE: 24 April 2019
REFERENCE: OIM/IT/OIOS

FROM: DE: Sudhir Rajkumar, Representative of the Secretary General for the Investments of the Assets of the United Nations Joint Staff Pension Fund

OIC

SUBJECT: OBJECT: The Office of Investment Management response to the Office of Internal Oversight Services related to Assignment No. AT2017/801/01

1. The Office of Investment Management (OIM) of the United Nations Joint Staff Pension Fund (UNJSPF) acknowledges receipt of the Draft Report on the audit of information and communication technology services provided by the United Nations International Computing Centre (UNICC).

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 (Annex I – Audit recommendations) including detailed responses and comments.

cc: Herman Bril, Director
William Wilkinson
Isabela Perle Munch
Eduardo Hilzinger
Zachary Ikiara
Cynthia Avena-Castillo

APPENDIX I

Management Response

Audit of information and communications technology services provided by a United Nations agency to 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: (a) present the updated business case and transition strategy to the ICT Steering Committee for review and approval to ensure that the costs and benefits are desirable, viable and in the best interest of OIM; and (b) update its transition strategy in alignment with the completed business case.	Important	Yes	Information Systems Officer	31 May 2019	OIM will provide the following: - Business case documents (for each UNICC project under the project agreement) - Minutes of the ICT Steering Committees including recommendations made based on the submission - Business case and draft statement of work for the new Infrastructure Service Provider (ISP)
2	OIM should review its actual usage of the services provided by the United Nations agency and use it as the basis to determine future service requirements and the related budgets.	Important	Yes	Project Management Officer	30 April 2019	OIM will provide the following: - Detailed breakdown of 2018 actual usage - Detailed breakdown of 2019 new SDA - Draft 2020 budget related to ICC services
3	OIM should: (a) periodically perform a verification of its physical and virtual assets hosted and managed by service providers; (b) identify, decommission and dispose of idle	Important	Yes	Information Systems Officer	31 May 2019	OIM will provide the following: - Terms of Reference (ToR) of the quarterly vendor performance review approved by OIM and ICC

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

APPENDIX I

Management Response

Audit of information and communications technology services provided by a United Nations agency to the Office of Investment Management of the United Nations Joint Staff Pension Fund

	servers and network equipment; (c) update the configuration management database to ensure correct billing; and (d) improve the due-diligence process during preparation of contractual agreements by conducting a holistic review of existing ICT infrastructure and agreements.					- Report of the next review of assets performed in 2Q2019 by OIM as per the new SDA with ICC - Updated list of active assets - Evidence of requests to decommission inactive assets - Updated OIM CMDB matching ICC - Updated service delivery agreement (SDA)
4	OIM should: (a) ensure that project agreements describe the projects in sufficient detail and clearly link deliverables to project costs; (b) document the project benefit realization plans; and (c) ensure that closure reports are documented at the end of each project.	Important	Yes	Project Management Officer	30 September 2019	OIM will provide the following for each project: - Updated project agreements (PA) - Project documents including bi-weekly progress reports - End project reports - Description of OIM's Programme Management Office (PMO) roles and responsibilities
5	OIM, in coordination with the United Nations agency, should: (a) initiate periodic service monitoring and review meetings to communicate issues, delays, status of services/projects and status of accounts, invoices and credits; and (b) transfer recurring professional services to one-time services with clear deliverables and key performance indicators.	Important	Yes	Senior Information Systems Officer	31 May 2019	OIM will provide the following: - Minutes of the next quarterly meeting in 2Q2019 - Service reports for all services - Availability reports for all services - Actual usage and credit note report - Updated project agreements (PA) and service delivery agreement (SDA)

APPENDIX I

Management Response

Audit of information and communications technology services provided by a United Nations agency to the Office of Investment Management of the United Nations Joint Staff Pension Fund

6	OIM should: (a) request the United Nations agency to provide detailed breakdown for the credit notes of 2016-2017 and 2018 for each service; (b) reconcile the advance payments against the unused services and recover the net overpayments; (c) request the agency to provide quarterly credit notes rather than biennial; and (d) strengthen the invoice certification process to ensure that payments are not approved for unused services.	Important	Yes	Project Management Officer	31 May 2019	OIM will provide the following: - Detailed breakdown of past credit notes - Reconciliation report comparing invoices vs actual usage + credit notes - Quarterly credit note - New invoice certification process
7	OIM should communicate its change management requirements to the United Nations agency to ensure that it is informed about the changes before their implementation.	Important	Yes	Project Management Officer	15 May 2019	OIM will provide the following: - Memo communicating change management requirements to ICC, including OIM's Change Advisory Board (CAB) ToR - List of change requests performed by ICC and reviewed during the quarterly meeting in 2Q2019
8	OIM should: (i) periodically monitor the access logs of the file server to ensure that confidential information is not accessed by unauthorized parties; (ii) ascertain from the United Nations agency the reasons for its delayed response to the ICT security incident of July 2018; (iii) implement mitigating controls in coordination with the agency for the vulnerabilities communicated to it after the ethical hacking exercise; and (iv)	Important	Yes	Information Security Officer	30 September 2019	OIM will provide the following: - Evidence of OIM periodic log review process and controls - Memo escalating ICT security incident of July 2018 - New ethical hacking assessment ensuring that identified vulnerabilities have been addressed - Memo communicating to ICC the need for redundancy of power supply

Management Response

Audit of information and communications technology services provided by a United Nations agency to the Office of Investment Management of the United Nations Joint Staff Pension Fund

	communicate to the agency the need to ensure redundancy of power supply to OIM equipment.					and evidence of implementation in next review meeting