INTERNAL AUDIT DIVISION

REPORT 2023/007

Audit of the Integrated Pension Administration System's Member Self-Service and Employer Self-Service modules in the United Nations Joint Staff Pension Fund

The Pension Administration needs to enhance the effectiveness of the Member Self-Service and Employer Self-Service modules

25 March 2023
Assignment No. AT2022-800-02

Audit of the Integrated Pension Administration System's Member Self-Service and Employer Self-Service modules in the United Nations Joint Staff Pension Fund

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of the Integrated Pension Administration System's Member Self-Service (MSS) and Employer Self-Service (ESS) modules in 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 use of MSS and ESS by the user community and the management of the modules by the Pension Administration. The audit covered the period from 1 January 2020 to 30 September 2022 and included a review of: (a) system design and development; (b) identity and user access management; (c) information technology operations; (d) change management; and (e) vulnerability management.

The audit indicated the need for the Pension Administration to enhance the effectiveness of MSS and ESS modules. OIOS made five recommendations. To address the issues identified in the audit, the Pension Administration needed to:

- Document its assessment of the desired future state of the ESS and MSS modules considering the other new initiatives in progress, clarify the roles and responsibilities for the ESS module, and mitigate the business continuity risk arising from assignment of functions to one staff member;
- Strengthen mechanisms for identity proofing and authentication of participants and beneficiaries and the digital documents uploaded by them through the MSS module;
- Establish mechanisms for: periodic analysis of MSS profiles and email IDs to identify and address data anomalies/discrepancies; periodic review of ESS user access and re-certification; and authenticating ESS users against the Microsoft Azure Directory;
- Incorporate the MSS module in disaster recovery exercises to assure its availability to clients; and
- Strengthen service management for client requests by: establishing a mechanism for providing feedback to clients on the status of resolution of their requests; and recording and communicating the reasons for cancellation and closure of their requests.

The Pension Administration accepted the recommendations and has initiated action to implement them. Actions required to close the recommendations are indicated in Annex I.

CONTENTS

Audit of the Integrated Pension Administration System's Member Self-Service and Employer Self-Service modules in the United Nations Joint Staff Pension Fund

I. BACKGROUND

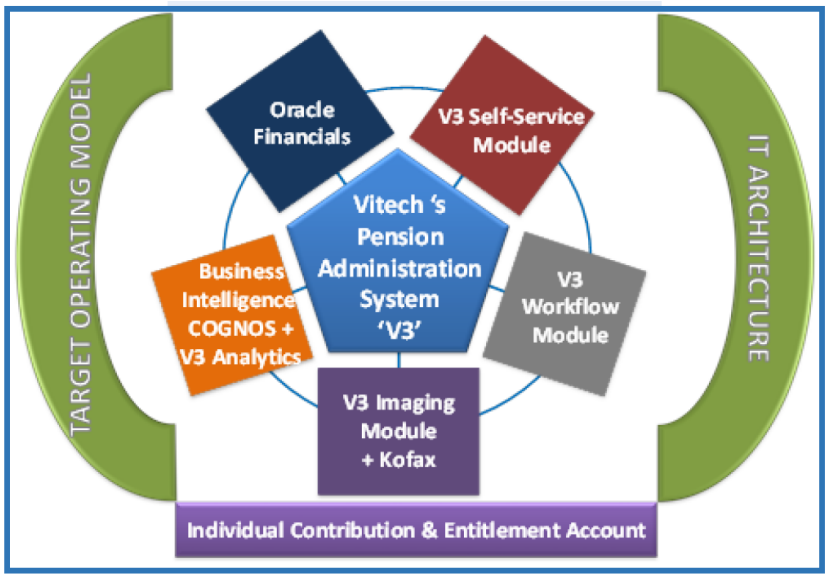
1. The Office of Internal Oversight Services (OIOS) conducted an audit of the Integrated Pension Administration System's (IPAS) Member Self-Service (MSS) and Employer Self-Service (ESS) modules in the Pension Administration of the United Nations Joint Staff Pension Fund (UNJSPF).

2. UNJSPF was established in 1949 by the General Assembly to provide retirement, death, disability and related benefits for the staff of the United Nations and other organizations admitted to the membership of the Fund. UNJSPF is administered by the United Nations Joint Staff Pension Board (the Pension Board).

3. The Pension Administration's clients comprise: (i) participants; (ii) retirees and other beneficiaries; and (iii) individuals who act on behalf of beneficiaries, such as family members and other interested parties (hereafter collectively referred to as 'beneficiaries'). While the Pension Administration also provides services to its member organizations including the secretaries of the various Staff Pension Committees (SPC), these entities are considered as the Fund's strategic partners in support of clients. Currently, there are approximately 219,573 participants/beneficiaries and approximately 1,200 users from the Fund's member organizations.

4. Self-service portals in IPAS are split into the ESS module for member organizations and MSS module for participants and beneficiaries. These modules aim to reduce the administrative burden on UNJSPF staff by providing functionality that empowers member organizations, participants and beneficiaries to perform certain tasks themselves, without having to contact the Pension Administration for assistance. The modules use the same database as the Line of Business interface used by the Pension Administration staff, and are integrated with the Vitech Pension Administration System 'V3' (version 9) as shown in Figure 1.

Figure 1: IPAS architecture



5. Client Services within the Pension Administration is responsible for managing and monitoring of MSS, whereas the responsibility for managing and monitoring of ESS is shared between the Financial and Operations Services. ESS is operationally managed by a business analyst who reports to the Chief Financial Officer. The Information Management Systems Service (IMSS) is responsible for computing and office automation support, acquisition and maintenance of software/hardware, design of systems, development and implementation of technology-driven solutions, cybersecurity, and project management for MSS as well as ESS.

6. Complete data on the Pension Administration's expenditure relating to implementation of MSS and ESS was not readily available. Based on data obtained from Umoja, the best estimate of the expenditure incurred on implementation of V3 since 2014 was approximately $41 million.

7. Comments provided by the Pension Administration 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 the use of MSS and ESS by the user community and the management of the modules by the Pension Administration.

9. This audit was included in the 2022 risk-based work plan of OIOS due to the risk that potential weaknesses in ESS and MSS modules could result in failure to achieve their intended objectives/benefits.

10. OIOS conducted this audit from September to November 2022. The audit covered the period from 1 January 2020 to 30 September 2022. Based on an activity-level risk assessment, the audit covered risk areas in ESS and MSS which included: (a) system design and development; (b) identity and user access management; (c) information technology operations; (d) change management; and (e) vulnerability management.

11. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data; (d) survey; and (e) walkthrough.

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

III. AUDIT RESULTS

A. System design and development

Need to document the roadmap and future state architecture for ESS and MSS

13. The status report to the Pension Board (JSPB/59/R.21) on the implementation of IPAS and the Target Operating Model (TOM) states that the enhanced TOM recognizes the importance and benefits of driving more activity towards web-based self-service applications for participants and beneficiaries as well as member organizations, and that TOM will enable, among others: (a) standardization of the operational environment; (b) establish efficient and effective mechanisms that will allow the Pension Administration and member organizations to communicate on errors or outstanding issues related to individual participants and beneficiaries; and (c) drive more activity towards web-based self-service applications.

14. As indicated earlier, MSS and ESS were managed by different services (MSS by Client Services, and ESS by the Financial and Operations Services). This situation was not conducive to standardizing the operational environment, including maintenance and user support. Also, issues related to participation in the Pension Fund and the contribution made by the participants are related activities because contribution depends on participation, and vice-a-versa. However, Financial Services dealt with contributions through a manual workaround outside ESS, whereas participation issues were dealt with by Operations Services. Additionally, there were two interfaces (Financial interface and Human Resources [HR] interface) to the V3 system which were outside ESS but used for handling contribution and participation issues. The lack of integration of these features diminished the potential benefit to be derived from implementing the ESS module. The Pension Administration stated that it decided not to use ESS for handling of contributions data and instead implemented interfaces which provide the required testing environment and enable the monthly reconciliation of contributions. ESS does not have automated features to record mass entries or mass updates, which are done by the interface. The decision to implement the Financial and HR interfaces through middleware to IPAS, without using MSS, allowed streamlining the collection of HR and Financial data from the multiple systems used by member organizations.

15. Also, there was no clarity in the roles and responsibilities for the ESS module to address evolving requirements. For instance, during the COVID-19 pandemic, with the need to upload documents relating to contribution, participation and After Service Health Insurance (ASHI) information remotely, it became necessary for the Pension Administration to establish a secure means for uploading such documents to prevent exposure of participants' personal information to cybersecurity-related risks. However, there was no plan to enhance ESS with additional security features to mitigate the related risks (such as use of multifactor authentication).

16. Operational decisions relating to ESS were being made by the business analyst in Financial Services, but this individual did not have the authority to make decisions related to business continuity. Further, since there was no backup arrangement for the business analyst, user support became unavailable during the individual's absence, which also impacted the availability of ESS for timely upload of important documents. For example, during the latest user certification exercise, there were significant delays arising from the absence of the business analyst on leave, since that staff member was the only point of contact for member organizations, and the same individual also kept the approved users' roster and exercised decision making/approving duties for user access.

17. Some functionalities envisaged as part of the TOM were not implemented for ESS, which also impacted its usability as originally intended. OIOS noted the following:

(a) Contribution data was sourced from member organizations and was meant to be fed directly into ESS. However, this data flow into ESS was stopped due to data integrity issues. Data fed by member organizations could not be validated in ESS for accuracy. As such, the validation of contribution data was done using a staging workaround in the ESS development environment, after which the data was manually uploaded into the V3 system. This arrangement was neither optimal nor secure because the development environment was not subjected to the same data protection controls as in the production environment. Typically, in the development environment, logging and monitoring of data is insufficient, backend access controls are weak, and developers use libraries and other software modules which could be vulnerable.

(b) ESS was originally intended to enable member organizations to submit contribution data relating to their participants. However, this functionality had not been implemented for all the member organizations; it was only implemented for smaller organizations. HR and contributions data were received through the HR and Financial interfaces, respectively. Out of the Fund's 24 member organizations, 16 submitted HR data on a monthly basis using the HR interface, whereas 11 submitted contributions data annually through the Financial interface.

(c) In line with its strategic goal to improve the client experience, increase efficiency and enhance security, the Pension Administration had enhanced the functionalities of the MSS module. For example, during the COVID-19 pandemic, the Pension Administration added the option of uploading documents in MSS, and new interfaces such as e-Pension and 'Kofax Total Agility' solutions are being created. The e-Pension module is envisioned to enable functionalities such as digital submission of 'Benefit Election', dynamic data validation checks, and member profile-based 'smart guidance' (i.e., displaying only the options relevant to the concerned member). Similarly, implementation of the 'Kofax Total Agility' solution will automate the highly labour-intensive procedure to process the documentation uploaded in MSS by enabling validation of fields and automated signature verification. The e-Pension and 'Kofax Total Agility' solutions were expected to be completed in 2023.

(d) The Pension Administration originally envisaged a message centre in ESS for communication with member organizations, which was not implemented. As such, there is no current functionality for secure communication between the Pension Administration and member organizations. Email communication still remains the mode for communicating sensitive and confidential information. Also, one of the high-level requirements of the implementation of 'Kofax-Total Agility' solution is the availability of a 'MSS secure mailbox' which will enable the participants and beneficiaries to upload documents securely and enable the Pension Administration to manage the uploaded documents efficiently. The Pension Administration stated that the document upload via MSS secure mailbox was implemented in 2020, prior to the adoption of the Kofax Total Agility solution. Kofax Total Agility project requirements were revised to incorporate the upload feature via MSS secure mailbox.

18. There was no documented assessment of the future viability of MSS and ESS that holistically considered the other new initiatives currently ongoing in Pension Administration, such as Digital Certificate of Entitlement (DCE), Customer Relationship Management (CRM), and technological upgradation. The Pension Administration stated that it intends to document the future state architecture with the implementation of the new CRM system, which is expected to start in 2023.

Need to enhance the user experience of MSS

19. User experience is critical for the success of any digital system. System design should be based on a sound understanding of user needs to make the system useful to its users. MSS is an internet-facing service that allows participants and beneficiaries to access their pension information. Therefore, system functionalities should simplify the user interface and minimize the need for intervention by Pension Administration staff.

20. Client Services was responsible for managing the MSS module. Since MSS was considered to be useful to participants and beneficiaries, the Pension Administration made enhancements such as the document upload functionality.

21. MSS provided role-based access to participants and beneficiaries regarding disbursements, documents, e-forms, proof documents, personal information, validation requests, restoration, transfer-in requests, benefit estimates and document upload. OIOS noted the following with regard to the user experience of MSS:

(a) Simplification of the client experience is described by the Pension Administration as one of its strategic objectives. This should enable participants and beneficiaries to make simple changes in their personal information through MSS, such as changes to their banking information, for example. However, participants and beneficiaries could not do so by using MSS. They were required to physically submit

change documents either in person or through authorized channels such as focal points within the concerned member organizations.

(b) MSS did not have the functionality to securely communicate personally identifiable information (such as change in marital status, for example). MSS also did not alert the participants and beneficiaries to changes made to their personal information, which is contrary to best practice that seeks to mitigate the risk of cyber impersonation.

(c) A feature of MSS was to allow participants to perform pension benefit simulations. However, the simulation tool did not provide reliable estimates in a number of scenarios. For example: (i) it calculated the estimate based on the last service period and ignored earlier periods for participants who had a break in service; (ii) it did not incorporate the value of deferred retirement benefits at age 55 or 58; (iii) it ignored periods of contributory service for participants with transfer-in from an outside international organization; and (iv) it ignored previous active periods of participation for beneficiaries who returned to active participation status after retirement for a new period of participation.

(d) The annual Certificate of Entitlement for beneficiaries was submitted through three channels (i.e., paper-based, MSS and DCE). The Pension Administration stated that the paper-based channel enabled it to verify the residence of beneficiaries under the two-track system. OIOS is of the view that the Pension Administration should devise appropriate means to allow beneficiaries of the two-track system to download the Certificate of Entitlement documents through MSS to expedite the validation of the process and make system more user-friendly for them.

(e) Participants and beneficiaries used the document upload functionality of MSS to submit documents and forms to the Pension Administration. However, these documents were held in the MSS repository without notifying the processor that the document was available for initiating appropriate action. The Pension Administration had to resort to manual intervention for extracting, uploading and indexing the documents into IPAS. This process was prone to error and delays in processing of benefits or updating of information in IPAS. The Pension Administration stated that extracting, uploading, and indexing the documents uploaded in MSS into IPAS has been automated with the integration of the MSS upload feature with Kofax Total Agility.

(f) Participants and beneficiaries needed to register in order to use MSS. The registration process required them to provide their 'Unique Identification Number (Unique ID)', 'Last Name' and 'Date of Birth'. However, MSS did not have user validation features to prevent a user with an existing profile from creating a duplicate profile as explained later in the report (an analysis of MSS user profiles identified 58 duplicates).

(g) Integration of MSS with the CRM solution (currently iNeed) is necessary for timely management and resolution of user queries/issues. Currently, when a user submits a query using the 'Contact Us' option, the system is not able to recognize the user's login credentials to generate the user's Unique ID, name and related information to initiate an automated workflow.

(1) The Pension Administration should: (a) document its assessment of the desired future state of the Employer Self-Service and Member Self-Service modules considering the other new initiatives in progress; and (b) clarify the roles and responsibilities for the Employer Self-Service module and mitigate the business continuity risk arising from assignment of functions to one staff member.

The Pension Administration accepted the recommendation and stated that the desired future state for MSS is documented in the Project Initiation Document (PID) of the Customer Relationship

Management (CRM) project, as approved by the Pension Board in July 2021. The PID provides the context, background, and details on the UNJSPF strategy, future state (to-be), and functional specification. Based on an assessment with the IPAS vendor, it was determined that the ESS module could not be used to submit separation documents due to technical limitations. Therefore, the Fund decided to limit the use of ESS to receive ASHI authorizations and ASHI import files. To address the audit recommendation, CRM project documents –including the future state of MSS and ESS - will continue to be updated as required. OIOS reviewed the PID of the CRM project and noted that it did not mention the desired future state of MSS and ESS, other than the functional requirements for self-service capabilities. Recommendation 1 remains open pending receipt of evidence that: (a) assessment of the desired future state of the ESS and MSS modules have been documented considering the other new initiatives in progress; and (b) the roles and responsibilities for the ESS module have been clarified, and the business continuity risk arising from assignment of functions to one staff member has been mitigated.

B. Identity and user access management

Need to strengthen identity proofing and authentication of MSS users

22. In order to confirm the identity of a participant or beneficiary, the Pension Administration requires them to submit supporting documents such as passport/driving license and bank statements which are manually matched against the signature of the participant or beneficiary on file. However, the current practice of matching the signature to verify the identity of the participant or beneficiary was not fully effective and needed to be strengthened.

23. It is essential for the Fund to ascertain the identity of the user who is uploading the digital documents, as well as the authenticity of the uploaded digital documents, to prevent potential abuse. In view of the geographically distributed population of the Fund's participants and beneficiaries, and the technical limitations in many remote locations, a single method for identity proofing and authentication may not be practical. Alternative methods may need to be used to verify the identity of the participant or beneficiary, such as multifactor authentication, biometric authentication or authentication through submission of a code generated by the DCE application.

24. The Pension Administration stated that it has initiated a project with the support of an inter-agency entity to incorporate multi-factor authentication for participants and beneficiaries.

(2) The Pension Administration should strengthen mechanisms for identity proofing and authentication of participants and beneficiaries and the digital documents uploaded by them through the Member Self-Service module.

The Pension Administration accepted recommendation 2 and stated that it would be addressed with the implementation of multi-factor authentication to IPAS MSS.

Need to establish a mechanism for periodic analysis of MSS and ESS user profiles

25. Periodic analysis of MSS and ESS user profiles is essential to assess and validate the quality of the underlying data.

26. There was no mechanism for periodic analysis of MSS profiles to identify possible data anomalies. Further, remedial activities for identified anomalies were not defined. OIOS' review of data in MSS showed the following anomalies:

(a) User roles for MSS were not defined. While the Pension Administration indicated that there should be only one role for users, OIOS noted five roles for MSS users (see Table 1 below) which indicated that ad hoc roles were created. Also, there was no clarity as to when these roles and scenarios were applicable, which led to inconsistent assignment of the roles.

Table 1: Examples of MSS user roles

Role name	Number of users with assigned role
100-Member User-Member User	135,638
100-Alt Payee-Alt payee	5,446
100-Member User-Member role +User 110-Alt Payee-Alt Payee role	4,829
100-Alt Payee-Alt Payee role + 110-Member User-Member User role	40
120-Member User-Member User	1

(b) MSS user information was incomplete (see Table 2 below). Certain required fields were not populated, or there was no standard naming convention for country names. The Pension Administration stated that it is developing guidance on country names for future reference.

Table 2: Examples of incomplete MSS user information

Field names	Gaps identified
Participant or beneficiary address missing	75,313 (53 per cent of the total users)
Inconsistent country naming standard	'Other', 'Stateless', 'Israel (Occupy Territory)', 'Occupied Palestinian Territory', '(Yugoslavia)', 'Macao' (list is indicative)

(c) There were anomalies in the age of users, and the living status of some users was not known (see Table 3 below). This indicated possible issues with data integrity. MSS user profile data needs to be reviewed, validated and cleaned.

Table 3: Examples of anomalies in MSS user profile

Fields	Number of cases
Age	374 above or equal to age 122
Login since account creation	740 (living status not known)

(d) Each user should only have one Unique ID. However, there were 58 cases of two or more active Unique ID for the same participant or beneficiary. The Pension Administration stated that actions to address and disable erroneous entries will continue as needed.

(e) Best practice is that where email ID is a mandatory requirement (such as in MSS), a unique email ID should be used to establish accountability, protect private and sensitive information, and prevent unauthorized access to an online resource. Also, use of common or generic email should be prohibited. OIOS' analysis of MSS users' email ID indicated instances of generic or common email IDs and no email IDs (even though it is a mandatory requirement) – see Table 4 below. Allowing the same email addresses to be used by multiple users indicated the lack of validation controls which is contrary to best practice and an impediment to secure multifactor authentication.

Table 4: Examples of MSS email management anomalies

Email management issue	Number of cases
Use of generic email for organizations	838 cases (Example: un.pension.id@undp.org: 26)
Use of common email for users	13 users with bashir.ebra@gmail.com 12 users with 7 users with akmsharfuddin@gmail.com 7 users with nilarko@gmail.com 7 users with mmamo@unicef.org; aghah@un.org
No email IDs (mandatory field)	Two active users

27. SPCs were given access to ESS, but there was no oversight of the user administration function for provisioning and de-provisioning. This was because there was a no established mechanism to get the information regarding the current membership of SPCs and SPC secretaries which changed quite often.

28. The Pension Administration had multiple authentication mechanisms for ESS. One method is the Active Directory, and the other is through access control lists within applications themselves. The latter is no longer a best practice, and the Fund may not have full visibility over user activities and timely de-provisioning of users. The Pension Administration stated that it is in the process of migrating users to cloud-based Microsoft Azure Directory. Periodic user access review and re-certification of users' in ESS was not institutionalized and depended on the availability of the one individual who was managing ESS.

(3) The Pension Administration should establish mechanisms for: (a) periodic analysis of Member Self-Service profiles and email IDs to identify and address data anomalies/ discrepancies; (b) periodic review of Employer Self-Service user access and re-certification; and (c) authenticating Employer Self-Service users against the Microsoft Azure Directory.

The Pension Administration accepted recommendation 3 and stated that the review of MSS user profiles and emails IDs will be included in the scope of the data quality action plan, as applicable. Also, the new user access portal will require the designated focal points from each member organization to certify the list of relevant users requiring access to ESS. Further, IMSS is already properly authenticating 'line of business' users against the Active Directory and using multi-factor tokens. Furthermore, access to ESS is controlled using whitelisted IP addresses from UNJSPF member organizations.

C. Information technology operations

Need to incorporate MSS in the disaster recovery exercise

29. The disaster recovery guidelines and procedures require that ICT service providers should develop, document and implement disaster recovery plans. These should include recovery time objectives and recovery point objectives for each system, restoration priorities, all roles, responsibilities, and up-to-date contact information of staff involved in recovery activities, detailed procedures and guidelines for restoration, and detailed list of all dependent subsystems/subcomponents.

30. The Pension Administration had identified its critical applications, as well as the recovery time objective and recovery point objective for each critical application. MSS was defined as a critical application in the IMSS Service Continuity and Availability Plan as well as IMSS Service Continuity and Recovery Procedures. However, the results of the last disaster recovery exercise conducted in September 2021 indicate that MSS was not part of the exercise. The lack of such testing may limit the availability of MSS and have an adverse impact on the Fund's clients.

(4) The Pension Administration should incorporate the Member Self-Service module in its disaster recovery exercises to assure its availability to clients.

The Pension Administration accepted recommendation 4 and stated that MSS disaster recovery test plan and test results will be provided to address the audit recommendation. Further, implementation of the recommendation requires the completion of the legal and procurement review of the statement of work for cloud services. The migration to cloud services will change the current disaster recovery strategy as 'all ICT services' will failover between data centres.

Need to strengthen service management for MSS

31. The service management process should include mechanisms for gathering, reviewing, updating and escalating existing and additional MSS related issues for timely resolution. The Pension Administration used iNeed as its service management application for logging in user requests or problems with MSS.

32. MSS service requests were raised by email, website, telephone or in-person. OIOS noted the following inconsistencies in resolution and closure of service requests which prevented Pension Administration from effectively monitoring and resolving the service requests:

(a) The status of service requests was categorized as cancelled, pending, open, resolved and closed.

(b) Clients who raised an issue were not notified about the status of resolution, even when their issue was not resolved but closed after a certain period of time.

(c) In some cases, the same issues were raised by clients a number of times at different time intervals, but they were not appropriately recorded in IPAS and the issue remained unresolved but closed (see examples in Table 5 below). In one instance, out of 11 requests for service opened relating to a death notification, only three were recorded in IPAS and closed, five requests were not recorded in IPAS, and three were cancelled and not recorded in IPAS.

Table 5: Same issue raised multiple times (closed, cancelled and not reflected in IPAS)

Agent_Pri	SR_Type	SR_Num	Title	Descriptic	SR_Source	Status	Sub_Area	Urgency	Assigned_	Assigned_	Actual_Start_Date
2-High	RFS	RFS-1-8132487264	Retiree/Be	0004448-	Web	Cancelled	Retiree/Be	Medium	HARTANT	UNJSPF Se	11/07/2020 20:22
2-High	RFS	RFS-1-8132487284	Retiree/Be	0004448-	Web	Closed	Retiree/Be	Medium	HARTANT	UNJSPF Se	11/07/2020 20:31
3-Mediun	RFS	RFS-1-8134898114	Retiree/Be	0004448-	Web	Closed	Retiree/Be	Medium	HARTANT	UNJSPF Se	15/07/2020 20:42
2-High	RFS	RFS-1-8138378736	0004448-	0004448-	Email	Closed	Retiree/Be	Medium	CONCORD	UNJSPF Se	21/07/2020 19:48
3-Mediun	RFS	RFS-1-8143410809	Retiree/Be	0004448-	Web	Closed	Retiree/Be	Medium	STANCU, I	UNJSPF Se	30/07/2020 06:48
2-High	RFS	RFS-1-8145627529	Retiree/Be	0004448-	Web	Closed	Retiree/Be	Medium	STANCU, I	UNJSPF Se	03/08/2020 17:59
2-High	RFS	RFS-1-8154165210	Mother pe	UID: 000-	Email	Closed	Retiree/Be	Medium		UNJSPF Se	14/08/2020 20:12
2-High	RFS	RFS-1-8158148189	Retiree/Be	0004448-	Web	Closed	Retiree/Be	Medium	STANCU, I	UNJSPF Se	20/08/2020 09:42
2-High	RFS	RFS-1-8158148309	Retiree/Be	0004448-	Web	Cancelled	Retiree/Be	Medium	STANCU, I	UNJSPF Se	20/08/2020 09:46
2-High	RFS	RFS-1-8158174719	Retiree/Be	0004448-	Web	Cancelled	Retiree/Be	Medium	STANCU, I	UNJSPF Se	20/08/2020 10:09
2-High	RFS	RFS-1-8162367235	Death of r	Hello dear	Email	Closed	Retiree/Be	Medium	STANCU, I	UNJSPF Se	24/08/2020 16:54

(5) The Pension Administration should strengthen service management for client requests by establishing a mechanism for: (a) providing feedback to clients on the status of resolution of their requests; and (b) recording and communicating the reasons for cancellation and closure of their requests.

The Pension Administration accepted recommendation 5 but stated that all clients receive feedback in response to their requests. Client Services' response to a query informs the client that the query is resolved. If no further communication is received from the client, within five days, the corresponding ticket automatically changes to closed status. For duplicate queries, Client Services answers the request with the latest date. Client Services does not currently communicate the reason for service request cancellation to clients to avoid diverting resources from the time dedicated to address actual queries. To address the recommendation, Client Services will assess the functionalities available in the new CRM system that is being procured and identify mechanisms to: (a) provide feedback to clients on the status of resolution of their requests, and (b) record and communicate the reason for cancellation and closure of client queries to the extent that is feasible.

D. Change management

Change management procedures were generally adequate

33. Formal change management procedures facilitate a standardized approach to handling all requests (including maintenance and patches) for changes to applications, procedures, processes, system service parameters, and the underlying platforms.

34. The Pension Administration managed its changes in a change management tool 'JIRA'. OIOS reviewed the changes requested for MSS and ESS and noted that: (a) change management procedures were being complied with; and (b) changes were being recorded and resolved in a timely manner based on the nature of the change required. OIOS therefore concluded that change management procedures related to MSS and ESS were generally adequate.

E. Vulnerability management

Vulnerability management was generally adequate

35. Organizations should conduct continuous vulnerability assessments of their people, processes and technology (including ICT infrastructure, applications and systems) to proactively discover, analyze and remediate cybersecurity vulnerabilities.

36. The Pension Administration is part of the common secure programme managed by a United Nations entity. It also relies on the threat intelligence information provided by a third-party security service provider. The Pension Administration had implemented a vulnerability management process which included monthly vulnerability scans of its virtual local area networks and websites. Further, an advanced ethical hacking exercise was conducted to identify possible weaknesses in its information assets and determine deviations from its security policies that could potentially materialize into a security incident. The Pension Administration had an established process for conducting monthly vulnerability assessment with the support of a third-party service provider.

37. The websites of MSS and ESS were scanned monthly for potential vulnerabilities, which were of low impact and informational in nature. The Pension Administration stated that it prioritizes the high

criticality and medium severity vulnerabilities, and low and information vulnerabilities are noted for future remediation.

IV. ACKNOWLEDGEMENT

38. OIOS wishes to express its appreciation to the Management and staff of the Pension Administration of UNJSPF for the assistance and cooperation extended to the auditors during this assignment.

Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of [audit title]

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	The Pension Administration should: (a) document its assessment of the desired future state of the Employer Self-Service and Member Self-Service modules considering the other new initiatives in progress; and (b) clarify the roles and responsibilities for the Employer Self-Service module and mitigate the business continuity risk arising from assignment of functions to one staff member.	Important	O	Receipt of evidence that: (a) assessment of the desired future state of the ESS and MSS modules have been documented considering the other new initiatives in progress; and (b) the roles and responsibilities for the ESS module have been clarified, and the business continuity risk arising from assignment of functions to one staff member has been mitigated.	31 July 2024
2	The Pension Administration should strengthen mechanisms for identity proofing and authentication of participants and beneficiaries and the digital documents uploaded by them through the Member Self-Service module.	Important	O	Receipt of evidence that the mechanisms for identity proofing and authentication of participants and beneficiaries and the digital documents uploaded by them through MSS have been strengthened.	31 December 2023
3	The Pension Administration should establish mechanisms for: (a) periodic analysis of Member Self-Service profiles and email IDs to identify and address data anomalies/ discrepancies; (b) periodic review of Employer Self-Service user access and re-certification; and (c) authenticating Employer Self-Service users against the Microsoft Azure Directory.	Important	O	Receipt of evidence that mechanisms have been established for: (a) periodic analysis of MSS profiles and email IDs to identify and address data anomalies/discrepancies; (b) periodic review of ESS user access and re-certification; and (c) authenticating ESS users against the Microsoft Azure Directory.	31 December 2024
4	The Pension Administration should incorporate the Member Self-Service module in its disaster recovery exercises to assure its availability to clients.	Important	O	Receipt of evidence that the MSS module has been included in the disaster recovery exercises to assure its availability to clients.	31 December 2024
5	The Pension Administration should strengthen service management for client requests by	Important	O	Receipt of evidence that the Pension Administration has strengthened service	31 December 2024

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

STATUS OF AUDIT RECOMMENDATIONS

Audit of [audit title]

	establishing a mechanism for: (a) providing feedback to clients on the status of resolution of their requests; and (b) recording and communicating the reasons for cancellation and closure of their requests.			management for client requests by establishing a mechanism for: (a) providing feedback to clients on the status of resolution of their requests; and (b) recording and communicating the reasons for cancellation and closure of their requests.	

APPENDIX I

Management Response

UNITED NATIONS **NATIONS UNIES**

UNITED NATIONS JOINT S TAFF PENSION FUND
CAISSE COMMUNE DES PENSIONS DU PERSONNEL DES NATIONS UNIES

NEW YORK (Headquarters)
P.O. Box 5036, UNITED NATIONS, N.Y., N.Y. 10017
Tel: (212) 963 -6931; Fax: (212) 963 -3146
E -mail: UNJSPF@UN.ORG
Cable: UNATIONS NEWYORK
Web: http://www.unjspf.org

OFFICE AT GENEVA
c/o PALAIS DES NATIONS
CH - 1211, Geneva 10
Tel: +41 (0) 22 928 8800; Fax: +41 (0) 22 928 9099
E -mail: UNJSPF.GVA@UNJSPF.ORG
Web: http://www.unjspf.org

MEMORANDUM

Ref: New York, 1 March 2023

To / A: Mr. Gurpur Kumar, Deputy Director Internal Audit Division, OIOS

From / De : Rosemarie McClean, Chief Executive of Pension Administration, United Nations Joint Staff Pension Fund

Subject / Objet: **UNJSPF response to draft report audit of the Integrated Pension Administration System's Member Self-Service and Employer Self-Service modules in the United Nations Joint Staff Pension Fund (Assignment No. AS2022-800-02)**

1. Reference is made to your memorandum dated 15 February 2023, in which you submitted for the Fund's review and comments, the draft report of the above-mentioned audit.

2. As requested, the Pension Administration's action plan to address the audit recommendations is included in **Annex I**. Factual corrections and clarifications are provided in **Annex II**.

3. The Pension Administration would like to thank OIOS auditors for the constructive exchanges with management.

cc.: Mr. D. Penklis, Deputy Chief Executive
Mr. K. Soll, Chief Financial Officer
Mr. D. Dell'Accio, Chief Information Officer
Ms. M. O'Donnell, Chief of Operations
Mr. A. Blythe, Chief Client Services
Ms. K. Manosalvas, Risk Officer, Audit Focal Point

ANNEX I

Audit Recommendations Audit of the Integrated Pension Administration System's Member Self-Service and Employer Self-Service modules in 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	The Pension Administration should: (a) document its assessment of the desired future state of the Employer Self-Service and Member Self-Service modules considering the other new initiatives in progress; and (b) clarify the roles and responsibilities for the Employer Self-Service module and mitigate the business continuity risk arising from assignment of functions to one staff member.	Important	Yes	IMSS, Client Services, Financial Services	July 2024	a) The desired future state for Member Self-Service (MSS) is documented in the Project Initiation Document (PID) of the Customer Relationship Management (CRM) project, as approved by the Pension Board in July 2021. The PID provides the context, background, and details on the UNJSPF Strategy, Future State (to-be), and Functional Specifications. Based on an assessment with IPAS vendor, it was determined that the ESS Module could not be used to submit separation documents due to technical limitations. Therefore, the Fund decided to limit the use of the ESS Module to receive ASHI authorizations and ASHI Import files for Financial Services. To address the audit recommendation, CRM project documents – including the future state of MSS and ESS - will continue to be updated as required. b) A User Access Portal (UAP) will be deployed, which will enable designated Focal Points, i.e., SPCs and Unit/Section Chiefs, to submit a user maintenance request. The UAP requires a minimum of two PA business owners for administering the Focal Points. The Focal Point, during the logoff process, will be required to confirm that all listed users under his/her control are still valid users. The UAP access will require Focal Points to use VPN or Citrix Workspace to gain access. In addition, IMSS ESU will conduct an annual user recertification exercise.
2	The Pension Administration should strengthen mechanisms for identity proofing and authentication of participants and beneficiaries and the digital documents uploaded by them	Important	Yes	Enterprise Security Unit	December 2023	The audit recommendation will be addressed with the implementation of a multi-factor authentication (MFA) to IPAS member self-service.

[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.

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	through the Member Self-Service module.					
3	The Pension Administration should establish mechanisms for: (a) periodic analysis of Member Self-Service profiles and email IDs to identify and address data anomalies / discrepancies; (b) periodic review of Employer Self-Service user access and re-certification; and (c) authenticating Employer Self-Service users against the Microsoft Azure Directory.	Important	Yes	All business functions and IMSS	December 2024	a) The review of MSS user profiles and email IDs will be included in the scope of the data quality action plan, as applicable. b) The new User Access Portal will require designated Focal Points from each member organization, during the log-off process, to certify that the list of relevant users still require access to ESS. In addition, IMSS ESU will continue conducting the annual user recertification exercise. c) IMSS is already properly authenticating LOB users against Active Directory and using multifactor authentication tokens. Furthermore, access to ESS is controlled using whitelisted IP Addresses from UNJSPF member organizations.
4	The Pension Administration should incorporate the Member Self-Service module in its disaster recovery exercises to assure its availability to clients.	Important	Yes	Enterprise Operations Unit / Risk Management	December 2024	MSS Disaster Recovery test plan and test results will be provided to address the audit recommendation. The implementation of the recommendation requires the completion of the legal and procurement review of the Statement of Work for Cloud Services. The migration to Cloud Services will change the current disaster recovery strategy as 'all ICT services' will failover between data centers.
5	The Pension Administration should strengthen service management for client requests by establishing a mechanism for: (a) providing feedback to clients on the status of resolution of their requests; and (b) recording and communicating the reasons for cancellation and closure of their requests.	Important	Yes	Client Services	December 2024	All clients receive feedback in response to their requests. Client Services (CS) response to a query, informs the client that the query is resolved. If no further communication is received from the client, within five days, the corresponding ticket automatically changes to closed status. For duplicate queries, CS answers the request with the latest date. CS does not currently communicate the reason for service request cancellation to clients to avoid diverting resources from the time dedicated to address actual queries. To address the recommendation, Client Services will assess the functionalities available in the new CRM system that is being procured and identify mechanisms to: (a) provide feedback to clients on the status of resolution of their requests. (b) record and communicate the reason for cancellation and closure of client queries to the extent that is feasible.

ANNEX II
Factual Corrections or Clarifications to the Audit Report

1. **Paragraphs 13-15 Contributions:** ESS is used by the Fund's Member Organizations to submit ASHI files. The Pension Administration decided not to use ESS for the handling of contributions data and implemented instead Financial Interfaces, which provide the required testing environment and enable the monthly reconciliation of contributions. ESS does not have automated features to record mass entries or mass updates, which are done by the Interface. The decision to implement the Financial and HR Interfaces through the Middleware to IPAS, without using MSS, allowed streamlining the collection of HR and Financial Data from the multiple ERP systems of Member Organizations.

2. **Paragraph 15 – Access to ESS Module:** Access to ESS portal is performed in a secure area. Access to ESS is controlled by Firewall, users can only log-in from whitelisted IP Addresses i.e., UNJSPF member organizations. Staff working remotely can only access ESS via either VPN or Citrix Workspace, both requiring an Active Directory account that uses multifactor authentication tokens.

3. **Paragraph 16 – ESS Module Roles and responsibilities:** Access to ESS module is granted by IMSS Service Desk while the Enterprise Security Unit conducts an annual user recertification exercise. A staff member in Financial Services controls and validates user lists and access requests for ESS.

4. **Paragraph 17d MSS secure mailbox:** The document upload via MSS Secure mailbox was implemented in 2020, prior to the adoption of the Kofax Total Agility solution. Kofax Total Agility project requirements were revised to incorporate the Upload feature via MSS Secure mailbox. This integration created efficiencies by allowing uploaded documents to be auto scanned into V3 through a batch process and reducing manual work.

5. **Paragraph 18 Enhancements to MSS:** The enhancements to MSS module were not implemented in ad hoc manner but as part of the Fund's overall CARE strategy. The Fund's paperless strategy envisioned in the CARE Strategy Pillars One and Two, has guided the enhancements implemented to make MSS module more client friendly.

6. **Paragraph 21a Changes in personal information through MSS:** The Fund is further securing MSS with the implementation of multifactor authentication prior to enabling the Online Submission process via MSS module.

7. **Paragraph 21d Certificate of Entitlement for Two-track beneficiaries:** To expedite the process, beneficiaries on the two-track can submit their Certificate of Entitlement (CE) using the Digital Certificate of Entitlement or can return their signed certificate using the MSS upload. Beneficiaries cannot download the CE from MSS due to the need to verify the country of residency through the receipt of the CE document at the physical address.

8. **Paragraph 21e Automated processing for documents in MSS repository:** Manual intervention for extracting, uploading, and indexing the documents uploaded in MSS into IPAS' has been automated with the integration of the MSS Upload feature with Kofax Total Agility. Currently, the documents arrive to Kofax through an automatic scan and are auto indexed using the MSS UID. Records Management staff validates the indexation to complete the process. V3 system auto-closes the Workflow once the documents are processed.

9. **Paragraph 22 Signature verification.** The process has been strengthened with the implementation of the Kofax Total Agility solution in December 2022. Currently, forms uploaded via MSS that contain signatures are processed through the automated signature verification feature.

10. **Paragraphs 26a and 28:** The Pension Administration notes that there are only two roles in MSS: Member user and Alt Payee (Dependents). In addition, a user can be a dependent and member if the spouse works for the UN, in which case the role order will depend on what the member was before member or dependent. A process is in place for the verification of ESS users.