INTERNAL AUDIT DIVISION

REPORT 2020/020

Audit of data governance, management and reporting in the Pension Administration of the United Nations Joint Staff Pension Fund (Assignment No. AT2020-800-01)

The Pension Administration needs to implement a data governance and management framework with clearly assigned roles and responsibilities for data ownership and stewardship

8 September 2020
Assignment No. AT2020-800-01

Audit of data governance, management and reporting in the Pension Administration of the United Nations Joint Staff Pension Fund

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of data governance, management and reporting in the Pension Administration of the United Nations Joint Staff Pension Fund (UNJSPF). The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over data governance, data management and reporting in the Pension Administration of UNJSPF. The audit covered the period from January 2018 to December 2019. Based on an activity-level risk assessment, the audit covered risks areas in data management, governance and reporting which included: (a) data governance and management; (b) data quality; (c) data privacy, confidentiality and security; and (d) reporting.

The Pension Administration needs to implement a data governance and management framework with clearly assigned roles and responsibilities for data ownership and stewardship.

OIOS made eight recommendations. To address issues identified in the audit, the Pension Administration needed to:

- Define and implement a data governance and management framework; document the enterprise-wide inventory of its data assets, and clearly assign roles and responsibilities over data ownership and stewardship;
- Establish a comprehensive data quality policy and quality improvement plan, establish data quality metrics, and develop a plan to train staff on data quality management;
- Undertake a comprehensive risk assessment of data privacy and classification for its data assets, implement and embed privacy management standards in business processes and information systems, and define a retention policy and schedule for its documents and records;
- Expand the incident management procedure to include reporting of events related to data and information and inform users of the amended procedure;
- Address information and communications technology security weaknesses identified and develop security baselines for its systems to ensure the effectiveness of external network security monitoring services;
- Complete the documentation on business intelligence design and data models and publish the methodology for the benefits benchmark calculation dashboard;
- Ensure that business intelligence user requirements are comprehensively documented, and testing strategies are defined, complete with testing scenarios, to validate the reliability of business intelligence reports and dashboards; and
- Facilitate timely access to business intelligence, ensure adequate protection of data downloaded from business intelligence systems on to end-user systems, and develop a comprehensive plan to train staff and member organizations on business intelligence.

The Pension Administration accepted the recommendations and has initiated action to implement them.

CONTENTS

Audit of data governance, management and reporting in the Pension Administration of the United Nations Joint Staff Pension Fund

I.   BACKGROUND

1.   The Office of Internal Oversight Services (OIOS) conducted an audit of data governance, management and reporting 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 UNJSPF. It is administered by the United Nations Joint Staff Pension Board.

3.   As of December 2019, UNJSPF serviced 131,538 participants and 79,975 beneficiaries-retirees. UNJSPF facilitated payment of periodic benefits worth $2.7 billion and collected $2.68 billion annually from member organizations and participants. Benefits were paid in over 190 countries in various currencies.

4.   UNJSPF generated, collected, used, processed and retained a wide variety of data and records, including business, financial data and personally identifiable information. The data and records were collected from several sources, namely, member organizations, individuals, employees, and vendors using several information and communications technology (ICT) systems including the Integrated Pension Administration System (IPAS), interfaces, paper-based forms and electronic mail. Additionally, the Pension Administration internally generated data and maintained the data and records in various databases and file systems.

5.   The Pension Administration participated in the Digital and Technology Network of the United Nations High-Level Committee on Management which adopted 10 principles for personal data protection and privacy at its 36th meeting in October 2018.

6.   Comments provided by the Pension Administration 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 data governance, management and reporting in the Pension Administration of UNJSPF.

8.   This audit was included in the 2020 risk-based work plan of OIOS due to risks associated with data governance, management and reporting, and their potential implications for UNJSPF.

9.   OIOS conducted this audit from January to May 2020. The audit covered the period from January 2018 to December 2019. Based on an activity-level risk assessment, the audit covered risks areas in data management, governance and reporting which included: (a) data governance and management; (b) data quality; (c) data privacy, confidentiality and security; and (d) reporting.

10.   The audit methodology included: (a) interviews with key personnel; (b) review of documentation; (c) analytical review of data; (d) ICT security tests; and (e) survey of member organizations and staff. The audit scope did not include review of the management of data in Umoja (the enterprise resource planning

system of the United Nations Secretariat) and the human resources system (Inspira) which were used by the Pension Administration to carry out some operational activities related to procurement, human resources, travel and financial record-keeping.

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

III.   AUDIT RESULTS

A.   Data governance and management

<u>Lack of a data governance and management framework</u>

12.   Best practices define data governance as exercising authority and control over the management of data assets[1]. Data governance ensures that data and information are consistently defined and understood across the enterprise. While data governance defines organizational structures, data owners, policies, rules, processes, business terms, and metrics for the end-to-end lifecycle of data, data management is the technical implementation of data governance. A typical data governance and management framework includes establishing: (i) data strategy and oversight; (ii) data standards and quality; (iii) data security; and (iv) reporting.

13.   Though the Pension Administration had consistently rated 'data management' as a high-risk area in its enterprise risk register, due to issues related to data quality and accuracy, it had not taken steps to mitigate this risk by developing a data strategy within a defined data governance and management framework. In 2009, the Pension Administration had hired an external consultant to conduct a workshop with management to develop policies on data governance and quality, but it did not carry the initiative further. The lack of defined data governance and management mechanisms caused the following gaps:

(i)   The terms of reference for existing information governance mechanisms did not include data governance and management to facilitate stewardship and oversight. The Pension Administration had an Information Technology Executive Committee chaired by the Chief Executive, and the Information Technology Steering Committee comprising of middle management. However, these committees did not take an integrated view of data across the Pension Administration. The Pension Administration needs to leverage the existing committees to establish a data governance and management framework. Also, a related OIOS survey on data governance and management with UNJSPF's member organizations[2] showed that 15 member organizations expected the Pension Administration to implement a data governance and management framework.

(ii)   There was lack of clarity on data ownership which created ambiguity over the responsibility for ensuring timely resolution of data inaccuracies. For example, the Accounts Section considered the participant contract data to be under its ownership and desired to have the ability to correct the data to expedite processing. However, it could not do so because all requests for correction of data had to be processed through the Pension Entitlement Services Section.

(iii)   A data asset inventory was not documented to facilitate timely oversight and protection of data as an asset and disclose its value to the Pension Administration and its stakeholders. Initial steps to document the data inventory were taken during the audit. As of April 2020, the Pension Administration had identified

---

[1] Data assets refer to a system, application output file, document, database, or web page that is used to generate value to stakeholders.

[2] The OIOS survey was sent to all 24 member organizations (including four United Nations entities). OIOS received 18 completed responses.

239 data assets. This initial data inventory could serve as a starting point for developing a data governance and management framework.

(iv)   The Pension Administration had a portfolio of 25 ICT applications which required documentation of the respective data models. However, there were no formalized data models and data definitions for the conceptualization of data for use in business intelligence (BI), analytics and decision making. Further, there were no tools for updating and storing the data models. For example, the IPAS vendor provided the Pension Administration with a generic model that did not reflect actual implementation. This gap hindered the Pension Administration's ability to develop an effective BI system. Similarly, the Pension Administration did not document the metadata and master data for its Financial Reporting system.

14.   Absence of a data governance and management framework could adversely affect stewardship and oversight of the data assets and result in data errors, processing delays, and poor client satisfaction.

---

(1)   The Pension Administration of UNJSPF should: (i) define and implement a data governance and management framework; (ii) document the enterprise-wide inventory of its data assets; and (iii) clearly assign roles and responsibilities over data ownership and stewardship.

The Pension Administration accepted recommendation 1 and stated that the Information Technology Executive Committee will include the definition and implementation of a data management framework in the list of priorities. The Pension Administration will complete an inventory of its data assets, which will serve as a basis to identify data owners and data stewards. Recommendation 1 remains open pending: (i) implementation of a data governance and management framework; (ii) documentation of an enterprise-wide inventory of data assets; and (iii) assignment of roles and responsibilities for data ownership and stewardship.

B.   Data quality

Lack of data quality policy and data quality management

15.   A data quality programme should include concepts and practices to improve data quality. Best practices include data quality policies and guidelines, data quality measurement, data cleansing and correction, data quality process improvement, and data quality education. Public pension funds, as best practice, also embrace data quality as a critical aspect of their operations.

16.   The Pension Administration lacked an integrated approach to data quality management specifying the quality metrics and budget for ensuring data quality. It developed a quality policy in 2002-2003 but abolished it in 2017. There were no adequate mechanisms or a data quality improvement plan to ensure that data quality procedures were embedded into the services provided to its stakeholders. The following gaps were noted:

(i)   Problems with data quality had been a constant drain on resources since the implementation of IPAS in 2015. There was a constant need to apply data fixes to IPAS for correcting data errors. Between April 2019 and February 2020, 85 data fixes were designed, 44 of which were open as of April 2020 for deployment. Further, a recommendation of the Board of Auditors (A/73/5/Add.16, chapter II, para. 36) that the Pension Administration undertake a data cleansing exercise, identify and close all the workflows that remained open owing to issues in IPAS was still under implementation.

(ii)   An expression of interest issued by the Pension Administration in September 2019 for an independent assessment of IPAS requested by General Assembly resolution 73/274 did not specifically include an evaluation of data quality, which would have enabled the Pension Administration to validate the quality of data contained in IPAS. Upon inquiry, the Pension Administration stated that it will include data quality in the review.

(iii)   To facilitate data collection from stakeholders and ensure the quality of the data provided, the Pension Administration had established various procedures and forms. However, it did not have adequate mechanisms to periodically review and update these procedures and forms. For instance, there were 74 procedure manuals ('procedures general') used for pension administration in the legacy systems which had not been updated to reflect changes due to the implementation of IPAS. Therefore, workflow processes and data were prone to errors.

(iv)   Data interfaces had been a constant source of data errors and remained continuously under improvement. There were 31 known issues (e.g., duplicated unique identification numbers) related to data interfaces in various stages of remediation. Five recommendations made in a previous OIOS audit of data interfaces and monthly contributions in UNJSPF (Report 2019/038) were still under implementation.

(v)   Problems with data quality were also a source of concern for the Fund's member organizations. In response to a related survey question, 7 member organizations stated that the quality of data in relation to their entity in IPAS needed to be improved. The comments received indicated various problems with data interfaces (e.g., spouses and dependents not captured, long time taken to migrate the data from the interface staging database into IPAS, and error messages). The Pension Administration stated that it was taking action to bring dependent information into IPAS.

(vi)   OIOS conducted several data quality tests through 28 queries in IPAS. The results showed that the Pension Administration needs to cleanse and improve data quality in IPAS. Data discrepancies included persons with duplicate unique identification numbers, incorrect participant status, active participants assigned a date of death, deceased persons without date of death, open workflows for change of address, 742 pending forfeitable[3] withdrawal settlements worth $3.4 million (reasons for delay for these settlements could not be confirmed), and 5,309 cases[4] with missing mandatory documents required for processing pension application (as of April 2020, 2,875 cases out of 5,309 were more than one year old).

(vii)   The lack of data quality was also noted in external communications and e-mail addresses used by Pension Administration to send out its monthly newsletters. For instance, there was the publication of an article on the digital certificate of entitlement project by the ICT vendor of the Pension Administration which disclosed the name of a participating member organization prior to signing a formal agreement. Further, the Pension Administration did not have adequate procedures to review the quality of email addresses used for sending out its monthly newsletters to remove fake and invalid addresses.

(viii)   Data completeness is vital for establishing and maintaining high data quality. Therefore, rigorous and transparent verification processes are required to ensure the quality (i.e., completeness and accuracy) of data, without which the data cannot be relied upon. Further, information in the grievance redressal system (iNeed) was incomplete because it was being used only in the Fund's New York Office but not at its Geneva Office. Additionally, the queries received through e-mails before implementing iNeed were not migrated into the iNeed system. The Pension Administration also did not consider collection and use of

---

[3] Article 46 (a) of the UNJSPF regulations specifies that the right to a withdrawal settlement or residual settlement shall be forfeited if for two years after payment has been due the beneficiary has failed to submit payment instructions or has failed or refused to accept payment.
[4] The number of cases with one of the missing mandatory documents required for processing the pension application had decreased from a high of 16,427 in 2017 to 5,309 as of April 2020.

data in languages other than its official working languages. This prevented it from providing adequate responses to queries received in languages other than the official working languages.

17.   The absence of a comprehensive data quality policy and quality improvement programme could cause data errors, processing delays, and necessitate frequent correction of data errors.

> **(2)   The Pension Administration of UNJSPF should: (i) establish a comprehensive data quality policy and quality improvement plan; (ii) establish data quality metrics; and (iii) develop a plan to train staff on data quality management.**
>
> *The Pension Administration accepted recommendation 2 and stated that it will issue a data quality policy and develop and implement a data quality improvement plan to provide proper coordination, guidance, quality measurement and training for data clean-up and improvement actions. Recommendation 2 remains open pending receipt of evidence of the: (i) implementation of a data quality policy and quality improvement plan; (ii) establishment of data quality metrics; and (iii) development of a staff training plan on data quality management.*

C.   Data privacy, confidentiality data security

Need to strengthen controls on data privacy and confidentiality

18.   Data privacy, confidentiality and security are integral to a data governance and management framework. The Secretary-General's bulletin ST/SGB2007/6 (Information Sensitivity, Classification, and Handling) requires the classification and secure handling of confidential information. Further, in 2018, the High Level Committee on Management adopted the 10 principles on personal data protection and privacy and encouraged United Nations organizations to implement appropriate administrative, physical and technical safeguards to protect the security of personal data, including against unauthorized or accidental access, damage, loss or other risks presented by data processing. The Pension Administration also adopted the information security standard ISO 27001 which broadly recommends the classification of data in accordance with their legal requirements, value, criticality and sensitivity so that data may be used and protected more efficiently.

19.   The Pension Administration had consistently rated the risks related to data privacy, confidentiality and security as high in its enterprise risk register. However, the rationale for the high-risk rating was not based on any formal or comprehensive risk assessment of data privacy. A data classification and handling policy issued in October 2013 was never implemented. In the absence of a formal data classification policy, the required data protection controls were not applied, as the sensitivity of the data that required protection was unspecified. The Pension Administration stated that it considered all data and information as 'confidential'. However, OIOS noted a lack of common understanding among staff on confidentiality which caused inconsistent treatment of similar data sets. Moreover, the need for transparency in appropriate situations may be compromised by summarily classifying all data and information as confidential.

20.   Lack of data privacy risk assessment and undefined classification procedures caused the following:

(i)   There was no consistent practice regarding the tagging/marking of data, documents, records and information that needed to be classified. For example, some ICT policies were marked as confidential while the minutes of the quarterly senior management meetings were not marked. Similarly, there was no standard practice to classify emails based on their content, and data stored in databases were also not tagged and classified. Without data being tagged or marked, appropriate protection cannot be applied. For instance, personally identifiable medical information stored in IPAS was visible to anyone with basic access

to the system; banking information, certificates and passport images were stored in the iNeed system without any retention period; and sensitive and personal data was present on several shared network drives of the Pension Administration.

(ii)   Policies for managing the Pension Administration's website and social media accounts needed to be defined to facilitate the privacy of content. OIOS noted that the Pension Administration did not have a cookie policy on its website to obtain user consent for tracking activity and also did not consistently use privacy notices on its website and for email communications.

(iii)   Data privacy requirements and controls should be extended to data shared with third parties, e.g., vendors and other service providers. The Pension Administration had a portfolio of 111 vendors (2019-2020). Some of these vendors provided services that required storing sensitive and personal information in vendors' systems and premises (e.g., network security operations service provider (SOC) and the consulting actuary). No analysis was undertaken to identify the vendors that stored personal and sensitive information of the Pension Administration on their systems, and how the Pension Administration would be notified in case of any loss or breach of such data.

(iv)   The Pension Administration's incident management procedure did not provide guidance on how to manage incidents related to loss, theft or unauthorized disclosure, modification or destruction of private and confidential information from ICT systems, mobile devices, hardcopies (paper/files) or sensitive data with vendors. Though the Pension Administration stated that the scope of the contract with the SOC service provider included information leak detection, this aspect still needed to be included in the overall incident management policy and also communicated to all users.

(v)   The Pension Administration also lacked a document retention policy (required according to the Secretary-General's bulletin ST/SGB/2007/5). The absence of a retention policy poses the risk of costly e-discovery[5] of historical documents, lagged system performance, risk of data loss or theft, and costly storage space.

> **(3)   The Pension Administration of UNJSPF should: (i) undertake a comprehensive risk assessment of data privacy and classification for its data assets; (ii) implement and embed privacy management standards in business processes and information systems; and (iii) define a retention policy and schedule for its documents and records.**
>
> *The Pension Administration accepted recommendation 3 and stated that it will undertake a data classification exercise. The results will be considered to assess and enhance related business and information systems controls. It further stated that it will formalize the retention policy for documents and records.* Recommendation 3 remains open pending the receipt of: (i) a comprehensive risk assessment of data privacy and classification for data assets; (ii) implementation of privacy management standards in business processes and information systems; and (iii) a retention policy and schedule for documents and records.
>
> **(4)   The Pension Administration of UNJSPF should expand the incident management procedure to include reporting of events related to data and information and inform users of the amended procedure.**

---

[5] Electronic discovery is identifying, collecting and producing electronically stored information. It includes, but is not limited to, emails, documents, presentations, databases, voicemail, audio and video files, social media, and web sites.

The Pension Administration accepted recommendation 4 and stated that it will update the incident management policy and procedure to cover incidents related to loss, theft, or unauthorized disclosure, modification or destruction of data and information. Recommendation 4 remains open pending receipt of: (i) an updated incident management procedure; and (ii) evidence that users have been informed of the amended incident management procedure.

Need to strengthen controls on data security controls

21.	OIOS audits in the past had pointed out several areas that required strengthening of data security. Data security in the Pension Administration was considered primarily as an ICT issue. Adequate controls cannot be prioritized in the absence of a data asset inventory, data classification policy and data privacy risk assessment.

22.	███
██

███
██

███
███
██

██
███
███
███

███
███
███
███

███
███
███
████████████████

23.   Lack of data security integration with data governance and management could also hamper data availability. In 2020, the Pension Administration lost access to BI and the SharePoint data storage service for over 21 hours due to a failure in the critical infrastructure. The incident breached the Pension Administration's service availability targets and also corrupted the IPAS disaster recovery database. A similar incident had occurred in the same infrastructure in 2017.

> **(5)   The Pension Administration of UNJSPF should: (i) address the ICT security weaknesses identified; and (ii) develop ICT security baselines for its systems to ensure the effectiveness of external network security monitoring services.**
>
> *The Pension Administration accepted recommendation 5 and stated that it will consider the aspects identified by OIOS to further strengthen data security controls. It also stated that it is developing a security baseline with regard to threat events that could impact its information systems. Metrics are being defined and configured within the context of SOC services.* Recommendation 5 remains open pending receipt of evidence that: (i) ICT security weaknesses identified in the current report have been addressed; and (ii) ICT security baselines have been developed.

D.   Reporting

Need to strengthen controls over BI reporting

24.   BI provides decision support data and allows users at all levels in an organization to access, interact with, and analyze data to manage the business, improve performance, discover opportunities, and operate efficiently. The success of BI to assist management in decision-making depends on its proper governance (design, documentation, reliability, access, availability, security and training).

25.   In the absence of a data governance and management framework, the Pension Administration lacked a well-defined BI strategy. There was no underlying mechanism to assess the data required, and translating the data into actionable information for decision-making to serve the stakeholders efficiently. BI was in the early stages of deployment as of April 2020. This gap caused the following:

(i)   A comprehensive user requirement document compiling BI requirements from staff and member organizations had not yet been established. Several staff knew of the BI initiative but provided no inputs

---

[6] Active directory is a Windows Operating System directory service that facilitates working with interconnected, complex and different network resources in a unified manner.

into its design. Also, some member organizations commented on the limited understanding/training on the features of BI and inaccuracies in the pension reconciliation exception (PRE) report.

(ii)   There was lack of documentation on BI design and data models which prevented effective use of reports and loss of knowledge due to attrition of a key BI developer. Further, the lack of documentation also hampered the interpretation of BI results to users and stakeholders. For example, the logic behind the BI model used for calculating the 15-day benchmark performance was not published with the benchmark performance numbers so that users could properly understand the logic and assumptions behind this calculation. Publishing the benchmark calculation logic is important because General Assembly resolution 73/274 tied the performance of senior management, in part, to the performance benchmark.

(iii)   The Pension Administration also lacked a comprehensive user acceptance testing strategy and documentation to test the reliability of BI. Eighteen out of the 20 acceptance tests were completed by only two business users from the New York Office. BI reports sometimes required manual intervention and correction. As noted under section B of the present report, IPAS still contained some poor-quality data which could render BI unreliable.

(iv)   Several users in member organizations did not have access to BI. Responses to the OIOS survey showed that 10 of the 18 member organizations that responded did not have access to BI. The access portal to provision user access was still under development.

(v)   The Pension Administration had not assessed the controls required on the BI data downloaded in the end-user systems (desktops, laptops, drives and mobile devices) in Excel format. BI data once downloaded in Excel had no protection (e.g., password protection) or auditability (how it has been modified or circulated further).

(vi)   The Pension Administration has not established a proper training plan for BI. Though some presentations and demonstrations had been made to users and member organizations, a proper training plan and calendar still needed to be established.

(vii)   The Pension Administration stated that it was developing a BI dashboard that is expected to assist in data cleansing. However, without clearly defined data quality metrics, this dashboard may be of limited use. The Pension Administration also stated that it was working on additional data interface projects to improve data quality such as: (a) the monthly contributions reconciliation interface designed to reconcile financial contributions and address exceptions; (b) the separations interface project designed to receive correct separation documents in a timely manner; and (c) the attachments interface designed to receive verified attachments like birth certificates. However, most of these projects were in early stages of development.

> **(6)   The Pension Administration of UNJSPF should: (i) complete the documentation on business intelligence design and data models; and (ii) publish the methodology for the benefits benchmark calculation dashboard.**
>
> *The Pension Administration accepted recommendation 6 and stated that it will complete the documentation of BI, including the data model, which is in progress. The methodology for the calculation of the benefit processing benchmark was endorsed by the Chief Executive. The methodology will be referenced in the BI dashboard as well as in reports disclosing the benefit benchmark results.* Recommendation 6 remains open pending receipt of evidence that: (i) BI design and data models have been documented; and (ii) the methodology for the benefits benchmark calculation dashboard has been published.

> **(7)** **The Pension Administration of UNJSPF should ensure that: (i) business intelligence user requirements are comprehensively documented; and (ii) testing strategies are defined, complete with testing scenarios, to validate the reliability of business intelligence reports and dashboards.**
>
> *The Pension Administration accepted recommendation 7 and stated that it will ensure that the development of BI dashboards is aligned with the established system development methodology, and that comprehensive testing is applied prior to deployment.* Recommendation 7 remains open pending receipt of evidence that: (i) user requirements for BI have been comprehensively documented; and (ii) a testing strategy has been defined, complete with testing scenarios, to validate the reliability of BI reports and dashboards.
>
> **(8)** **The Pension Administration of UNJSPF should: (i) facilitate timely access to business intelligence; (ii) ensure adequate protection of data downloaded from business intelligence systems on to end-user systems; and (iii) develop a comprehensive plan to train staff and member organizations on business intelligence.**
>
> *The Pension Administration accepted recommendation 8 and stated that: (i) a new SharePoint based user access site is under development and in the meantime, access is granted through the Service Desk; (ii) the implementation of Power BI will enable to control the download and export function; (iii) a user guide for the Power BI tool is available online; and (iv) additional training will be provided as requested.* Recommendation 8 remains open pending receipt of evidence that: (i) a SharePoint user access site has been developed to facilitate timely access to BI; (ii) controls for protection of data downloaded from the BI system on to end-user systems have been established; and (iii) a comprehensive plan has been developed to train staff and member organizations on BI.

IV. ACKNOWLEDGEMENT

26. 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.

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

STATUS OF AUDIT RECOMMENDATIONS

Audit of data governance, data management and reporting in the Pension Administration of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[7]/ Important[8]	C/ O[9]	Actions needed to close recommendation	Implementation date[10]
1	The Pension Administration of UNJSPF should: (i) define and implement a data governance and management framework; (ii) document the enterprise-wide inventory of its data assets; and (iii) clearly assign roles and responsibilities over data ownership and stewardship.	Important	O	(i) Implementation of a data governance and management framework; (ii) documentation of an enterprise-wide inventory of data assets; and (iii) assignment of roles and responsibilities for data ownership and stewardship.	31 December 2021
2	The Pension Administration of UNJSPF should: (i) establish a comprehensive data quality policy and quality improvement plan; (ii) establish data quality metrics; and (iii) develop a plan to train staff on data quality management.	Important	O	Receipt of evidence of the: (i) implementation of a data quality policy and quality improvement plan; (ii) establishment of data quality metrics; and (iii) development of a staff training plan on data quality management.	31 December 2021
3	The Pension Administration of UNJSPF should: (i) undertake a comprehensive risk assessment of data privacy and classification for its data assets; (ii) implement and embed privacy management standards in business processes and information systems; and (iii) define a retention policy and schedule for its documents and records.	Important	O	Receipt of: (i) a comprehensive risk assessment of data privacy and classification for data assets; (ii) implementation of privacy management standards in business processes and information systems; and (iii) a retention policy and schedule for documents and records.	31 December 2021
4	The Pension Administration of UNJSPF should expand the incident management procedure to include reporting of events related to data and information and inform users of the amended procedure.	Important	O	Receipt of: (i) an updated incident management procedure; and (ii) evidence that users have been informed of the amended incident management procedure.	31 March 2021
5	The Pension Administration of UNJSPF should: (i) address the ICT security weaknesses identified; and (ii) develop ICT security baselines for its systems	Important	O	Receipt of evidence that: (i) ICT security weaknesses identified in the current report	30 September 2021

---

[7] 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.

[8] 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.

[9] Please note the value C denotes closed recommendations whereas O refers to open recommendations.

[10] Date provided by the Pension Administration of UNJSPF in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of data governance, data management and reporting in the Pension Administration of the United Nations Joint Staff Pension Fund

				have been addressed; and (ii) ICT security	
	to ensure the effectiveness of external network security monitoring services.			baselines have been developed.	
6	The Pension Administration of UNJSPF should: (i) complete the documentation on business intelligence design and data models; and (ii) publish the methodology for the benefits benchmark calculation dashboard.	Important	O	Receipt of evidence that: (i) BI design and data models have been documented; and (ii) the methodology for the benefits benchmark calculation dashboard has been published.	(i) 31 December 2021 (ii) 31 December 2020
7	The Pension Administration of UNJSPF should ensure that: (i) business intelligence user requirements are comprehensively documented; and (ii) testing strategies are defined, complete with testing scenarios, to validate the reliability of business intelligence reports and dashboards.	Important	O	Receipt of evidence that: (i) user requirements for BI have been comprehensively documented; and (ii) a testing strategy has been defined complete with testing scenarios, to validate the reliability of BI reports and dashboards.	30 June 2021
8	The Pension Administration of UNJSPF should: (i) facilitate timely access to business intelligence; (ii) ensure adequate protection of data downloaded from business intelligence systems on to end-user systems; and (iii) develop a comprehensive plan to train staff and member organizations on business intelligence.	Important	O	Receipt of evidence that: (i) a SharePoint user access site has been developed to facilitate timely access to BI; (ii) controls for protection of data downloaded from the BI system on to end-user systems have been established; and (iii) a comprehensive plan has been developed to train staff and member organizations on BI.	31 December 2021

APPENDIX I

Management Response

MEMORANDUM

Ref: New York, 1 September 2020

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   /   **UNJSPF response to draft report audit of data governance, data**
Objet: **management and reporting in the Pension Administration of the United**
              Nations Joint Staff Pension Fund (Assignment No. AS2020/800/01)

1.   Reference is made to your memorandum dated 4 August 2020, in which you submitted for the Fund's review and comments, the draft report on the above-mentioned audit.

2.   As requested, please find attached the Fund secretariat's comments to the audit recommendations **Annex I**. Clarifications to the observations contained in the report are presented in **Annex II**.

3.   The Fund secretariat wishes to thank OIOS auditors for the detailed review and useful audit recommendations to strengthen data governance and data management processes.

cc.:   Ms. J. Sareva, Chief Risk Management and Legal Services Section
         Mr. D. Dell'Accio, Chief Information Officer
         Ms. M. O'Donnell, Chief of Operations
         Mr. K. Soll, Chief Financial Officer
         Ms. K. Manosalvas, Risk Officer, Audit Focal Point

Fund secretariat response to audit of data governance, management and reporting

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title responsible individual	Implementation date	Client comments[3]
1	The Pension Administration of UNJSPF should: (i) define and implement a data governance and data management framework; (ii) document the enterprise-wide inventory of its data assets; and (iii) clearly assign roles and responsibilities over data ownership and data stewardship.	Important	Yes	Chief of RMLS	December 2021	(i) The Fund's Information Technology Executive Committee will include the definition and implementation of a data management framework in the list of priorities; (ii) and (iii) The Fund will complete its inventory of data assets, which will serve as a basis to identify data owners and data stewards.
2	The Pension Administration of UNJSPF should: (i) establish a comprehensive data quality policy and quality improvement plan; (ii) establish data quality metrics; and (iii) develop a plan to train staff on data quality management.	Important	Yes	Chief of RMLS	December 2021	(i), (ii) and (iii) The Fund will issue a data quality policy; and develop and implement a data quality improvement plan to provide proper coordination, guidance, quality measurement and training for data clean-up and improvement actions.
3	The Pension Administration of UNJSPF should: (i) undertake a comprehensive risk assessment of data privacy and classification for its data assets; (ii) implement and embed privacy management standards in business processes and information systems; and (iii) define a retention policy and schedule for its documents and records.	Important	Yes	Chief of RMLS, Chief Information Officer	December 2021	(i) and (ii) The Fund will undertake a data classification exercise. The results data classification will be considered to assess and enhance related business and information systems controls as needed; (iii) The Fund will formalize the retention policy for documents and records.
4	The Pension Administration of UNJSPF should expand the incident management procedure to include reporting of events	Important	Yes	Chief of Information Officer	March 2021	The Fund will update the incident management policy and procedure to cover incidents related to loss, theft or unauthorized disclosure,

---

[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] Please indicate feasibility and realistic timelines for implementation of the recommendation.

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title responsible individual	Implementation date	Client comments[3]
	related to data and information and inform users of the amended procedure.					modification or destruction of data and information.
5	The Pension Administration of UNJSPF should: (i) address ICT security weaknesses identified; and (ii) develop ICT security baselines for its systems to ensure the effectiveness of external network security monitoring services.	Important	Yes	Chief Information Officer	September 2021	(i) The Fund will consider the aspects identified by OIOS to further strengthen data security controls. (ii) The Fund is developing a security baseline with regard to threat events that could impact its information systems. Metrics are being defined and configured within the context of the Security Operations Center (SOC) services.
6	The Pension Administration of UNJSPF should: (i) complete the documentation on business intelligence design and data models; and (ii) publish the methodology for the benefits benchmark calculation dashboard.	Important	Yes	(i) Chief Information Officer (ii) Chief of Operations	(i) December 2021 (ii) December 2020	(i) The Fund will complete the documentation of business intelligence, including the data model, which is in progress; (ii) The methodology for the calculation of the benefit processing benchmark was endorsed by the Chief Executive. The methodology will be referenced in the business intelligence dashboard as well as in reports or publications disclosing the benefit benchmark results.
7	The Pension Administration of UNJSPF should ensure that: (i) business intelligence user requirements are comprehensively documented; and (ii) testing strategies are defined, complete with testing scenarios, to validate the reliability of business intelligence reports and dashboards.	Important	Yes	Chief Enterprise Application Section	June 2021	(i) and (ii) The Fund will ensure that the development of business intelligence dashboards is aligned with the established system development methodology; and that comprehensive testing is applied prior to deployment. While this is an ongoing process, the controls recommended for the existing dashboards/reports will be implemented by the second quarter of 2021.
8	The Pension Administration of UNJSPF should: (i) facilitate timely access to business intelligence; (ii) ensure adequate protection of data downloaded from business intelligence systems on to end-user systems; and (iii) develop a comprehensive plan to train staff and	Important	Yes	Chief Information Officer	December 2021	(i) A new SharePoint based user access site is under development. In the meantime, access is granted through IMSS Service Desk; (ii) The implementation of Power BI will enable to control the download / export function; (iii) A User Guide for Power BI tool is available online.

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title responsible individual	Implementation date	Client comments[3]
	member organizations on business intelligence.					Additional training will be provided as requested.

Annex II
Comments and clarifications on the factual accuracy of the audit observations documented in the Draft Report Audit of data governance, data management and reporting

Data quality

Paragraph 16 (i): Data fixes were put in place to address IPAS workflows with issues. As reflected in the final report of the Board of Auditors for the year ended 2019, the Fund has already implemented recommendation "A/73/5/Add.16, chap. II, para. 36" by undertaking a data cleansing exercise, which identified and closed all the workflows that remained open owing to issues in IPAS.

Paragraph 16 (v) and (vi), related to data quality in IPAS: The Fund is taking action to bring dependent information into IPAS. The Fund has also started to update retroactive employment information, including leave-without-pay and part-time statuses. It is further noted that the number of withdrawal settlements for forfeiture and cases with missing mandatory documents are not due to data quality issues. There has been a substantial reduction in these cases over the last few years.

Paragraph 16 vii, related to lack of data quality in external communications: The issue referenced by OIOS does not relate to data quality but to the unauthorized publication of an article by an external vendor, for which the Fund took immediate corrective action. As for the management of the email addresses, the Fund changed the service provider for the distribution of the monthly newsletter and automatically review to ensure information is sent only to existing addresses.

Paragraph 16 (viii) It needs to be clarified that the Fund did not migrate client queries already addressed as the iNeed system was implemented as an interim solution.

Data privacy, data confidentiality and data security

Paragraph 19: The conclusions documented in the draft report, indicating that the Fund is lacking a data classification policy and/or that required data protection controls are not applied are not factually correct.

With regard to the policy, the Fund adopted the UN Secretary General Bulletin on information sensitivity, classification and handling (ST/SGB/2007/6) and avoided duplicating efforts and provisions. On these bases, the Fund determined that all information, other that the information available in its public website, is 'confidential'.

With regard to the application of required data protection controls, the Fund implemented a large number of internal controls (i.e., Access controls mechanisms; Periodic and consistent user recertifications; Security monitoring conducted by a specialized third-party; etc.), which mitigated several aspects identified in the audit, including the establishment of a comprehensive information security management system.

Paragraph 20 (i): Access to systems such as IPAS, which contain personally identifiable information, is controlled through the IMSS "User Account Management Process" and related controls. System access is granted based on the *need-to-know* and *least-privilege-access*

principles. Annual access recertifications are conducted to validate accesses granted to users. In addition, staff are also periodically reminded of the need to complete mandatory trainings, and of their responsibilities regarding the handling of confidential information in accordance with the ICSC Code of Conduct of international civil servants.

Paragraph 20 ii, related to the policies for the website, the Fund has a privacy notice on the website, which although it does not explicitly reference "cookies", includes a mention of collection of information and tracking activity.

Paragraph 20 (iii), related to data privacy requirements and controls for third parties, the Fund notes that contracts established with external vendors and service providers included the United Nations standard clauses and the Non-Disclosure-Agreement (NDA). The UN General Terms on Contracts also include provisions related to confidentiality, disclosure and notification requirements.

Data Security

Paragraph 22 (iii), indicated that a comprehensive vulnerability scanning program for various ICT applications was not developed: The Fund has conducted and provided evidence of periodic vulnerability scans, which were also reported to the Information Security Steering Committee. The security tests of web services have been conducted on an ad-hoc basis and aligned with major changes. In addition, while the process continues to be strengthened, periodic reviews of IPAS logs have been conducted.

Paragraph 22 (vi), regarding user management aspects:
a) User access authorization could not be produced for 2 users, who joined the Fund several years before the existing ticketing system was implemented. Nevertheless, the Fund maintained evidence of the user access recertification.
b) The comparison made in the draft audit report between the access process followed by the Fund for the IPAS and the Business Intelligence (BI) systems is not appropriate. IPAS is the Fund's system of records, which requires broader access. BI is a business intelligence system with the specific and limited purpose of supporting data and statistical analysis.

Reporting

Paragraph 25 (i) The Fund conducted a recent demo and provided a User Guide to member organizations to promote better understanding and training on the use of business intelligence and pension reconciliation exception (PRE) report.

Paragraph 25 (iii), indicated that the Fund lacked a comprehensive user acceptance testing strategy and documentation for business intelligence. The Fund clarifies that each of the dashboards went through over a year of development and validation with weekly meetings of the key users. The development of business intelligence dashboards was further supported by the implementation of several data clean-up projects to increase the reliability of business intelligence reports.

Paragraph 25 (iv) and (v), related to the access of member organizations to business intelligence: The Fund notes that the development of the access portal for the provision of user access is completed, and member organizations can request access through IMSS Service Desk.