



## **INTERNAL AUDIT DIVISION**

### **REPORT 2025/086**

---

#### **Audit of risk identification, assessment and mitigation activities in the United Nations Joint Staff Pension Fund**

**The Fund initiated the integration of risk management functions within both OIM and the Pension Administration; however, to build a more robust framework, it needed to implement risk and control self-assessment workshops and strengthen implementation of risk mitigation actions**

**29 December 2025**

**Assignment No. AS2025-800-01**

# **Audit of risk identification, assessment and mitigation activities in the United Nations Joint Staff Pension Fund**

## **EXECUTIVE SUMMARY**

The Office of Internal Oversight Services (OIOS) conducted an audit of risk identification and assessment and mitigation activities in the United Nations Joint Staff Pension Fund (UNJSPF or Fund). The objective of the audit was to assess the adequacy and effectiveness of risk assessment and mitigation activities in UNJSPF. The audit covered the period from 1 January 2023 to 30 June 2025 and included: (a) risk identification and assessment; and (b) design and implementation of risk mitigation activities.

While the Fund has initiated the integration of risk management functions across the Office of Investment Management (OIM) and the Pension Administration, the audit identified gaps including a lack of bottom-up validation through structured Risk and Control Self-Assessment (RCSA) workshops, low staff training completion on risk management, and inadequate oversight over risk treatment plans.

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

- Update its enterprise risk management policy to align with the Three Lines Model and other best practices, including an effectiveness assessment framework for the risk management process.
- Establish timelines to complete the training on the Enterprise-Wide Risk Management process and organize refresher training for risk owners.
- Conduct RCSA workshops for key business processes.
- Revise risk scoring criteria to assign specific, quantifiable measures to likelihood and impact and develop standardized tools to aid risk owners in identification and assessment.
- Align its Anti-Fraud and Anti-Corruption framework considering all areas of the Fund's operations; and ensure comprehensive identification and assessment of fraud risk scenarios.
- Enhance its Governance, Risk and Control system (GRC System) by incorporating risk appetite and tolerance limits, cleaning the system data, and ensuring adequate training for all risk and control owners.
- Formally document procedures for the development and implementation of risk treatment and response plans and establish clear guidelines for classifying a risk as 'Accepted'.
- Document clear criteria for defining key controls within the Fund's risk and controls framework.

UNJSPF accepted all recommendations and has initiated action to implement them. Actions required to close the recommendations are indicated in Annex I.

# CONTENTS

I. BACKGROUND	1-2
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	2
III. AUDIT RESULTS	2-10
A. Risk identification and assessment	2-8
B. Design and implementation of risk mitigation activities	8-10
IV. ACKNOWLEDGEMENT	10
ANNEX I	Status of audit recommendations
APPENDIX I	Management response

# **Audit of risk identification, assessment and mitigation activities in the United Nations Joint Staff Pension Fund**

## **I. BACKGROUND**

1. The Office of Internal Oversight Services (OIOS) conducted an audit of risk identification and assessment and mitigation activities in the United Nations Joint Staff Pension Fund (UNJSPF or Fund).
2. UNJSPF was established in 1949 by the United Nations General Assembly to provide retirement, death, disability, and related benefits for staff of the United Nations and its member organizations. With over 150,000 participants and 90,000 beneficiaries worldwide, the Fund plays a critical role in ensuring long-term financial security for its stakeholders.
3. The UNJSPF functions within a unique tripartite governance structure that establishes the context for its Enterprise-wide Risk Management (EWRM) framework. This structure is defined by distinct reporting lines: the Pension Administration is led by the Chief Executive, who reports to the Pension Board, while the Office of Investment Management (OIM) is led by the Representative of the Secretary-General, who reports directly to the United Nations Secretary-General. This structure introduces complexity in risk oversight and accountability. The Enterprise-wide Risk Management Working Group (EWRM WG), co-chaired by the Chief Executive of Pension Administration and the Representative of the Secretary-General for Investments, serves as the central coordinating body for EWRM. It facilitates cross-functional collaboration, monitors the Fund's risk profile, and ensures that risk management practices are aligned with strategic objectives.
4. The Fund first established the EWRM Policy in 2006, which outlined core elements, including basic definitions, the five-step risk management process, and defined functional responsibilities. A key update occurred in the 2016 Policy, which elevated the strategic nature of risk management by formally integrating and defining the UNJSPF Risk Appetite Statement, establishing the link between strategy and risk-taking tolerance. This framework was refined in the July 2022 Policy, which incorporated necessary structural and naming changes, such as reflecting the change from the Investment Management Division (IMD) to OIM.
5. The Fund's EWRM Methodology has undergone changes over the years. The first EWRM methodology was issued in 2012. Over the years, the Fund prepared separate documents that detailed processes specific to the two main functional arms: the June 2021 OIM EWRM Methodology outlining the framework and mechanisms adopted within OIM, and the May 2022 EWRM Methodology detailing the process for Pension Administration.
6. The UNJSPF Risk Management and Compliance Function is responsible for identifying, measuring, and monitoring market and operational risks, implementing compliance measures, and ensuring that the Fund operates ethically and in accordance with its regulations. Key responsibilities include conducting ongoing risk assessments, providing risk management expertise, overseeing compliance activities, and reporting risk status to senior management and the Pension Board. The integration of Risk Management and Compliance functions within both OIM and the Pension Administration, effective as of January 2024, reinforces the Fund's commitment to coordinated and effective risk mitigation. To support the integration of risk management and compliance functions, the Risk Management and Compliance Service has grown from 10 to 22 posts. The Chief Risk and Compliance Officer (D-1) is supported by 21 Professional and one General Service staff (5 (P-5), 4 (P-4), 9 (P-3), 3 (P-2), 1 (G-7)).

7. The Fund procured the automated tool, the Governance, Risk and Control system (GRC System) in 2022 to document and map risks, risk factors, controls associated with all key processes, and the residual risks after the implementation of controls, and to document the action plans for ineffective controls. The GRC system aims to replace Excel-based risk registers with a centralized, structured digital platform that enables real-time monitoring, visibility, and governance. It integrates the Fund's EWRM and Internal Control Framework, providing a unified environment for risk identification, assessment, mitigation, and reporting across the Pension Administration and OIM. It provides structured modules for the risk register, control library, mitigation actions, testing, and dashboards, supporting real-time oversight and documentation.

8. Comments provided by UNJSPF are incorporated in italics.

## **II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY**

9. The objective of the audit was to assess the adequacy and effectiveness of risk assessment and mitigation activities in UNJSPF.

10. This audit was included in the 2025 risk-based work plan of OIOS due to the importance of the effective EWRM process in managing risks that threaten the achievement of UNJSPF's operational and strategic objectives.

11. OIOS conducted this audit from September to November 2025. The audit covered the period from 1 January 2023 to 30 June 2025 and included: (a) risk identification and assessment; and (b) design and implementation of risk mitigation activities.

12. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; and (c) walk-through of the GRC system.

13. OIOS assessed the reliability of data related to the Fund by: (a) reviewing existing information about the data and the GRC system; and (b) interviewing the Fund's personnel knowledgeable about the data. In addition, OIOS traced a random sample of data to source documents. Based on the assessment, OIOS determined that the data was sufficiently reliable for the purpose of addressing audit objectives.

14. The audit was conducted in accordance with the Global Internal Audit Standards.

## **III. AUDIT RESULTS**

### **A. Risk identification and assessment**

#### Need to update the enterprise risk management policy

15. The Fund's EWRM Policy of July 2022 established a good governance foundation by aligning with the best practices in EWRM and assigning responsibilities across the organization; however, it lacked an explicit articulation of the Three Lines of Model that ensures clear segregation of duties. Furthermore, the policy's "Risk Appetite Statement" remains fully qualitative without defining the outline for measurable tolerance limits found in best-in-class frameworks to guide decision-making. The policy also lacked a requirement for developing formal risk mitigation and control plans for moderate risks. Further, the policy did not have a formal framework to conduct an internal assessment of the overall effectiveness of its risk management process by identifying mandatory Key Assessment Indicators and specific management assessment questions. While the delegated fiduciary responsibility of the Representative of the Secretary-

General included mandatory reporting to the UN Secretariat, the Policy was not explicit regarding mandatory risk reporting requirements for OIM risks.

16. The Fund stated that the risk management framework was complemented by other policies, such as the Internal Control Policy presented to the Pension Board in 2014, which defined the internal control system, its objectives, and the roles within the Three Lines of Defense. However, the Fund acknowledged the need to update the EWRM policy to align with compliance with the Three Lines Model and other best practices.

**(1) UNJSPF should update its enterprise risk management policy to: (i) align with the Three Lines Model and other best practices, including an effectiveness assessment framework for the risk management process; and (ii) incorporate the mandatory risk reporting requirement to the United Nations Secretariat concerning risks related to OIM.**

*UNJSPF accepted recommendation 1 and stated that it will complete the review and reissuance of the enterprise risk management policy, which will align with the three lines model and other best practices to enhance the effectiveness of the risk management process. The updated EWRM policy will consider regular risk reporting to the appropriate levels, in line with the Fund's governance.*

The Fund is finalizing a common methodology applicable to both sides of the Fund

17. Both the Pension Administration (2022) and OIM (2021) had their own EWRM methodologies to assess risk, even though the Fund has one EWRM policy. Upon review of both methodologies, OIOS noted that:

- OIM EWRM methodology referred to a quarterly risk assessment exercise for risk owners; on the contrary, the Pension Administration methodology emphasized the need-based risk assessment exercise, depending upon the occurrence of events, to reflect changes in the risk profile, without any specific timeline.
- Both methodologies did not provide any guidance on risk appetite, setting tolerance limits for each key risk indicator, and establishing performance measures.
- Both methodologies did not provide any tools, such as templates or sample questionnaires, to facilitate implementation.

18. The Fund was developing a combined EWRM methodology to support the integration of the Risk Management function within both OIM and the Pension Administration. The July 2025 draft EWRM methodology outlines a unified governance and internal processes to be applied across the Fund as a whole.

The Fund initiated action to establish tolerance limits for all risks

19. The best practices in risk management indicate that organizations must define the risk appetite defining the tolerance limits.

20. The Fund's 2022 EWRM policy defined the risk appetite for the whole Fund, which was incorporated into the Fund's risk register in September 2024. Based on July 2025 draft EWRM methodology, the Fund had identified 50 risks in seven main risk categories, namely: Strategic, Governance, Compliance and Legal, Operational, Solvency, and Financial, in the risk register and defined the risk appetite (No Appetite, Low, Moderate, and High). Further, the Fund identified the 225 risk factors associated with the 50 risks. The Fund defined tolerance limits based on the nature of risk as shown in Table 1.

**Table 1: Examples of tolerance limits**

Risk name (50)	Risk Appetite (50)	Risk factor (225)	Key risk indicator (93)	Tolerance limit
Benefit payment	Low	Operational risk related to payroll	Number of benefit payments issued or returned by the bank due to internal user	Less than 100 cases
Client services	Low	Delayed response at the contact center	Percentage of calls answered	95 per cent or above of calls picked up by the contact center
Cash management and disbursement	Low	No additional cost for the beneficiary	Reduced check payments	Declining trend
ICT Security	Low	Information Security controls	Maintain ISO 27001 certification (27002 controls)	Satisfactory

21. The Fund established 93 key risk indicators and tolerance limit associated with 29 risks out of 50. For the remaining 21 risks, key risk indicators and tolerance limits were not established as of the fieldwork date. The Fund stated that they were in the process of reviewing risks, associated risk factors and establishing tolerance limits.

Need to improve the involvement of risk owners in the risk management process

22. The Fund defined that first-line managers are risk owners because they are in charge of their respective functions and directly affected by the consequences of risks in their areas. The review of the process for identification of risks and interviews with 24 risk owners and risk officers showed that:

- (a) The Fund identified 16 risk owners for the Pension Administration and 11 for OIM. OIOS interviews with the Fund's risk owners and risk officers did not find evidence that risk owners themselves identified and reported events to risk officers. The Fund stated that it met with risk owners quarterly to review risk and control status and risk ratings.
- (b) During interviews with risk owners, OIOS also noted a gap in their understanding of risk appetite, defining the tolerance limits, and establishing the key performance indicators to manage the risk. While the risk owners are accountable for managing risks, it was the risk team that was taking the lead in setting tolerance limits and establishing key risk indicators.

23. The Fund stated that to increase the engagement of risk owners and to create awareness on the EWRM process among all staff, three training modules (Risk management essentials, Internal control in practice, and Risk appetite: practical application) relating to the EWRM process have been developed in association with the United Nations System Staff College. The Fund required all the staff to complete this training. OIOS review of staff attending the training on both sides of the Fund indicated that only 53 per cent of the Fund's staff completed all three modules, and 39 per cent did not complete even a single module since November 2024, as shown in Table 2.

**Table 2: EWRM Training completion rate of UNJSPF staff**

Entity	Total Staff	Staff completed all modules		Staff completed two modules		Staff completed one module		Staff completed no module	
		Number	Percentage	Number	Percentage	Number	Percentage	Number	Percentage
PA	288	160	56	5	2	21	7	102	35
OIM	183	89	48	1	1	13	7	80	44
Total	471	249	53	6	1	34	7	182	39

24. For the risk owners, OIOS noted that 10 out of 16 in the Pension Administration and 4 out of 11 in OIM had completed the training. The Fund stated that the training is self-paced and staff can complete the training at their convenience. The Fund added that several new staff have recently joined the Fund to address the additional workload. In OIOS's opinion, to promote a risk culture in the Fund and to ensure effective engagement of risk owners, the Fund needed to establish timelines for completing EWRM training and include refresher courses for risk owners.

**(2) UNJSPF should establish timelines to complete the training on the EWRM process and organize refresher training for risk owners.**

*UNJSPF accepted recommendation 2 and stated that it will establish a plan and process to ensure completion of risk management training by staff and provide periodic briefings to risk owners.*

Need to institute a mechanism for conducting Risk and Control Self-Assessment (RCSA) workshops for key business processes

25. Organizations should engage the process owners and staff who execute daily activities in the risk management process. The globally recognized method for achieving this bottom-up, granular engagement is the Risk and Control Self-Assessment (RCSA) workshop, which systematically identifies process-level risks and validates the design and operational effectiveness of controls with those who use them.

26. The Fund stated that it implemented a mandatory and regular process for identifying and assessing risks and controls with the involvement of risk and control owners and other functional experts, as evidenced by the periodic risk assessments facilitated by the risk management team. However, the audit noted that the risk management team largely drove the compilation of risks, and risk owners were subsequently asked to ratify or confirm the existing risks and controls. The Fund has not formally instituted a systematic risk identification process, specifically the use of RCSA workshops involving relevant process owners and working-level staff.

27. Without the formal RCSA process to validate controls, the Fund lacks bottom-up assurance that the stated internal controls are both designed appropriately for the risk they are meant to address and function effectively in day-to-day operations. These workshops should engage Control Owners and process experts.

**(3) UNJSPF should conduct Risk and Control Self-Assessment (RCSA) workshops for key business processes.**

*UNJSPF accepted recommendation 3 and stated that it will document a methodology and process for conducting Risk and Control Self-Assessments to assess operational risks for key business processes. The methodology and process will specify the approach, either by process or cross functional, and tools selected by the Fund.*

Risk methodology, including scoring criteria, needed to be improved

28. The Fund uses a 3\*3 scale risk matrix to calculate the residual risk after taking into consideration the inherent risk relating to various operations and the effectiveness of internal controls in place to mitigate those risks. (Residual risk = Inherent risk exposure – Effectiveness of internal controls). Inherent risk exposure depends on the likelihood of an event occurrence and its impact on business operations. The impact could be strategic, reputational, operational, and financial. For instance, to calculate the likelihood of occurrence of events, scores were assigned as shown in Table 3.

**Table 3: Risk Scoring**

Likelihood	Score	Historic experience or forward looking
Likely	3	Event is expected to occur
Possible	2	Event may occur and/ or event has occurred previously
Unlikely	1	Event could potentially occur/ or event may not occur

29. The audit noted that the criteria used to score both likelihood and impact were overly qualitative without being supplemented by quantitative criteria. For Likelihood, scores are based on qualitative terms ("Likely," "Possible," "Unlikely") without assigning specific probability or frequency (e.g., "occurs once every two years"). Similarly, financial impact is defined ("low, moderate, or material") without linking these terms to specific monetary amounts or percentages. Consequently, risk scoring became highly dependent on individual judgment, hindering accurate and objective risk assessment.

30. In addition, the Fund’s methodology was missing standardized tools and templates found in the UN Secretariat's ERM Guide that are required to enforce control and consistency. The Fund would benefit from incorporating tools such as the Risk Assessment Interview Sample Questionnaire for consistent risk identification and a Formal Approval & Communication Template to establish a clear, documented audit trail for the authorization of risk treatment plans by risk owners, etc.

**(4) UNJSPF should: (i) review its risk scoring criteria and assign specific, quantifiable measures (e.g., probability ranges, frequency timelines, and monetary thresholds) to likelihood and impact criteria to the extent possible; and (ii) develop tools such as templates and questionnaires to aid the risk owners in risk identification and assessment.**

*UNJSPF accepted recommendation 4 and stated that it will develop and implement an enhanced risk quantification methodology. It will review risk scoring criteria to consider quantifiable measures to the extent possible and include supplementary risk and control assessment templates as required.*

Controls over the fraud risk assessment needed to be strengthened

31. The Fund adopted the Anti-Fraud and Anti-Corruption Framework of the United Nations Secretariat. To supplement the United Nations Secretariat Framework, OIM developed the Anti-Fraud and Anti-Corruption policy and Fraud Risk Management Framework Guide in 2019, and the Pension Administration developed the Pension Fraud Awareness, Reporting and Escalation Policy. The review of the policies showed the following on risk assessment.

- (a) **Timeline-** OIM Policy defined that fraud risk assessments were to be conducted once in three years, whereas the Pension Administration’s policy did not define a timeline. However, the audit noted that OIM conducted annual fraud risk assessments for selected areas, while the Pension Administration performed them every two years.
- (b) **Coverage-** The Pension Administration conducted a fraud risk assessment in 2024 and identified 33 fraud risk scenarios covering 24 processes or risk areas covering almost all the functional units. However, OIM covered two processes (human resources and procurement) in 2023 with 38 fraud scenarios and another two (fixed income and private markets) in 2024 with 36 fraud scenarios. OIM stated that they do extensive risk assessment for all possible scenarios for each process or risk area.
- (c) **Identification of new fraud scenarios-** OIOS noted that the Pension Administration identified six new fraud scenarios; no such information was readily available for OIM.

- (d) **Testing of controls-** Both the Pension Administration and OIM rely on the third party for testing key controls for statement of internal control purposes. OIOS noted that out of 33 fraud risk scenarios identified by the Pension Administration, the key controls were tested for 18 fraud scenarios, while similar information was not readily available for OIM.

32. Fund has zero tolerance for any risks related to fraud and corruption, meaning that all fraud concerns should be reported and investigated. Incomplete testing of anti-fraud controls could undermine the effectiveness of the Fund's fraud risk assessment.

- (5) UNJSPF should: (i) align its Anti-Fraud and Anti-Corruption framework considering all areas of the Fund's operations; and (ii) ensure comprehensive identification and assessment of fraud risk scenarios.**

*UNJSPF accepted recommendation 5 and stated that it will align its anti-fraud and anti-corruption framework, considering key fraud risk exposure areas. It will also enhance and align the fraud risk assessment methodology in line with best practices. Fraud risk assessments will continue to cover key fraud risk scenarios and anti-fraud controls based on risk and materiality criteria.*

Need to enhance the functionalities in the Governance, Risk and Control system (GRC System)

33. Starting from 2025, the Fund used the GRC system to implement the EWRM process. The review of the GRC system showed the following.

- (a) **Functionalities** - The GRC (IT) system did not have functionalities to include the risk appetite and the risk tolerance limits for the key risk indicators for the identified risks.
- (b) **Data migration and accuracy of data-** There were issues with the migration of data from risk registers in Excel format to the GRC system, requiring extensive data cleaning. Risk ratings in the GRC system did not match those in the Fund's risk register for 8 of 50 risks. Incomplete and duplicate information relating to risks and controls for both entities. For instance, for the risk "Data and Records Management" risk factors and controls were not populated into the system for the Pension Administration. Similarly, for "Fraud and Corruption" risk factors and controls were missing for OIM. Instances of duplicate information of risk factors and associated controls for the same risks were noted. Additionally, it was noted that some risk factors and control actions were not related to the associated risk.
- (c) **Training-** Few risk owners were adequately trained in using the GRC system.

34. The Fund stated that they have a separate Excel-based key risk indicator dashboard to track risk appetite and tolerance limits. In OIOS's opinion, since risk appetite and tolerance limits are indispensable to the risks and risk factors, and any changes to risk factors or controls will impact the tolerance limits, they need to be monitored together; the Fund needs to explore with the vendor to enhance the functionalities to incorporate the risk appetite and tolerance limits. About the accuracy of data issues, the Fund stated that the initial data migration of the UNJSPF risk register, such as risks, risk description, risk factors, risk owners, likelihood, impact, controls, and control owners, was done digitally with the help of templates provided by the vendor, and the system is not fully mature yet. The information will be reviewed before the system is fully rolled out to the process owners for their use in the second quarter of 2026.

35. The Fund further stated that they have provided training to the risk and control owners on the GRC system, and the risk team was directly involving the risk and control owners in necessary changes to the associated risks and controls. OIOS review of training provided to the risk and control owners in September 2025 indicated that all 16 risk and control owners from the Pension Administration side had completed the

training. In contrast, only 5 of 11 risk and control owners in OIM completed the GRC system training. During OIOS interviews with process owners, staff who received training on the GRC system indicated a need for refresher training due to the system's complexity.

**(6) UNJSPF should take steps to enhance the functionalities in the GRC system by: (i) incorporating risk appetite and tolerance limits; (ii) cleaning the data incorporated into the GRC system; and (iii) ensuring that all the risk and control owners are adequately trained on the GRC system.**

*UNJSPF accepted recommendation 6 and stated that it will complete the implementation of the GRC system with additional functionalities and train users accordingly.*

Due consideration was given to the risks associated with the emerging initiatives

36. OIOS review of risk identification and assessment process of the Fund noted that the Fund was aware of the emerging risk scenarios associated with “Solvency Risk” and the “Benefit Processing Risk” and is actively monitoring the risks. The Fund analyzed data on possible separation trends among the UNJSPF member organizations arising from funding cuts and the broader UN80 initiative launched by the UN Secretary-General. A Solvency Risk Dashboard has been developed to closely monitor developments relating to funding reductions across the UN system; in addition, the Fund has adequately discussed possible scenarios with the Fund's Consulting Actuary. Further, risks related to operational performance in benefit processing due to a surge in separations were appropriately considered in the UNJSPF risk register, concluding that due consideration was given to the risks associated with the emerging initiatives in identification and assessment.

## **B. Design and implementation of risk mitigation activities**

Controls in the management of risk treatment and response plans needed to be strengthened

37. According to the best practices, risk owners are responsible for developing mitigation plans to reduce identified risks to an acceptable level, aligned with the organization's risk appetite. The Fund's EWRM Policy (2022) provides that, for identified high-level risks, comprehensive risk treatment and response plans should be developed to outline mitigation strategies. These strategies should be selected based on the criteria of efficacy, feasibility and efficiency.

38. The Fund stated that risk treatment and response plans were prepared since the inception of the enterprise risk framework. The audit noted that risk treatment and response plans were prepared for high-level risks, namely cybersecurity, data privacy and confidentiality. No formal treatment plan was in place for the external factors risk, as the Fund has limited control over macroeconomic or geopolitical developments. The Risk team indicated that these risks are instead addressed through business continuity planning and scenario analysis.

39. During the period, additional plans were prepared for “cybersecurity” and “privacy and confidentiality” for Pension Administration and OIM respectively. The audit reviewed four versions of these plans – prepared in August, September, and December 2024, and March 2025 – and noted following:

- (a) There were some gaps in the development of risk treatment and response plan, which included:
- There was no evidence of review and approval of these plans.
  - Across all treatment plans, the “Required resources” field was consistently left blank.

- Privacy and confidentiality for OIM (In August and September 2024): the risk treatment plan was incomplete, with fields such as due date, current status, responsible person, action updates, and required resources left blank.
  - Cybersecurity for OIM (September and December 2024): two action items – “Complete ISMS policies and procedures annual review” and “Update the Access Control and Account Management Procedure” – were marked “In progress” in September 2024 but were missing from the December 2024 plan.
- (b) Many action updates were brief (one or two sentences) and insufficient, making it difficult to assess the operationalization of the plans. For example:
- **Privacy and confidentiality for OIM (March 2025):** In the March 2025 plan, the action “Develop office-wide data retention schedule, including personal data” had a due date of Q4 2024. The update only stated, “Retention schedule exists for each data domain,” while status remained “In progress,” creating ambiguity about completion and next steps. Another action, “AI Governance Workshop and decisions about AI Governance,” was marked “Completed,” but the update simply stated “AI Governance to be formalized,” suggesting a potential mismatch between status and progress.
  - **Privacy and confidentiality for Pension Administration (March 2025):** Three actions – “Development of Data Governance Framework, including creation of Data Governance Council,” “Development of data retention policy and schedule,” and “Conduct a comprehensive data confidentiality and privacy risk assessment” – all had a due date of Q4 2024, but their update fields were left blank in the risk register in March 2025.

40. A review of presentation slides and meeting minutes from EWRM WG over the past two years noted that the WG regularly discussed risk mitigation activities undertaken by risk owners. However, a structured comparison between planned and actual progress, nor discussions around delayed or not-yet-started actions, were not adequately provided to WG to systematically review or follow up on planned actions documented in the risk treatment plans.

41. In addition, the Fund has not developed formal, standardized guidelines detailing the required analysis, process, and documentation for a risk owner to classify a risk as 'Accepted' (unmitigated by action). While the Fund’s framework correctly provides the four high-level options for risk response (Acceptance, Avoidance, Reduction, Sharing), it lacked the required operational guidance, documentation templates, and mandatory sign-off thresholds that govern the high-stakes decision to accept a risk.

42. There was no formally defined process or designated authority for reviewing and approving risk treatment plans. Without consistent and complete development and documentation of risk treatment plans, there was an increased likelihood that key risks may not be effectively mitigated. The Fund needed to establish a formal procedure for the review and approval of risk treatment plans, which should clearly define the roles and responsibilities of risk owners and approving authorities, as well as timelines for submitting, reviewing and updating treatment plans.

**(7) UNJSPF should strengthen its controls over the development, implementation, and oversight of risk treatment and response plans by: (i) formally documenting procedures for their review, approval, and adequate implementation; and (ii) developing guidelines to classify a risk as 'Accepted' (unmitigated by action).**

*UNJSPF accepted recommendation 7 and stated that it will strengthen the procedures for the development, implementation and oversight of risk treatment and response plans, and their related automation. The GRC system will be leveraged to support oversight and reporting of these plans.*

*The risk treatment procedures will include guidelines for the selection of mitigation strategies, including the risk acceptance process.*

#### Testing of controls needed to be strengthened

43. The Fund relied on an external accounting firm to test the controls. The task order issued to the external firm specified that only key controls should be tested. OIOS noted:

- Pension Administration had 69 business controls (including sustainability-related controls), of which 59 were considered key controls. Additionally, there were 15 ICT controls, all of which were considered key. Of the total 74 key controls, 67 were reviewed by the external firm in the 2024 control testing. The control tests concluded that 64 controls were effective with no exceptions noted, and three controls—all ICT controls—were ineffective.
- Similarly, OIM had 39 business controls, of which 35 were classified as key. In addition, there were 14 ICT controls and 12 of them were key controls. Of the total 47 key controls in OIM, 45 were confirmed effective and two ICT controls were ineffective.
- In addition, the external firm also tested 31 out of 63 UNJSPF entity-level controls, and all of them were confirmed to be effective.

44. The external firm and the Fund’s risk team confirmed that the testing focused on controls over financial reporting rather than broader operational or strategic controls. There was also a risk that controls deemed non-key—and therefore excluded from testing—may still be critical for managing risks from an EWRM standpoint. The determination of key versus non-key controls was made by Fund management without documented criteria or definitions. The Fund stated that managers conduct their evaluation of controls informed or supported by the testing of controls conducted by an external firm. However, during interviews, many control owners cited the external firm testing as a basis for confidence in their controls.

45. The limited scope of external firm testing and the lack of proactive self-assessment by control owners may result in gaps in assurance over operational and strategic risks. The Fund was yet to adopt a structured control self-assessment process across the Fund, such as annual workshops facilitated by the Risk team to proactively review and confirm the effectiveness of their controls.

**(8) UNJSPF should document clear criteria for defining key controls within the Fund’s risk and controls framework.**

*UNJSPF accepted recommendation 8 and stated that it as part of its revised methodologies, it will enhance the criteria used for the identification of key controls.*

## **IV. ACKNOWLEDGEMENT**

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

Internal Audit Division  
Office of Internal Oversight Services

## STATUS OF AUDIT RECOMMENDATIONS

## Audit of risk identification, assessment and mitigation activities in the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical <sup>1</sup> / Important <sup>2</sup>	C/ O <sup>3</sup>	Actions needed to close recommendation	Implementation date <sup>4</sup>
1	UNJSPF should update its enterprise risk management policy to: (i) align with the Three Lines Model and other best practices, including an effectiveness assessment framework for the risk management process; and (ii) incorporate the mandatory risk reporting requirement to the United Nations Secretariat concerning risks related to OIM.	Important	O	Receipt of the updated enterprise risk management policy.	28 February 2027
2	UNJSPF should establish timelines to complete the training on the EWRM process and organize refresher training for risk owners.	Important	O	Receipt of confirmation that staff and risk owners have completed the required training.	30 September 2027
3	UNJSPF should conduct Risk and Control Self-Assessment (RCSA) workshops for key business processes.	Important	O	Receipt of evidence that the Fund initiated action to conduct Risk and Control Self-Assessment workshops.	30 September 2028
4	UNJSPF should: (i) review its risk scoring criteria and assign specific, quantifiable measures (e.g., probability ranges, frequency timelines, and monetary thresholds) to likelihood and impact criteria to the extent possible; and (ii) develop tools such as templates and questionnaires to aid the risk owners in risk identification and assessment.	Important	O	Receipt of evidence showing the development and implementation of the enhanced risk quantification methodology and the revised risk scoring criteria.	31 March 2028
5	UNJSPF should: (i) align its Anti-Fraud and Anti-Corruption framework, considering all areas of the Fund's operations; and (ii) ensure comprehensive identification and assessment of fraud risk scenarios.	Important	O	Receipt of the revised and aligned fraud risk assessment methodology documentation.	31 March 2027

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Please note the value C denotes closed recommendations whereas O refers to open recommendations.

<sup>4</sup> Date provided by UNJSPF in response to recommendations.

## STATUS OF AUDIT RECOMMENDATIONS

## Audit of risk identification, assessment and mitigation activities in the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical <sup>1</sup> / Important <sup>2</sup>	C/ O <sup>3</sup>	Actions needed to close recommendation	Implementation date <sup>4</sup>
6	UNJSPF should take steps to enhance the functionalities in the GRC system by: (i) incorporating risk appetite and tolerance limits; (ii) cleaning the data incorporated into the GRC system; and (iii) ensuring that all the risk and control owners are adequately trained on the GRC system.	Important	O	Receipt of evidence on the implementation of the enhanced GRC system functionalities and the completion of user training.	31 March 2028
7	UNJSPF should strengthen its controls over the development, implementation, and oversight of risk treatment and response plans by: (i) formally documenting procedures for their review, approval, and adequate implementation; and (ii) developing guidelines to classify a risk as 'Accepted' (unmitigated by action).	Important	O	Receipt of evidence of strengthened risk treatment and response procedures.	31 December 2027
8	UNJSPF should document clear criteria for defining key controls within the Fund's risk and controls framework.	Important	O	Receipt of the enhanced criteria for the identification of key controls.	31 March 2028

# **APPENDIX I**

## **Management Response**

# UNJSPF CCPPNU

United Nations Joint Staff Pension Fund

Caisse commune des pensions du personnel des Nations Unies

TO: Mr. Byung-Kun Min,  
A: Director Internal Audit Division,  
Office of Internal Oversight Services

DATE: 19 December 2025

REFERENCE:

THROUGH:  
S/C DE:

FROM: Rosemarie McClean,  
DE: Chief Executive,  
United Nations Joint Staff Pension Fund



[Rosemarie McClean \(Dec 19, 2025 13:55:42 EST\)](#)

Robert van der Zee,  
Acting Representative of the Secretary-General  
for the investment of the UNJSPF assets



[Robert Van der Zee \(Dec 19, 2025 14:16:16 EST\)](#)

SUBJECT: **UNJSPF response to draft report of the audit of risk identification, assessment and mitigation activities in the United Nations Joint Staff Pension Fund (UNJSPF)**  
OBJET: **mitigation activities in the United Nations Joint Staff Pension Fund (UNJSPF)**

1. Reference is made to your memorandum dated 17 December 2025, in which you submitted for the Fund's review and comments, the draft report of the above-mentioned audit.
2. As requested, the Fund's comments on the audit recommendations are included in Annex I. Factual corrections and clarifications are contained in Annex II.
3. The Fund would like to thank OIOS auditors for the constructive exchanges with management.

cc.: Mr. D. Dell'Accio, Deputy Chief Executive  
Mr. J. Nunez, Chief Risk and Compliance Section  
Ms. K. Manosalvas, Senior Risk Officer and Audit Focal Point

**ANNEX I**  
**Audit of risk identification, assessment, and mitigation activities in the United Nations Joint Staff Pension Fund**

<b>Rec. no.</b>	<b>Recommendation</b>	<b>Critical<sup>1</sup>/ Important<sup>2</sup></b>	<b>Accepted? (Yes/No)</b>	<b>Title of responsible individual</b>	<b>Implementation date</b>	<b>Client comments</b>
1	UNJSPF should update its enterprise risk management policy to: (i) align with the Three Lines Model and other best practices, including an effectiveness assessment framework for the risk management process; and (ii) incorporate the mandatory risk reporting requirement to the United Nations Secretariat concerning risks related to OIM.	Important	Yes	Chief Risk and Compliance	February 2027	i) The Fund will complete the review and reissuance of the enterprise risk management (EWRM) policy, which will align to the Three Lines Model and other best practices, to enhance the effectiveness of the risk management process. ii) The updated EWRM policy will consider regular risk reporting to the appropriate levels, in line with the Fund's governance.
2	UNJSPF should establish timelines to complete the training on the EWRM process and organize refresher training for risk owners.	Important	Yes	Chief Risk and Compliance	September 2027	The Fund will establish a plan and process to ensure completion of risk management training by staff and provide periodic briefings to risk owners.
3	UNJSPF should conduct Risk and Control Self-Assessment (RCSA) workshops for key business processes.	Important	Yes	Chief Risk and Compliance	September 2028	As part of the plan to update and improve the enterprise risk management framework, the Fund will document a methodology for conducting Risk and Control Self-Assessments to assess operational risks for key business processes. The methodology and process will specify the approach, either by process or cross functional, and tools selected by the Fund.

<sup>1</sup> 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.

<sup>2</sup> 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/ <sup>1</sup> / Important <sup>2</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
4	UNJSPF should: (i) review its risk scoring criteria and assign specific, quantifiable measures (e.g. probability ranges, frequency timelines, and monetary thresholds) to likelihood and impact criteria to the extent possible; and (ii) develop tools such as templates and questionnaires to aid the risk owners in risk identification and assessment.	Important	Yes	Chief Risk and Compliance	March 2028	The Fund will: i) Review risk scoring criteria to consider quantifiable measures to the extent possible. ii) Include supplementary templates as required.
5	UNJSPF should: (i) align its Anti-Fraud and Anti-Corruption framework, considering all areas of the Fund's operations; and (ii) ensure comprehensive identification and assessment of fraud risk scenarios.	Important	Yes	Chief Risk and Compliance	March 2027	i) The Fund will align its anti-fraud and anti-corruption framework, considering key fraud risk exposure areas. ii) The Fund will enhance and align the fraud risk assessment methodology in line with best practices. Fraud risk assessments will continue to cover key fraud risk scenarios and anti-fraud controls based on risk and materiality criteria.
6	UNJSPF should take steps to enhance the functionalities in the GRC system by: (i) incorporating risk appetite and tolerance limits; (ii) cleaning the data incorporated into the GRC system; and (iii) ensuring that all the risk and control owners are adequately trained on the GRC system.	Important	Yes	Chief Risk and Compliance	March 2028	The Fund will complete the implementation of the GRC system with additional functionalities, and train users accordingly.
7	UNJSPF should strengthen its controls over the development, implementation, and oversight of risk treatment and response plans by: (i) formally documenting procedures for their review, approval, and adequate implementation; and (ii) developing guidelines to classify a risk as 'Accepted' (unmitigated by action).	Important	Yes	Chief Risk and Compliance	December 2027	i) The Fund will strengthen the procedures for the development, implementation and oversight of risk treatment and response plans, and their related automation. The GRC system will be leveraged to support oversight and reporting of these plans. ii) The risk treatment procedures will include guidelines for the selection of

Rec. no.	Recommendation	Critical/ Important <sup>2</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
8	UNISPF should document clear criteria for defining key controls within the Fund's risk and controls framework.	Important	Yes	Chief Risk and Compliance	March 2028	mitigation strategies, including the risk acceptance process.  As part of its revised methodologies, the Fund will enhance the criteria used for the identification of key controls.

## ANNEX II

### Factual corrections and clarifications to the detailed results

**Paragraph 15:** The Fund wishes to highlight that it has made considerable progress in the implementation of a project to review and enhance the enterprise risk management framework. The Fund kindly requests OIOS to consider the following clarifications:

- i) The EWRM Policy defines the governance and roles and responsibilities in the risk management process. An explicit reference to the Three Lines Model will be added in the future versions of the policy.
- ii) It is not appropriate for an EWRM Policy to contain ‘measurable tolerance limits’. Risk indicators and limits should be separately documented to enable more frequent updates.
- iii) Regarding the lack of a requirement for formal mitigation planning for Moderate-Level risks, the EWRM Policy specifies under section 4 – Risk response and Internal Control Activities that *‘moderate risks will typically require the implementation of specific remedial or monitoring measures under the responsibility of the managers and supervisors’*.
- iv) The EWRM policy specifies that the UN Secretary-General delegated his fiduciary responsibility for the investments of the Fund to the Representative of the Secretary-General (RSG). The delegated fiduciary responsibility already includes mandatory risk reporting requirements to the UN Secretariat.

**Paragraph 26:** Regarding the statement that ‘the Fund has not formally instituted or mandated a systematic risk identification process, including risk and control self-assessment workshops with relevant process owners and working-level staff, the Fund notes that it has a mandatory and regular process in place for identifying and assessing risks and controls with the involvement of risk and control owners and other functional experts.

Regarding the statement that risk registers reflect a strategic risk view rather than a ground level view of possible control failures, the Fund wishes to clarify that risk assessment results consider both the strategic view from management as well as the input gathered from risk owners and working-level staff. As such, the input gathered from the RCSA workshops would be an input but might not be the ‘primary’ input for updating the Fund’s risk register.

**Paragraph 31:** Regarding the timeline and coverage of fraud risk assessments, the Fund notes that fraud risk assessments will continue to cover key fraud risk scenarios and anti-fraud controls based on risk and materiality criteria. Therefore, fraud risk assessments will not necessarily cover all fraud risks and controls in a certain year. Regarding items c) and d), the Fund further notes that the fraud risk assessments including new fraud scenarios identified and controls tested for OIM were provided to OIOS.

**Paragraph 33:** The Fund notes that there were no issues with the migration of data from Excel risk registers to the governance, risk, and compliance system (GRC) system. The system implementation was a complex undertaking since it involved integrating risk registers for all risk types, control databases, and control testing processes. It is further noted that data clean-up is required for the implementation of any system. The Fund launched the GRC system and related guidelines in September 2025 and was in the process of onboarding users at the time of the audit.