



## **INTERNAL AUDIT DIVISION**

### **REPORT 2025/078**

---

#### **Audit of business continuity and disaster recovery in the Office of Investment Management**

**The Office of Investment Management needed to strengthen governance of the business continuity management system and related processes**

**23 December 2025**

**Assignment No. AT2024-801-02**

# **Audit of business continuity and disaster recovery in the Office of Investment Management**

## **EXECUTIVE SUMMARY**

The Office of Internal Oversight Services (OIOS) conducted an audit of business continuity and disaster recovery in the Office of Investment Management (OIM) of the United Nations Joint Staff Pension Fund. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over business continuity and disaster recovery in OIM. The audit covered the period from January 2022 to June 2025 and included: (a) governance and oversight mechanisms; (b) risk management; and (c) business continuity and disaster recovery procedures.

OIM established a formal Business Continuity and Disaster Recovery governance structure and implemented its Business Continuity Management System based on the international standards. The risk management framework is considered adequate and the organization maintains a comprehensive risk register and a threat catalogue mapped to the organizational assets. However, OIOS noted areas for improvement as well. For example, the manual process for collecting and reporting Key Performance Indicators was inefficient. Furthermore, the lack of a cloud service exit process exposed OIM to business continuity risks. Additionally, there were gaps in the disaster recovery plan, including recovery objectives committed by key service providers being longer than business requirements, and insufficient test scenarios.

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

- Assess options and automate monitoring and reporting of key performance indicators.
- Develop a formal cloud exit process.
- Strengthen its business continuity management by quantifying negative financial and operational impact of known gaps between the business required recovery objectives and objectives committed by the key vendors.
- Strengthen its disaster recovery plan and test program by including additional scenarios related to cybersecurity threats.

OIM 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
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	2
III. AUDIT RESULTS	2-6
A. Governance and oversight mechanisms	2-4
B. Business impact analysis and risk management	4-5
C. Business continuity and disaster recovery procedures	5-6
IV. ACKNOWLEDGEMENT	7
ANNEX I      Status of audit recommendations	
APPENDIX I   Management response	

# **Audit of business continuity and disaster recovery in the Office of Investment Management**

## **I. BACKGROUND**

1. The Office of Internal Oversight Services (OIOS) conducted an audit of business continuity and disaster recovery in the Office of Investment Management (OIM) 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 membership in the Fund. As of 31 December 2024, the Fund comprised 25 member organizations and served around 240,000 participants and beneficiaries. The investments of UNJSPF are managed by OIM which has the fiduciary obligation to manage the Fund's investments in the best long-term interests of its participants and beneficiaries. As of December 2024, OIM managed an asset portfolio of \$95.4 billion.
3. Business continuity and disaster recovery are critical components of an organization's risk management and operational resilience framework. Business continuity refers to an organization's capability to continue delivering products and services within acceptable time frames at predefined capacity during a disruption. Disaster recovery focuses specifically on restoration of ICT systems, data, and infrastructure following a disruptive event.
4. In the context of OIM, ensuring the continuity of operations and the timely recovery of critical systems is essential to protect investment portfolios, and maintain confidence among beneficiaries and stakeholders. Since 2021 OIM has an active ISO 22301<sup>1</sup> certification which guides the structure and requirements for implementing and maintaining the organization's Business Continuity Management System (BCMS).
5. The BCMS is designed to ensure the continuity of OIM's most critical business functions, including trade execution, portfolio management, fixed-income trading, and risk and performance management. Any disruption affecting the investment process can lead to financial losses, erosion of stakeholder trust, and damage to the organization's reputation. This is important, as OIM's increasing reliance on digital platforms, cloud-based services, and third-party providers makes robust business continuity planning and execution even more vital.
6. OIM established a Business Continuity and Disaster Recovery Working Group (the Working Group) serving as the business continuity governance body and providing direction and support for BCMS development and maintenance. The Working Group ensures that: (a) BCMS requirements are integrated into the organization's business processes; (b) BCMS achieves its intended outcomes; and (c) BCMS is being continuously improved.
7. Comments provided by OIM are incorporated in italics.

---

<sup>1</sup> The international standard for Business Continuity Management Systems, providing a framework for organizations to prepare for, respond to, and recover from disruptive incidents.

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

8. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over business continuity and disaster recovery in OIM.

9. This audit was included in the 2025 risk-based work plan of OIOS due to high-risk areas in business continuity and disaster recovery.

10. OIOS conducted this audit from June 2025 to September 2025. The audit covered the period from January 2022 to June 2025. Based on an activity-level risk assessment, the audit covered higher and medium risks areas in business continuity and disaster recovery, which included: (a) governance and oversight mechanisms; (b) risk management; and (c) business continuity and disaster recovery procedures.

11. The audit methodology included: (a) interviews with key personnel, (b) review of relevant documentation, (c) assessment of the client's data management systems, (d) analytical review of data on BCMS management, and (e) process walkthroughs.

12. An analytical review of data included assessing and testing the reliability of data pertaining to business continuity and disaster recovery for accuracy and completeness, as well as a review of related documentation. Based on the review, OIOS determined that the data were sufficiently reliable for the purpose of addressing audit objectives.

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

## **III. AUDIT RESULTS**

### **A. Governance and oversight mechanisms**

#### Governance of Business Continuity Management System was adequate

14. Effectiveness of a business continuity management system depends on existing governance and oversight mechanisms in the organization. In 2018 OIM established a formal multi-tiered governance structure for BCMS which includes the Business Continuity and Disaster Recovery Working Group and the Crisis Management Team. According to the terms of reference, the Working Group was responsible for: (a) ensuring that business continuity policies, strategies, plans and procedures are documented and implemented; (b) identifying all critical suppliers and ensuring their business continuity arrangements are reviewed; and (c) recommending changes to policies, strategies, plans and procedures based on business continuity incidents and identified changes in risks. The Crisis Management Team was ultimately responsible for providing strategic direction and ultimate oversight of BCMS in the event of a crisis.

15. Review of the Working Group meeting minutes confirmed that all meetings followed a comprehensive agenda and covered at minimum: (a) BCMS performance review, (b) business continuity risks and BIA, (c) internal and external issues relevant to BCMS, and (d) opportunities for continual improvement. The Working Group was also responsible for ensuring that BCMS awareness training was provided to OIM personnel. To fulfil this requirement, the organization used an e-learning platform to create and deliver the mandatory BCMS awareness training.

16. The crisis management team meetings conducted on a quarterly basis also covered BCMS items, including changes to the BCMS environment, business continuity test results, status of the risk assessment and business impact analysis. The action items created following the meetings were assigned estimated

completion dates and owners and their status was monitored. For example, a recovery time objective which was not met during the core infrastructure services disaster recovery test conducted in August 2023 was subsequently achieved in the 2024 disaster recovery tests due to the effective engagement of the Crisis Management Team in the remediation process.

#### OIM adopted industry standard for Business Continuity Management System

17. OIM implemented BCMS in compliance with the ISO 22301 international standard. The certification was successfully renewed in March 2024 and remains valid until March 2027. This compliance commitment ensures that the program is structured, auditable, and subject to external validation.

18. BCMS assessments were performed by the United Nations International Computing Centre in 2023 and 2024. The assessments did not result in any non-conformities or observations. Additionally, no active issues were recorded in the register for non-conformities and corrective actions for BCMS. Further, BCMS was aligned with the enterprise-wide risk management policy of UNJSPF.

#### Need to strengthen process for business continuity and disaster recovery monitoring and reporting

19. The OIM business continuity management system requires periodical reporting of the established key performance indicators (KPIs) to the Working Group, the Crisis Management Team and executive management with the objective to strengthen the business continuity monitoring process.

20. OIOS noted that currently the OIM business continuity team manually collects data on KPIs (see Appendix I, example of the BCMS key performance indicators), analyses it and prepares related reports. OIM selected KPIs focusing on metrics that measure the core BCMS objectives, including recovery success, restorability and continuous improvements. The KPIs, such as number of incidents and success rate of business continuity exercises, serve the needs of BCMS, but the current manual collection and reporting process hinders operational efficiency and limits KPI value for continual improvement. For example, the static information on KPIs restricts OIM ability to do trend analysis and identify root causes of related issues.

21. OIOS was of the opinion that the process for periodic reporting on the established KPIs could be improved by automating the data collection and analysis process. The automation will allow OIM to have real-time data on KPIs, perform trend analysis and identify root causes of the business continuity issues for their timely remediation.

**(1) OIM should assess options and automate monitoring and reporting of key performance indicators to strengthen the business continuity management system.**

*OIM accepted recommendation 1 and stated that OIM management will initiate a feasibility study aimed at evaluating potential automation solutions and make a determination whether it is a viable option subject to resources availability.*

#### Need to develop a cloud exit process

22. Best practices for business continuity management emphasize that a framework for cloud service provider management should cover acquisition, use, management and exit from cloud services to prevent business disruptions and data loss.

23. Vendor management procedures lacked a formal cloud exit process to facilitate transition or termination of cloud service providers delivering critical business services. The exit process is critical,

given the organization's heavy reliance on cloud services to support its critical business functions, ranging from specialized platforms that manage the full investment life cycle to office productivity applications. For example, there was no clarity on the procedures to follow in the event of the Microsoft Office 365 agreement termination, whether due to a management decision to discontinue the service or to transition to another vendor. Without a defined cloud exit strategy, OIM may face multiple business continuity risks including operational disruptions and data loss, should it need to transition cloud service providers or terminate contracts with them.

**(2) OIM should develop a formal cloud exit process to strengthen its business continuity management.**

*OIM accepted recommendation 2 and stated that it will develop a standard operating procedure detailing the steps for a formal vendor exit procedure that provides guidance and requirements on exit strategies for all critical vendors.*

## **B. Business impact analysis and risk management**

### Risk management framework was adequate

24. Risk assessment and business impact analysis are essential components of a business continuity management system which required to identify potential threats and assess their impact on critical operations, enabling organizations to prioritize resources and develop effective recovery strategies.

25. OIM conducted a comprehensive risk assessment on an annual basis. The process was guided by a formal methodology ensuring a consistent approach to risk identification, evaluation and treatment. The organization maintained a comprehensive BCMS risk register accompanied by a threat catalogue mapped to the organizational assets. During the last risk assessment exercise, completed in 2024, OIM identified and assessed 23 business continuity risks and 31 information security risks for their monitoring and treatment.

26. OIM also performed business impact analysis (BIA) exercises on an annual basis to identify mission critical ICT services supporting critical business functions, and converted business requirements into quantifiable recovery targets, such as recovery time objective (RTO) and recovery point objective (RPO)<sup>2</sup>. During BIA conducted in 2024, OIM identified critical business functions of 40 business units in OIM and used their operational requirements to update the business continuity strategies. Furthermore, OIM has integrated its network of third-party vendors into BIA, thereby ensuring that assurance received from the vendor business continuity capability review is linked to the specific recovery requirements.

27. OIOS noted that all critical vendors, including providers of ICT infrastructure, investment management, and financial custody services, were identified and mapped to the business processes that they supported. BIA report served as the primary input for developing and refining the organization's business continuity and disaster recovery strategies. The BIA and the risk assessment were integrated into the BCMS structure. The results of both processes were reviewed by the Crisis Management Team, ensuring that OIM management had clear oversight of the organization's current risk posture and critical dependencies.

---

<sup>2</sup> RTO is the time frame within which an asset (product, service, network) must come back online if it goes down. RPO is a time-based measurement of the maximum amount of data loss that is tolerable to an organization in case of an incident.

### Need to quantify operational impact of RTO and RPO gaps from key vendors

28. The OIM business continuity strategy for vendors states that OIM should seek contractual assurance that the key service providers follow the best business continuity and disaster recovery practices and their services meet recovery objectives required by the organization. In case a vendor fails to meet the required recovery objectives, the organization should assess and document the operational and financial impacts resulting from the deficiency.

29. OIM obtained and monitored service level agreements and assurance reports, such as SOC 2<sup>3</sup> reports, for the key vendors. The vendors generally followed good business continuity practices including committed RTOs and RPOs for OIM operations.

30. Through the BIA exercises conducted in collaboration with the business owners, OIM determined acceptable levels of downtime and data loss for the critical business functions and defined required recovery objectives. OIOS review showed that some of the critical business functions in OIM, such as asset and investment management and financial custody services, requested RTOs and RPOs that were shorter than those committed by the respective key vendors. OIM accepted the risk of having longer RTOs and RPOs provided by the vendors, citing cost considerations and without risk quantification. This condition could pose an operational and financial risk to OIM.

**(3) OIM should strengthen its business continuity management by quantifying negative financial and operational impact of known gaps between the business required recovery objectives and those committed by the key vendors.**

*OIM accepted recommendation 3 and stated that it will work to update vendor criticality definition, criteria and threshold, including quantifying the operational and financial impact of a vendor breaching the recovery time objectives. OIM will also update vendor segmentation assessment template accordingly.*

## **C. Business continuity and disaster recovery procedures**

### Disaster Recovery plan for critical ICT systems was adequate

31. The United Nations disaster recovery guidelines and procedures require that a disaster recovery plan should include restoration priorities for each system, recovery objectives, defined roles and responsibilities, procedures and guidelines for restoration, and a detailed list of all dependent systems.

32. OIM developed its disaster recovery plan as a subset of the business continuity plan to focus specifically on restoration of ICT infrastructure, systems and data following a disruptive event. The primary goal of the OIM disaster recovery plan was to restore operations of the critical OIM ICT systems to full processing capabilities within the pre-defined RTOs established through BIA exercise. The plan outlined the crisis management roles, devolving chain of command, contact details and specific roles and responsibilities for the various IT recovery teams.

33. The scope of the disaster recovery plan was focused on the recovery of critical hosted ICT infrastructure and recovery of OIM business critical applications which are hosted either in the cloud or with other providers. OIOS noted that the critical ICT systems listed in the organization's configuration

---

<sup>3</sup> A report for service organizations that store, process, or handle customer data. It demonstrates compliance with controls related to security, availability, processing integrity, confidentiality and privacy.

management database<sup>4</sup>, including Windows and Linux servers, network equipment firewalls and switches, were covered by specific recovery strategies, such as backup or replication. Furthermore, the plan was supported by technical recovery procedures for the critical applications directly supported by the OIM infrastructure team, validating its alignment with the business needs.

#### Need to strengthen disaster recovery test planning

34. A disaster recovery plan should incorporate representative test scenarios based on real-life threats to ensure its effectiveness in safeguarding business-critical ICT systems in the event of a significant disruption. Conducting disaster recovery tests allows an organization to ensure that the business continuity arrangements are accurate, complete and up to date. OIM relies on an annually updated business continuity test program to verify the effectiveness of the business continuity arrangements and their accuracy.

35. The tests were planned and executed annually, ensuring that critical areas are reviewed in a structured cycle and covered various scenarios, including the core ICT infrastructure failover and loss of the primary data centre. The tests also included validation of the failover of core vendor platforms, data backup restoration, and dedicated exercises for highly critical functions such as equity trading and fund transfers. OIM also conducted tabletop exercises to validate crisis management and communication response to cybersecurity incidents. The test results were subjected to formal management review and sign-off by relevant business owners and IT focal points, ensuring that test outcomes were officially recognized and accountability for deficiencies was established.

36. OIOS review of a disaster recovery test sample confirmed that test results were translated into concrete procedural improvements. Test reports captured deficiencies identified during the tests, driving updates to the operational documentation. For instance, a disaster recovery test of OIM ICT infrastructure conducted in August 2023, exposed the need for greater technical clarity for the configuration of several network services, leading to a subsequent update to the related recovery runbook and procedures.

37. However, OIOS noted that the test program did not incorporate critical real-life scenarios, for instance, responding to a major cybersecurity incident such as a ransomware attack that corrupts critical databases and compromises data integrity or disrupts system access. Instead, it focused on traditional scenarios such as infrastructure and connectivity services failure, emergency notification testing and execution of manual trades. This condition could result in extended outages and data loss due to ineffective traditional recovery plans.

**(4) OIM should strengthen its disaster recovery plan and test program by including additional scenarios related to cybersecurity threats.**

*OIM accepted recommendation 4 and stated that it will develop a cyber ransomware recovery procedure and incorporate this in its business continuity test program.*

---

<sup>4</sup> A centralized repository that stores information about an organization's IT assets and their attributes.

#### **IV. ACKNOWLEDGEMENT**

38. OIOS wishes to express its appreciation to the management and staff of the Office of Investment Management 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 business continuity and disaster recovery in the Office of Investment Management

Rec. no.	Recommendation	Critical <sup>5</sup> / Important <sup>6</sup>	C/ O <sup>7</sup>	Actions needed to close recommendation	Implementation date <sup>8</sup>
1	OIM should assess options and automate monitoring and reporting of key performance indicators to strengthen the business continuity management system.	Important	O	Receipt of evidence OIM has assessed and automated monitoring and reporting of key performance indicators.	31 December 2026
2	OIM should develop a formal cloud exit process to strengthen its business continuity management.	Important	O	Receipt of evidence that a formal cloud exit process has been developed.	31 December 2026
3	OIM should strengthen its business continuity management by quantifying negative financial and operational impact of known gaps between the business required recovery objectives and those committed by the key vendors.	Important	O	Receipt of evidence OIM has implemented a process to quantify operational and financial impact of vendors breaching the recovery time objectives.	30 June 2026
4	OIM should strengthen its disaster recovery plan and test program by including additional scenarios related to cybersecurity threats.	Important	O	Receipt of evidence that scenarios related to cybersecurity threats have been incorporated into the disaster recovery test program.	30 June 2026

<sup>5</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>6</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>7</sup> Please note the value C denotes closed recommendations whereas O refers to open recommendations.

<sup>8</sup> Date provided by [entity] in response to recommendations. [Insert "Implemented" where recommendation is closed; (implementation date) given by the client.]

# **APPENDIX I**

## **Management Response**

Management Response

Audit of business continuity and disaster recovery in the Office of Investment Management

Rec. no.	Recommendation	Critical <sup>9</sup> / Important <sup>10</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OIM should assess options and automate monitoring and reporting of key performance indicators to strengthen the business continuity management system.	Important	Yes	Chief of IT	Q4 2026	OIM acknowledges the audit recommendation to automate monitoring and reporting of key performance indicators to the Business Continuity Management System (BCMS). OIM concurs with the observation that current BCMS processes are largely manual, which may impact efficiency, consistency, and scalability. To address this, OIM management will initiate a feasibility study aimed at evaluating potential automation solutions and make a determination whether it is a viable option subject to resources availability.
2	OIM should develop a formal cloud exit process to strengthen its business continuity management.	Important	Yes	Head of Vendor Management	Q4 2026	OIM will develop a Standard Operating Procedure (SOP) detailing the steps for a formal vendor exit/termination procedure that provides guidance and requirements on exit strategies for all critical vendors (i.e. Tier 1). OIM will also develop a Vendor Exit template which will cover areas such as cloud, data, access, financial, roles and responsibilities, etc.

<sup>9</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>10</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.

## Management Response

## Audit of business continuity and disaster recovery in the Office of Investment Management

Rec. no.	Recommendation	Critical <sup>9</sup> / Important <sup>10</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
3	OIM should strengthen its business continuity management by assessing financial and operational impact of known gaps in the recovery time objective and recovery point objective committed by the key vendors.	Important	Yes	Head of Third-Party Risk Management	Q2 2026	Second line TPRM function will work alongside various first line functions including the Enterprise Vendor Management Office (EVMO) and the Business Continuity Management (BCM) team to deliver the following outcomes: <ol style="list-style-type: none"> <li>1) Updated definition of vendor criticality which is based on the degree of importance, reliance and impact in the event of service failure or unavailability.</li> <li>2) Updated vendor criticality criteria and thresholds, which includes quantifying the operational and financial impact of the vendor breaching the RTO.</li> <li>3) Updated Vendor Segmentation Assessment (VSA) template, owned by the EVMO team, which reflects the latest impact categories and thresholds.</li> </ol>
4	OIM should strengthen its disaster recovery plan and test program by including additional scenarios related to cybersecurity threats.	Important	Yes	Chief Information Security Officer	Q2 2026	OIM recognizes the importance of cybersecurity within the Business Continuity Management System (BCMS) and conducts table-top exercises that simulate cybersecurity scenarios. Furthermore, OIM is actively sourcing for a Cyber Insurance cover. To address this area of improvement, OIM will develop a Cyber/Ransomware

**Management Response**

**Audit of business continuity and disaster recovery in the Office of Investment Management**

Rec. no.	Recommendation	Critical <sup>9</sup> / Important <sup>10</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						recovery procedure and incorporate this in its BC test program.