Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2024/042

Audit of business continuity and disaster recovery at the Pension Administration of the United Nations Joint Staff Pension Fund

The Pension Administration needs to strengthen business continuity and disaster recovery processes, including organizational resilience

10 September 2024
Assignment No. AT2023-800-02

Audit of business continuity and disaster recovery at the Pension Administration of the United Nations Joint Staff Pension Fund

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of business continuity and disaster recovery at the Pension Administration of the United Nations Joint Staff Pension Fund. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the effective management of business continuity and disaster recovery at the Pension Administration. The audit covered the period from January 2021 to June 2024 and included a review of: (a) governance and risk management; (b) organizational resilience; and (c) recovery policies and procedures.

The audit showed that the Pension Administration needs to strengthen business continuity and disaster recovery processes, including organizational resilience.

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

- Strengthen the mitigation of cloud-specific risks by: conducting periodic tests and simulation exercises to validate the effectiveness of the related controls; and implementing mechanisms for continuous monitoring of the cloud environment, emerging threats, and for updating the business continuity and disaster recovery plan as necessary;
- Conduct annual internal self-assessments and gap analyses of its business continuity and disaster recovery practices to identify areas for remediation and improvement;
- Establish a detailed methodology for consistently assessing and reporting the performance against the criteria in the business continuity and disaster recovery plan; and integrate metrics and analysis relating to disaster recovery incidents, the related response time, incident impact and recovery times into the performance dashboard;
- Develop a comprehensive organizational resilience policy that includes: guidelines for anticipating, preparing for and responding to a range of internal and external threats; a plan for coordination and collaboration among all relevant stakeholders; and metrics and monitoring tools to evaluate the effectiveness of organizational resilience;
- Develop a comprehensive training plan for business continuity and disaster recovery that includes real use case scenarios and periodic awareness sessions for its staff;
- Expand the scope of disaster recovery testing to include a broader range of scenarios, incorporating cybersecurity threats and emerging risks into testing protocols; establish mechanisms for periodic review and update of disaster recovery scenarios to reflect evolving threats and risks; and test the incident response plan periodically to mitigate incidents proactively; and
- Identify potential disruption scenarios, their impact on Client Services and communication, and appropriate response procedures; implement formal guidance for Client Services and contact centres detailing scenario-based responses and escalation procedures; and establish a formal procedure for activating contact centres including delineation of clear roles, responsibilities and escalation protocols during a disaster.

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

CONTENTS

Audit of business continuity and disaster recovery at 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 business continuity and disaster recovery at 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 staff of the United Nations and other organizations admitted to its membership. The Finance function of the Pension Administration was centralized in New York, whereas other functions (such as client services, pension entitlements and records management) were performed by the New York and Geneva Offices, each serving a separate set of member organizations.

3. Business continuity is defined as an organization's capability to continue delivering products and services within acceptable timeframes at a predefined capacity during a disruption. A business continuity plan is an enterprise-wide set of processes and instructions to ensure the continuation of business processes, including information and communications technology (ICT), in the event of a disruption. It provides the plans for the enterprise to recover from minor incidents (e.g., localized disruptions of business components) to major disruptions (e.g., fire, natural disasters, extended power failures, and equipment/ telecommunications failure). Business continuity plans are to be supported by ICT disaster recovery plans, including recovery strategies to ensure quick and effective recovery following a disruption.

4. UNJPSF had constituted a business continuity/recovery working group (hereafter referred to as "the Working Group") composed of members from the Pension Administration and the Office of Investment Management (OIM) to serve as the dedicated governance mechanism to review and address ongoing business continuity/recovery matters. The objective of the Working Group was to coordinate the tasks required for developing and maintaining an effective business continuity management system based on business impact analysis and testing of business continuity scenarios.

5. The Risk Management Unit (RMU) in the Pension Administration conducted annual business continuity risk assessments and business impact analyses in coordination with business units. RMU is responsible for ensuring that the procedures contained in the business continuity and disaster recovery plan are regularly reviewed and updated in coordination with the relevant functions and in alignment with the business continuity management policy and related requirements. RMU also served as the secretariat of the Working Group and documented disaster recovery test plans and test results, including lessons learned and corrective actions as required.

6. The Information Management Systems Service (IMSS) within the Pension Administration is responsible for providing and maintaining ICT systems and services and coordinating the implementation of strategic decisions made by the Pension Administration. IMSS had outsourced the following ICT services to a United Nations agency: (a) data centre management; (b) server hosting; (c) data storage and backup services; (d) email and messaging; (e) desktop management services (file and print services, Active Directory administration); (f) network management (partially); and (j) disaster recovery server hosting. IMSS was also responsible for conducting disaster recovery tests and resolving related issues.

7. The ICT infrastructure of the Pension Administration was hosted in two data centres in New Jersey and Geneva, and the server room at the Dag Hammarskjold Plaza. At the time of the audit, critical applications and systems including data centres were planned to be migrated to a private cloud client by the end of September 2024.

8. Comments provided by the Pension Administration are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

9. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the effective management of business continuity and disaster recovery at the Pension Administration.

10. This audit was included in the 2023 risk-based work plan of OIOS due to high risks related to business continuity and disaster recovery which are critical to the Pension Administration's operations.

11. OIOS conducted this audit from February to June 2024. The audit covered the period from January 2021 to June 2024. Based on an activity-level risk assessment, the audit covered risk areas in business continuity and disaster recovery which included: (a) governance and risk management; (b) organizational resilience; and (c) recovery policies and procedures.

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

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

III. AUDIT RESULTS

A. Governance and risk management

<u>Need to assess and consider cloud-specific risks in the business continuity and disaster recovery plan</u>

14. Business continuity and disaster recovery plans should address the risks associated with the migration of critical applications and data centres into a cloud environment by identifying and mitigating cloud-specific risks to safeguard sensitive data, prevent data loss and ensure uninterrupted services to the Fund's participants and beneficiaries.

15. The Pension Administration had planned to migrate by the end of September 2024 its critical applications and data centres from an on-premises infrastructure managed by a United Nations agency to a private cloud client managed by a leading cloud service provider. The Pension Administration informed the Working Group that the move to the cloud would change the business continuity risks, and that the overall risk was lower as it will adopt an expedited multi-site disaster recovery, increased automation (which decreased the chances of error), and robust testing. Further, the Working Group was given details about the automatic data synchronization and activation of primary and secondary data centres during disruption. At the time of audit, several critical ICT services had been moved to the cloud, while other critical services including the Integrated Pension Administration System (IPAS) and new systems such as Kofax and customer relationship management were being migrated.

16. At the time of the audit, the Pension Administration was yet to incorporate in its existing business continuity and disaster recovery plan the cloud-specific business continuity/disaster recovery risks such as data security and privacy, data loss, service availability and performance, data backup and recovery, change management and version control, dependency on third-party providers, and incident response and recovery

planning. This is essential to effectively safeguard the interests of the Fund's participants and beneficiaries and ensure the resilience of critical operations in the cloud environment.

(1) The Pension Administration should strengthen the mitigation of cloud-specific risks by: (a) conducting periodic tests and simulation exercises to validate the effectiveness of the related controls; and (b) implementing mechanisms for continuous monitoring of the cloud environment, emerging threats, and for updating the business continuity and disaster recovery plan as necessary.

The Pension Administration accepted recommendation 1 and stated that as part of the migration to the cloud project, it records all risks and issues and identifies remediation actions. The Pension Administration will conduct periodic tests to validate the effectiveness of the recovery controls implemented in the cloud environment. Also, the Pension Administration has adopted and implemented procedures and tools to monitor the availability of the cloud environment and related threats. Existing monitoring will enable revising recovery procedures as required.

Need to strengthen business continuity and disaster recovery in accordance with policy

17. The Pension Administration's business continuity management policy provides that the business continuity system will incorporate the 'ISO/IEC 22301: 2019 Security and Resilience - Business Continuity Management Systems' guidance and requirements. Also, according to the business continuity and disaster recovery plan of the Pension Administration, an internal self-assessment would be conducted annually to ensure proper implementation of the business continuity management system, and conformity with the requirements of ISO/IEC 22301. Further, details of the internal self-assessment were to be defined in the plan, and the results were to be reported to the Deputy Chief Executive and relevant managers. The Pension Administration stated that the internal self-assessment verifies compliance against the ISO 22301 standard, and the Working Group regularly monitors the implementation and effectiveness of the business continuity and recovery arrangements.

18. OIOS' review indicated that the internal self-assessment had not been conducted since 2018 to assess the implementation of business continuity management in the Pension Administration. Consequently, the Pension Administration had limited visibility as to: (a) the effectiveness of its business continuity management; (b) areas of non-conformance or gaps which could potentially increase its vulnerability to disruption; (c) potential gaps in resilience and preparedness for mitigation and recovery from business continuity incidents; and (d) accountability and oversight in ensuring compliance with business continuity standards and protocols.

(2) The Pension Administration should conduct annual internal self-assessments and gap analyses of its business continuity and disaster recovery practices to identify areas for remediation and improvement.

The Pension Administration accepted recommendation 2 and stated that it will conduct an annual internal self-assessment and gap analysis of its business continuity and disaster recovery practices.

Need to strengthen performance monitoring and evaluation for business continuity and disaster recovery

19. According to the business continuity and disaster recovery plan, the Pension Administration will use key performance indicators, assessment criteria and targets to review and report the performance and effectiveness of its business continuity and disaster recovery.

20. Pension Administration had developed a performance dashboard to present the performance and effectiveness of its business continuity and disaster recovery process. However, the results were not compared against the criteria in the business continuity and disaster recovery plan in their entirety to have a realistic reflection of facts. Also, there was not enough granularity in performance monitoring to reflect how the targets relating to business continuity and disaster recovery were met. Further, the performance dashboard did not include figures relating to handling and response to disaster recovery incidents which further limits its use as a performance monitoring and evaluation tool.

21. This condition may lead to inaccurate assessment of the performance and effectiveness of business continuity and disaster recovery. Limited incident handling and response metrics may also hinder the Pension Administration's ability to identify and address potential gaps in the disaster recovery process.

(3) The Pension Administration should: (a) establish a detailed methodology for consistently assessing and reporting the performance against the criteria in the business continuity and disaster recovery plan; and (b) integrate metrics and analysis relating to disaster recovery incidents, the related response time, incident impact and recovery times into the performance dashboard.

The Pension Administration accepted recommendation 3 and stated that it will enhance the performance monitoring methodology and add metrics related to the handling and response to disaster recovery incidents in the business continuity performance dashboard.

B. Organizational resilience

Need to develop an organizational resilience policy and plan for the Pension Administration

22. The Pension Administration's current business continuity and disaster recovery plan was well defined, outlining the crisis management roles, reporting relationship, chain of command, escalation procedures and contact details for the crisis management team and members of recovery and support teams. Periodic tests were conducted to ensure the effectiveness and timeliness of these plans. However, there was no policy or formal mechanism on organizational resilience to systematically anticipate, prepare for and respond to threats and opportunities arising from sudden or gradual changes in the Pension Administration's internal and external environment.

23. The Pension Administration had defined the scope of business continuity activities to cover crisis, disasters and emergencies only. However, there could be incidents affecting organizational resilience and continuity of operations that may not fall under the definition of a crisis (significant impact), disaster or emergency (immediate threat). For example, events such as physical closure of one of the offices may not be considered as an issue from the business continuity and disaster recovery perspective because it does not fall under the scope of a crisis, disaster or emergency. Lessons drawn by the United Nations Office at Geneva were not formally integrated into the Pension Administration's organizational resilience mechanisms, thereby limiting the Pension Administration's capability to anticipate, prepare for and respond to events arising from sudden or gradual changes in its internal and external environment, especially those that develop gradually or originate from external changes (such as adoption of the cloud, or from the legacy IPAS to the new Velocity), unexpected disruption (physical closure of premises), or changes that are not covered by existing business continuity and disaster recovery plans.

(4) The Pension Administration should develop a comprehensive organizational resilience policy that includes: (a) guidelines for anticipating, preparing for and responding to a range of internal and external threats; (b) a plan for coordination and collaboration

among all relevant stakeholders; and (c) metrics and monitoring tools to evaluate the effectiveness of organizational resilience.

The Pension Administration accepted recommendation 4 and stated that it will develop an organizational resilience policy covering: (a) guidelines for handling internal and external threats; (b) coordination and collaboration mechanisms among relevant stakeholders; and (c) metrics and monitoring mechanisms to assess the effectiveness of organizational resilience.

Need to strengthen awareness amongst all stakeholders

24. According to the business continuity and disaster recovery plan of the Pension Administration, it will implement an annual work plan of training and awareness to ensure that staff with business continuity responsibilities have the required awareness and competencies to perform their roles effectively.

25. The Pension Administration stated that regular business continuity training/briefings were conducted, and awareness materials were available on the intranet. Additionally, prior to each business continuity and disaster recovery test, briefing was provided to the recovery teams, and crisis management simulation exercises help reinforce managers' response to crisis, disaster or emergency scenarios. OIOS' interviews with key managers indicated that more awareness and dissemination of information was needed on business continuity and disaster recovery as well as crisis management because many staff members were not aware of where to look for relevant guidance, and what their roles should be in a disaster scenario if their supervisor is also impacted by the disaster and does not have the capability to provide instructions. Also, the consultants who led the two crisis management simulation exercises conducted in March 2022 and May 2023 had advised the Fund to consider real use cases (rather than hypothetical) and develop specific materials for training sessions, as well as scenario plans and tabletop exercises so that stakeholders may relate to them and understand them better.

(5) The Pension Administration should develop a comprehensive training plan for business continuity and disaster recovery that includes real use case scenarios and periodic awareness sessions for its staff.

The Pension Administration accepted recommendation 5 and stated that it will enhance the business continuity and disaster recovery training plan to consider a range of disruption scenarios, and awareness sessions for staff.

C. Recovery policies and procedures

Need to strengthen the selection of scenarios for disaster recovery tests

26. Business continuity and disaster recovery tests aim to assess the Pension Administration's preparedness to activate and execute the recovery scenarios defined in the plan. Disaster recovery tests should incorporate representative scenarios based on real-life threats to ensure the effectiveness of the recovery plan in safeguarding critical business functions in the event of a disaster.

27. OIOS' review indicated that the disaster recovery tests did not include scenarios when critical business functions (including email and SharePoint) may be impacted by cybersecurity threats (except for the tabletop exercise conducted in December 2023, which considered a scenario based on cybersecurity), or emerging risks such as social engineering. Also, real-life scenarios and organization-specific materials need to be used for scenario plans and tabletop exercises to assure that critical business functions will be effectively recovered in the event of a disaster.

28. The Pension Administration’s incident management process and procedure defined an incident as an unplanned interruption or reduction in the quality of an information technology service. Currently, the purpose of the incident management process in the Pension Administration was to monitor and manage the progress of all incidents until service was restored to users. This approach was reactive in nature, whereas an incident response plan should proactively aim to detect, contain and manage incidents. Periodic tests of incident response plans are required to enable the Fund to deal with cybersecurity incidents efficiently and effectively to minimize their consequences and strengthen organizational resilience.

(6) The Pension Administration should: (a) expand the scope of disaster recovery testing to include a broader range of scenarios, incorporating cybersecurity threats and emerging risks into testing protocols; (b) establish mechanisms for periodic review and update of disaster recovery scenarios to reflect evolving threats and risks; and (c) test the incident response plan periodically to mitigate incidents proactively.

The Pension Administration accepted recommendation 6 and stated that it will: (a) expand the scope of disaster recovery tests to cover varied scenarios, emerging risks and threats; (b) consider the results of risk assessments and business impact analysis to identify relevant risks and threats for disaster recovery scenarios; and (c) schedule regular tests of the incident response plan.

Need to strengthen procedures for activating contact centre and escalation mechanism

29. A contact centre should have scripted guidelines detailing scenario-based responses to ensure timely and effective communication with clients, especially during disaster scenarios.

30. Client Services is responsible for day-to-day interactions with clients, providing key information and responding to queries received through the Fund’s website, telephone calls received by the contact centres located in Valencia and New York managed by a United Nations agency, and outreach activities. Disruption of Client Services in a disaster scenario could significantly impact participants and beneficiaries.

31. In a disaster scenario where the disruption is severe, and the Pension Administration’s operations are impacted for an extensive period (e.g., 5 days or more), Client Services is expected to do the following: (a) confirm that the UNJSPF website is operational; (b) based on the availability of the website, and depending on the severity of the disruption, communicate to UNJSPF stakeholders; (c) if applicable, inform stakeholders of unavailability of walk-ins or other functions during the disruption and advise alternative mechanisms; and (d) continue answering calls (Tier 1) and client queries received through the UNJSPF website.

32. OIOS noted that there were no scripted guidelines for the contact centre detailing the disaster scenario-based expected response to enable them to follow the right process and escalation procedure in the most-timely manner. This weakness could lead to delays or inconsistencies in responding to client queries or providing key information during disaster scenarios.

(7) The Pension Administration should: (a) identify potential disruption scenarios, their impact on Client Services and communication, and appropriate response procedures; (b) implement formal guidance for Client Services and contact centres detailing scenario-based responses and escalation procedures; and (c) establish a formal procedure for activating contact centres including delineation of clear roles, responsibilities and escalation protocols during a disaster.

The Pension Administration accepted recommendation 7 and stated that it will: (a) identify and assess the impact of disruptions impacting Client Services; and (b) develop a procedure and guidance for Client Services and contact centre staff with responses and escalation for various scenarios, specifying activation procedures with roles assigned to contact centre staff.

IV. ACKNOWLEDGEMENT

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

Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity and disaster recovery at the Pension Administration of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	The Pension Administration should strengthen the mitigation of cloud-specific risks by: (a) conducting periodic tests and simulation exercises to validate the effectiveness of the related controls; and (b) implementing mechanisms for continuous monitoring of the cloud environment, emerging threats, and for updating the business continuity and disaster recovery plan as necessary.	Important	O	Receipt of evidence that the mitigation of cloud-specific risks strengthened by: (a) conducting periodic tests and simulation exercises to validate the effectiveness of the related controls; and (b) implementing mechanisms for continuous monitoring of the cloud environment, emerging threats, and for updating the business continuity and disaster recovery plan as necessary.	31 March 2025
2	The Pension Administration should conduct annual internal self-assessments and gap analysis of its business continuity and disaster recovery practices to identify areas for remediation and improvement.	Important	O	Receipt of evidence that annual internal self-assessments and gap analysis of its business continuity and disaster recovery practices were conducted to identify areas for remediation and improvement.	31 March 2025
3	The Pension Administration should: (a) establish a detailed methodology for consistently assessing and reporting the performance against the criteria in the business continuity and disaster recovery plan; and (b) integrate metrics and analysis relating to disaster recovery incidents, the related response time, incident impact and recovery times into the performance dashboard.	Important	O	Receipt of evidence that: (a) a detailed methodology for consistently assessing and reporting the performance against the criteria in the business continuity and disaster recovery plan established; and (b) metrics and analysis relating to disaster recovery incidents, the related response time, incident impact and recovery times integrated into the performance dashboard.	31 March 2025
4	The Pension Administration should develop a comprehensive organizational resilience policy that includes: (a) guidelines for anticipating, preparing for and responding to a range of internal and external threats; (b) a plan for coordination and collaboration	Important	O	Receipt of evidence that a comprehensive organizational resilience policy developed that includes:(a) guidelines for anticipating, preparing for and responding to a range of internal and external threats; (b) a plan for coordination and	31 March 2025

[1] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

[2] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

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

[4] Date provided by the Pension Administration in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity and disaster recovery at the Pension Administration of the United Nations Joint Staff Pension Fund

	among all relevant stakeholders; and (c) metrics and monitoring tools to evaluate the effectiveness of organizational resilience.			collaboration among all relevant stakeholders; and (c) metrics and monitoring tools to evaluate the effectiveness of organizational resilience.	
5	The Pension Administration should develop a comprehensive training plan for business continuity and disaster recovery that includes real use case scenarios and periodic awareness sessions for its staff.	Important	O	Receipt of evidence that a comprehensive training plan for business continuity and disaster recovery developed that includes real use case scenarios and periodic awareness sessions for its staff.	31 October 2025
6	The Pension Administration should: (a) expand the scope of disaster recovery testing to include a broader range of scenarios, incorporating cybersecurity threats and emerging risks into testing protocols; (b) establish mechanisms for periodic review and update of disaster recovery scenarios to reflect evolving threats and risks; and (c) test the incident response plan periodically to mitigate incidents proactively.	Important	O	Receipt of evidence that: (a) the scope of disaster recovery testing expanded to include a broader range of scenarios, incorporating cybersecurity threats and emerging risks into testing protocols; (b) mechanisms for periodic review and update of disaster recovery scenarios established to reflect evolving threats and risks; and (c) the incident response plan tested periodically to mitigate incidents proactively.	31 October 2025
7	The Pension Administration should: (a) identify potential disruption scenarios, their impact on Client Services and communication, and appropriate response procedures; (b) implement formal guidance for Client Services and contact centres detailing scenario-based responses and escalation procedures; and (c) establish a formal procedure for activating contact centres including delineation of clear roles, responsibilities and escalation protocols during a disaster.	Important	O	Receipt of the evidence that: (a) potential disruption scenarios, their impact on Client Services and communication, and appropriate response procedures have been identified; (b) formal guidance for Client Services and contact centres detailing scenario-based responses and escalation procedures implemented; and (c) a formal procedure for activating contact centres including delineation of clear roles, responsibilities and escalation protocols during a disaster established.	31 March 2025

APPENDIX I

Management Response

UNJSPF

EPPO FAO IAEA ICGEB ICCROM ICAO ICC IFAD ILO IMO IOM IPU
ISA ITU ITLOS STL UN UNESCO UNIDO UNWTO WHO WIPO WMO

CCPPNU

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

MEMORANDUM

Ref: UNJSPF/CEPA/06092024

New York, 6 September 2024

To / A: Mr. Byung-Kun Min, Director Internal Audit Division, OIOS

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

Subject / Objet: **<u>UNJSPF response to draft report audit of business continuity and disaster recovery in the Pension Administration</u>**

1. Reference is made to your memorandum dated 23 August 2024, in which you submitted for the Fund’s review and comments, the draft report of the above-mentioned audit.

2. As requested, the Pension Administration’s comments to the audit recommendations are included in **<u>Annex I</u>**.

3. The Pension Administration would like to express its appreciation to OIOS auditors for the constructive exchanges with management and valuable recommendations made.

cc.: Mr. D. Penklis, Deputy Chief Executive
Mr. J. Nunez, Chief Risk and Compliance Officer
Mr. D. Dell’Accio, Chief Information Officer
Ms. M. O’Donnell, Chief of Operations
Mr. A. Blythe, Chief Client Services
Ms. K. Manosalvas, Audit Focal Point

ANNEX I
Audit of business continuity and disaster recovery in the Pension Administration

.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Responsible	Implementation date	Client comments
1	The Pension Administration should strengthen the mitigation of cloud-specific risks by: (a) conducting periodic tests and simulation exercises to validate the effectiveness of the related controls; and (b) implementing mechanisms for continuous monitoring of the cloud environment, emerging threats, and for updating the business continuity and disaster recovery plan as necessary.	Important	Yes	Enterprise Operations Section	March 2025	a) As part of the migration to the Cloud project, the Fund records all risks and issues and identifies remediation actions. The Fund will conduct periodic tests to validate the effectiveness of the recovery controls implemented in the Cloud environment; b) The Fund has implemented procedures and tools to monitor the availability of the Cloud environment and related threats. Existing monitoring will enable revising recovery procedures as required.
2	The Pension Administration should conduct annual internal self-assessments and gap analyses of its business continuity and disaster recovery practices to identify areas for remediation and improvement.	Important	Yes	Risk Management	March 2025	The Pension Administration will conduct an annual internal self-assessment and gap analysis of its business continuity and disaster recovery practices.
3	The Pension Administration should: (a) establish a detailed methodology for consistently assessing and reporting the performance against the criteria in the business continuity and disaster recovery plan; and (b) integrate metrics and	Important	Yes	Risk Management	March 2025	The Pension Administration will: a) enhance the performance monitoring methodology; and b) add metrics related to the handling and response to disaster recovery incidents in

[1] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

[2] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Responsible	Implementation date	Client comments
	analysis relating to disaster recovery incidents, the related response time, incident impact and recovery times into the performance dashboard.					the business continuity performance dashboard.
4	The Pension Administration should develop a comprehensive organizational resilience policy that includes: (a) guidelines for anticipating, preparing for and responding to a range of internal and external threats; (b) a plan for coordination and collaboration among all relevant stakeholders; and (c) metrics and monitoring tools to evaluate the effectiveness of organizational resilience.	Important	Yes	Risk Management	March 2025	The Fund will develop an organizational resilience policy covering: a) guidelines for handling internal and external threats; b) coordination and collaboration mechanisms among relevant stakeholders; and c) metrics and monitoring to assess the effectiveness of organizational resilience.
5	The Pension Administration should develop a comprehensive training plan for business continuity and disaster recovery that includes real use case scenarios and periodic awareness sessions for its staff.	Important	Yes	Risk Management, BSS/Training	October 2025	The Fund will enhance the business continuity and disaster recovery training plan to consider a range of disruption scenarios, and awareness sessions for staff.
6	The Pension Administration should: (a) expand the scope of disaster recovery testing to include a broader range of scenarios, incorporating cybersecurity threats and emerging risks into testing protocols; (b) establish mechanisms for periodic review and update of disaster recovery scenarios to reflect evolving threats and risks; and (c) test the incident response plan periodically to mitigate incidents proactively.	Important	Yes	Enterprise Operations Section	October 2025	The Fund will: a) Expand the scope of disaster recovery tests to cover varied scenarios, emerging risks and threats; b) The results of risk assessments and business impact analysis will be considered to identify relevant risks and threats for disaster recovery scenarios; c) Schedule regular tests of the incident response plan.

.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Responsible	Implementation date	Client comments
7	The Pension Administration should: (a) identify potential disruption scenarios, their impact on Client Services and communication, and appropriate response procedures; (b) implement formal guidance for Client Services and contact centres detailing scenario-based responses and escalation procedures; and (c) establish a formal procedure for activating contact centres including delineation of clear roles, responsibilities and escalation protocols during a disaster.	Important	Yes	Client Services	March 2025	The Fund will: a) identify and assess the impact of disruptions impacting Client Services; b) develop a procedure and guidance for Client Services and Contact Center staff with responses and escalation for various scenarios; and specify activation procedures and roles assigned to Contact Centre staff.