Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2017/037

Audit of business continuity and disaster recovery in the secretariat of the United Nations Joint Staff Pension Fund

There was need to align the business continuity strategy with the results of the business impact analysis and ensure completeness of the related procedures and tests

19 May 2017
Assignment No. AT2015/800/02

Audit of business continuity and disaster recovery in the secretariat of the United Nations Joint Staff Pension Fund

EXECUTIVE SUMMARY

The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over effective and efficient management of the business continuity and disaster recovery in the secretariat of the United Nations Joint Staff Pension Fund (UNJSPF). The audit covered the period January 2015 to February 2017 and included a review of business continuity and disaster recovery processes in the Fund secretariat.

The UNJSPF secretariat had determined that monthly payroll processing for all current retirees and beneficiaries worldwide was the core activity requiring business continuity and disaster recovery planning. Except for payroll processing, the Fund's strategy did not include recovery plans for other core processes (such as client services and pension entitlements), even though their impact in the event of a disaster was assessed as "high" or "catastrophic". There was need to align the Fund's business continuity strategy with the results of its business impact analysis and ensure the completeness of the related procedures and tests to ensure an adequate response in the event of a disruption.

OIOS made 6 recommendations. To address issues identified in the audit, the Fund needed to:

- Strengthen its business impact analysis process by assessing the impact of unavailability of information and communications technology (ICT) systems and internal/external service dependencies;
- Update its business continuity strategy taking into consideration its own assessment of the "high"/"catastrophic" impact of outage of core business processes such as client services and pension entitlements; and document the business continuity procedures to be followed for these processes in the event of an outage;
- Implement payroll reconciliation reports in the Integrated Pension Administration System (IPAS) to mitigate the risk of erroneous payroll in the event of a disruption entailing the unavailability of its New York staff to perform manual reconciliations;
- Document disaster recovery plans and procedures for all of its critical ICT systems; and clarify and communicate the roles and responsibilities of ICT recovery team members including vendors and service providers;
- Update its configuration management database with a full inventory of hardware and software directly or indirectly linked to its critical systems; and perform periodic assessment of these dependencies as part of disaster recovery planning; and
- Enhance the testing of its business continuity and disaster recovery plans by: documenting the disaster scenarios to be tested; and including the activation of disaster recovery systems such as IPAS, e-mail and shared drives in its testing activities.

The UNJSPF Secretariat did not accept four recommendations. OIOS maintains that these recommendations relate to significant residual risks that need to be mitigated. These unaccepted recommendations have been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risks.

CONTENTS

Audit of business continuity and disaster recovery in the secretariat 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 in the secretariat of the United Nations Joint Staff Pension Fund (UNJSPF).

2. UNJSPF was established by the General Assembly to provide retirement benefits and social security protection (death, disability and other related benefits) for the staff of the United Nations and 23 other member organizations. The services provided by the UNJSPF secretariat included: (i) paying retirement, disability, death and other related benefits; (ii) calculating, processing and maintaining entitlements; (iii) establishing and maintaining records for all participants and pensioners/beneficiaries; (iv) collecting, pooling and reconciling contributions; and (v) responding to inquiries of participants, retirees and beneficiaries. The Fund secretariat's Operations (i.e., client services, pension entitlements and records management) were performed by both the New York and Geneva Offices, each office serving a separate set of member organizations.

3. A business continuity plan is an enterprise-wide group of processes and instructions to ensure the continuation of business processes – including, but not limited to, information and communications technology (ICT) – in the event of an interruption. 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, equipment and/or 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 established a business continuity/recovery working group in 2007 composed of members from the Fund secretariat and the Investment Management Division (IMD) with the mandate to: (i) coordinate business continuity and disaster recovery activities; (ii) develop plans and procedures to address various emergency scenarios; (iii) provide adequate guidance and direction for the Fund's business continuity management; and (iv) monitor the development of any business continuity management related projects. Similarly, an enterprise-wide risk management working group was established to coordinate the tasks required for managing risks, including those related to business continuity and recovery.

5. The Information Management Systems Service (IMSS) within the Fund secretariat's New York Office was responsible for provision and maintenance of the Fund's ICT systems and services, and coordinating the implementation of strategic decisions made by the Fund's management. IMSS outsourced the following ICT services to the United Nations International Computing Centre (UNICC): (i) data centre management; (ii) server hosting; (iii) data storage and backup services; (iv) e-mail and messaging; (v) desktop management services (file and print services, Active Directory administration); (vi) network management (partially); and (vi) disaster recovery server hosting.

6. The ICT infrastructure of the Fund secretariat was hosted in two data centres and one server room: (i) the UNICC Data Centre in New Jersey (NADC); (ii) the UNICC Data Centre in Geneva; and (iii) the Dag Hammarskjold Plaza (DHP) server room.

7. On 3 August 2015, the Fund rolled out the Integrated Pension Administration System (IPAS) to replace the legacy pension entitlement system, the financial accounting system, the content management system, as well as other stand-alone ICT systems. The ICT infrastructure of IPAS was hosted in NADC

and the disaster recovery infrastructure was hosted in Geneva, requiring manual activation and configuration when needed.

8. Comments provided by the Fund secretariat 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 and efficient management of business continuity and disaster recovery in the UNJSPF secretariat.

10. This audit was included in the OIOS 2016 risk-based work plan for UNJSPF due to the risk that potential weaknesses in business continuity and disaster recovery processes may have an adverse impact on the services provided by the UNJSPF secretariat to its participants and beneficiaries, such as processing of benefit entitlements, payment of benefits, and maintaining participant and beneficiary information.

11. OIOS held the entry conference for this audit in April 2016 but field work was conducted between December 2016 and February 2017. The audit covered the period January 2015 to February 2017. Based on an activity-level risk assessment, the audit covered risk areas relating to business continuity and disaster recovery processes in the Fund secretariat.

12. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation, contracts, policies and procedures, system documentation, test plans, test results and incident reports; and (c) process walkthroughs.

III. OVERALL CONCLUSION

13. The UNJSPF secretariat had determined that monthly payroll processing for all current retirees and beneficiaries worldwide was the core activity requiring business continuity and disaster recovery planning. Except for monthly payroll processing, the Fund's strategy did not include continuity and recovery plans for other core processes such as pension entitlements (i.e. establishing and maintaining records for all participants and beneficiaries, and processing pension benefits), and client services, even though their impact in the event of a disaster was assessed as "high" or "catastrophic". There was need to align the Fund's business continuity strategy with the results of its business impact analysis and complete the related procedures and tests to ensure an adequate response in the event of a disruption at its New York or Geneva Offices.

IV. AUDIT RESULTS

A. Business continuity planning

Business impact analysis was incomplete

14. According to industry best practices, Business Impact Analysis (BIA) should be conducted to assess and prioritize the organization's requirements in response to disruptions and disasters. In its BIA, the UNJSPF secretariat had documented a methodology to determine its critical processes utilizing the measure of two variables. Variable-1 related to the level of complexity to recover operations, and Variable-2 pertained to the level of impact to customers and the Fund secretariat. The methodology

required that the Variable-1 (complexity) should be determined by assessing the input, output, information technology (IT) and staff dependencies of all business processes.

15. The report of the BIA conducted by the Fund in June 2015 included a high-level input, output, IT and staff dependency analysis. However, OIOS noted the following with regard to the assessment of input, output, IT and staff dependencies (i.e. Variable-1):

(i) IMSS serves as the internal ICT service provider of the Fund and a liaison point for the external ICT service providers. However, the impact of unavailability of IMSS services had not been analyzed as part of the BIA.

(ii) The Fund’s analysis of IT dependency did not identify a complete list of ICT systems needed for its business activities. It excluded systems such as automated call distribution and Mobile Office. Mobile Office plays a vital role in enabling remote access to the Fund’s critical systems and was planned to be used in disaster scenarios.

(iii) The Fund’s analysis of input dependencies did not assess how the outages or unavailability of external stakeholders would impact UNJSPF processes. For example the UNJSPF payroll process has input dependencies on the United Nations Treasury (receipt of monthly exchange rates needed for payroll calculations) and the United Nations Secretariat’s Statistics Office (quarterly customer price index needed for the cost of living adjustments). Additionally, the payroll process depends on the services of some United Nations agencies which assist UNJSPF to disburse funds to retirees and beneficiaries in certain countries and regions. There was no agreed recovery time objective (RTO) or alternative plans for the input-output dependencies with these stakeholders.

(iv) The Fund did not analyze how the outages or unavailability of vendors would impact UNJSPF processes. For example, the activities, controls and recovery objectives relating to: (a) the vendor providing software support and issue resolution to IPAS; and (b) the bank that provides interface for payments to beneficiaries and retirees, were not identified in the BIA. Contracts with these vendors did not include RTO for these services.

16. The Fund’s methodology to determine mission critical business processes did not indicate how the two criticality variables (i.e. level of complexity to recover operations, and level of impact to customers and the organization) were used to determine the criticality level of each process. Additionally, there was no evidence that the accumulated impact of outage of business activities and RTOs were appropriately considered in determining the criticality of each business process. Consequently, the BIA prepared by the Fund secretariat identified only the monthly payroll process (i.e. month-end closing, cash management, routing and disbursement of monthly payments) as mission critical. A number of other processes (such as client services and pension entitlements) which were assessed in the BIA as having potentially “high”/“catastrophic” impact were not considered as mission critical.

17. Inadequate and incomplete BIA may lead to a sub-optimal business continuity strategy. Additionally, unassessed dependencies may lead to longer than acceptable recovery times for critical business functions.

(1) The UNJSPF secretariat should strengthen its business impact analysis process by assessing the impact of unavailability of ICT systems and internal/external service dependencies.

The UNJSPF secretariat did not accept recommendation 1 stating that the recommendation has no value added as it will not modify the list of UNJSPF critical processes. Further, the risk of unavailability of vendors during a disaster is mitigated with: (i) use of multiple banks and vendors with global operations; (ii) contracts and service delivery agreements with disaster recovery clauses; (iii) maintenance contracts; and (iv) software support and issue resolution capability available in the Geneva Office. OIOS is of the view that the Fund's comments contradict its own methodology describing how BIA should be performed, and how critical processes should be determined by using the measure of two variables. The Fund's methodology states that Variable-1 ("complexity") should be determined by analyzing: (i) input dependency; (ii) output dependency; (iii) IT dependency; and (iv) staff dependency of all business processes. Failure to conduct a credible analysis of the "complexity" variable in accordance with the Fund's own BIA methodology resulted in inconsistencies within the BIA such as not flagging the Pension Entitlements and Client Services as critical processes even though these processes were rated as "high" and "catastrophic" for their accumulated impact of outage. Consequently, the Fund overlooked certain dependencies for its critical processes. For example, Mobile Office (remote access) would be needed to remotely invoke the disaster recovery site for the monthly payroll process which the Fund identified as critical. However, the BIA results did not indicate Mobile Office as a necessary system for business continuity. Additionally, the Fund's contracts and agreements with external stakeholders did not contain RTOs or alternative plans in case of a disruption to their services. Unknown RTOs could lead to longer disruption of critical processes. OIOS therefore maintains that corrective action is required to strengthen the BIA by assessing the impact of unavailability of ICT systems and internal/external service dependencies. This unaccepted recommendation has been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risks.

<u>Business continuity strategy was not aligned with impact levels of business processes</u>

18. The services provided by the UNJSPF Secretariat included:

i. Payment of retirement, disability, death and other related benefits (weekly and monthly);

ii. Calculation, processing and maintaining of entitlements (benefit processing);

iii. Responding to inquiries of participants, retirees and beneficiaries (client services);

iv. Collecting, pooling and reconciling contributions (accounts); and

v. Establishing and maintaining records for all participants and beneficiaries (record maintenance).

19. The Fund's business continuity strategy identified its core business continuity commitment as the monthly payroll (i.e., month-end closing of pension entitlements and payroll, cash management, and disbursement of payments to retirees/beneficiaries). The Fund's strategy aimed to pay all current retirees and beneficiaries worldwide on or around the beginning of each month.

20. The Fund's Operations (i.e., client services, pension entitlements and records management) are performed by its New York and Geneva Offices, each office serving a separate set of member organizations. In the BIA conducted in June 2015, the Fund assessed the impact levels over the time of interruption for each business activity. The accumulated impact of outage of some business activities in Operations was assessed as "high" or "catastrophic" (see Table 1). Notwithstanding the "high" and "catastrophic"' ratings for the accumulated impact of outage of client services and pension entitlements, the Fund did not document business continuity plans and procedures for these processes. There were no procedures documenting the priorities to be accorded by the office at the recovery site (say, Geneva) in

the event of a disruption at the other location (New York). Also, there were no procedures for redirecting priority telephone calls from the affected site to the recovery site. The rationale for Management's acceptance of the risk of not including these functions in business continuity planning, despite the "high" and "catastrophic" level of their accumulated impact, was not articulated in the Fund's business continuity strategy.

Table 1
Accumulated impact level of outage of some business activites performed by Operations

Process	*8-24 hours*	*48-72 hours*	*1 week*	*2 weeks*
Pension Entitlements	Acceptable	Acceptable	**High**	**Catastrophic**
Client Services	**High**	**Catastrophic**	**Catastrophic**	**Catastrophic**
Records management	Acceptable	Acceptable	Acceptable	**High**

Source: BIA report of UNJSPF

21. OIOS comparison of the Fund's business continuity strategies before and after June 2015 is indicated in Table 2. The initial BIA report of 2010 (which was prepared by a consultancy firm and was valid until June 2015) rated Operations as "highly critical" and stated that "Operations in New York and Geneva, if disrupted, would cause a significant impact to the customers of the Fund. These functions handle communications with customers on a daily basis, and process new entrants and changes in pension entitlements. Although the functions will not necessarily impact the processing of the monthly payroll, the lack of customer care would be noticeable after just a few days". However, in the BIA prepared by the Fund in June 2015, it downgraded the impact rating on "customer experience" of outage of Operations (i.e. pension entitlements, client services and records management) from "high" to "medium". Accordingly, these functions were excluded from the Fund's list of critical business processes. As a result, the new business continuity strategy of June 2015 did not take into consideration core activities such as processing of top priority entitlement cases (i.e. survivor benefits, disability benefits and reinstatements of suspended benefits) and responding to client inquiries, even though these activities had previously been identified as critical in the 2010 BIA. The reasons for downgrading the ratings for these processes were not articulated or explained in the BIA.

Table 2
Comparison of the Fund's business continuity strategies before and after June 2015

Recovery strategy	*Before June 2015*	*After June 2015*
Monthly payroll	Included	Included
Processing of critical benefit processing work types (Death in Service, Child Age 21, deletions, etc.)	Included	Not included
Processing of all worktypes (on a best-effort basis)	Included	Not included
Accounts (on a best-effort basis)	Included	Not included

Source: Business continuity plans of the UNJSPF Secretariat

22. OIOS is of the view that the business processes which were assessed in the BIA as posing "high" and "catastrophic" impact after a disruption (especially those having short RTOs such as pension entitlements and client services) should be included in the business continuity strategy in order to appropriately address their continuity requirements. Failure to do so may lead to unacceptable delays in the processing of top priority benefits (such as survivor, disability, and reinstatement of suspended benefits) and could prevent the Fund from effectively addressing client inquiries that may require urgent

assistance after a disaster. The resultant significant adverse impact on customer experience could also pose significant risks to the Fund's reputation as a service provider to participants/beneficiaries.

(2) The UNJSPF secretariat should: (i) update its business continuity strategy taking into consideration its own assessment of the "high"/"catastrophic" impact of outage of core business processes such as client services and pension entitlements; and (ii) document the business continuity procedures to be followed for these processes in the event of an outage.

The UNJSPF secretariat did not accept recommendation 2 stating that the Geneva Office is responsible for executing UNJSPF business continuity strategy which covers the most critical payroll processes; communication to all stakeholders; and regular execution of Pension Entitlements and Client Services functions from Geneva. The business continuity strategy, including Pension Entitlements and Client Services recovery tasks performed by the Geneva Office, is well-documented in the business continuity/recovery plan. There is no need to document additional procedures. OIOS notes that according to the Fund's business continuity strategy, "Pension entitlement activities performed by the New York Office will be temporarily on hold and will be resumed when normal operations are reestablished". The audit showed that no business continuity plans or procedures were documented for benefit processing, maintenance of participant information and client services activities. In the event of a disruption impacting the New York Office, if the Geneva Office continues to operate in a business as usual mode, participants of United Nations family organizations administered by the New York Office (representing 55 per cent of the Fund's participants) will not be served until the New York Office resumes operations. OIOS therefore maintains that business continuity procedures describing the work priorities, methods of re-direction of priority cases, and other recovery arrangements that would be activated in a disaster scenario need to be documented for pension entitlements (i.e., benefit processing, maintenance of participant records) and client services. This unaccepted recommendation has been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risks.

Need to develop payroll reconciliation reports in IPAS

23. The UNJSPF secretariat's business continuity/recovery plan was built for a scenario where a disruption would significantly affect the Fund's ability to process monthly payroll at its New York Office. The plan in the case of such an event was for the Fund's Geneva Office to process the monthly payroll. Accordingly, a procedure describing the activities assigned to various units in the Geneva Office to perform monthly payroll processing was documented in the business continuity plan. However, the procedure did not describe how payroll reconciliations would be performed by the Geneva Office. In normal conditions, payroll reconciliations are manually performed by the Payment Unit in New York. Due to the absence of payroll reconciliation reports in IPAS, which hitherto existed in the Fund's legacy system, the New York payroll team used information in IPAS and performed additional checks externally using Excel to ensure that the payroll is reconciled accurately. For business continuity purposes, there was no documented guidance provided to the Fund's Geneva payroll recovery team to mitigate the risk of incorrect payroll reconciliation in the event of a disruption in New York. The business continuity tests performed by the Fund did not include payroll reconciliation.

24. Automation of the reconciliation functionality and development of payroll reconciliation reports in IPAS would mitigate the risk of human dependency and error from manual reconciliation.

(3) The UNJSPF secretariat should implement payroll reconciliation reports in IPAS to mitigate the risk of erroneous payroll in the event of a disruption entailing the unavailability of its New York staff to perform manual reconciliations.

The UNJSPF Secretariat did not accept recommendation 3 stating that the UNJSPF business continuity strategy specifies that payroll reconciliations will be performed, as part of return to normal operations, by the Payments Unit in New York. Payroll reconciliations are not time critical, and therefore will be performed in New York as a detective (ex-post) control on the activities performed by the Geneva Office during a disaster. OIOS review of the Fund secretariat's business continuity/recovery procedures showed that manual reconciliation and verification of payroll were assigned to the Geneva Office. The Fund's comments contradict its documented payroll recovery procedure. OIOS therefore maintains that the Fund needs to implement payroll reconciliation reports in IPAS. This unaccepted recommendation has been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risks.

B. Disaster recovery planning

Lack of disaster recovery plans and procedures for critical ICT systems

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

26. The UNJSPF secretariat identified some of its critical ICT systems and installed its disaster recovery infrastructure in Geneva, hosted by UNICC – some replicating production data with a delay of less than 30 minutes. The disaster recovery infrastructure in Geneva provided a small-scale capacity to serve temporarily until the main site becomes available. Application systems in Geneva needed manual configuration to be activated in the event of a disaster impacting the production systems hosted in the New York area. IMSS was responsible for liaising with UNICC for restoration of mission critical systems at the UNICC Data Centre in Geneva.

27. OIOS noted the following in regard to disaster recovery planning:

(i) The disaster recovery plan did not contain a reference to the recent infrastructure and network diagrams.

(ii) The Fund did not document disaster recovery procedures for its ICT systems including critical ones such as IPAS, e-mail, and Mobile Office to describe the activation and configuration steps of the disaster recovery instances and checks to be performed after activation.

(iii) Some of the key systems such as telephone call distribution systems of Client Services, server and network management systems of IMSS, Mobile Office and remote access systems play a vital role (such as activation of disaster recovery systems in Geneva) during a disaster event. These systems were not identified as critical systems in the BIA report as a complete IT dependency analysis was not performed during the BIA.

(iv) The service level agreements with UNICC did not describe responsibilities and tasks to be followed in the event of system disruptions. The impact of this condition was evident when a critical IPAS server failed in October 2016, causing disruption.

(v) The privileged ICT user roles and credentials that need to be activated during disaster recovery were not documented. The privileged accounts and passwords should be stored in sealed envelopes in a safe in the Geneva Office to be accessed after the invocation of the disaster recovery plan.

28. The Fund stated that it would complete the documentation and procedures during the planning of the next disaster recovery tests. Lack of documented disaster recovery plans and procedures may result in long and unexpected recovery times with consequential longer unavailability of services.

(4) The UNJSPF secretariat should: (i) document disaster recovery plans and procedures for all of its critical ICT systems; and (ii) clarify and communicate the roles and responsibilities of ICT recovery team members including vendors and service providers.

The UNJSPF secretariat accepted recommendation 4 and stated that a new set of disaster recovery procedures has been drafted. According to best practices, disaster recovery procedures will continue to be focused on critical ICT systems as identified in the Fund's business impact analysis. Several ICT systems listed by OIOS are not required for the Fund's business continuity and disaster recovery strategy (i.e. Mobile Office-remote access and call distribution system in New York). OIOS review showed that the Geneva Office had no ICT capacity and no documented guidelines to activate the disaster recovery instances of critical ICT systems. During the most recent disaster recovery tests, the Fund's New York staff activated the servers and accounts remotely. Additionally, in certain scenarios (such as a pandemic or when the office premises are not accessible), Mobile Office and remote access could be used by staff to perform critical activities from any location. Recommendation 4 remains open pending receipt of: (i) documented disaster recovery plans and procedures for critical ICT systems; and (ii) evidence of communication of roles and responsibilities of ICT recovery team members, vendors and service providers.

Inadequate assessment of interdependencies between ICT systems

29. During disaster recovery planning, identification of system dependencies plays an important role because the state of operation of a component at the time of a failure may affect the functioning of a critical system.

30. The Fund did not analyze interdependencies and single points of failure in its ICT infrastructure. This may result in unanticipated failure in its most critical ICT systems, such as IPAS, due to unknown dependencies. OIOS noted the following:

(i) On 11 October 2016, a mission-critical IPAS server failed because of a planned maintenance activity on network equipment. At the time of the audit, the IPAS configuration dependency was not yet assessed and there was a risk of similar incidents in the future.

(ii) There were 12 IPAS-related mission-critical servers (interface servers, financials database server, Kofax servers) which were deployed only in NADC and did not have disaster recovery instances in Geneva. Data replication was not configured for these servers. The Fund did not analyze how the unavailability of these servers could impact IPAS service.

31. Additionally, server and network management systems which were critical to support the systems especially in a disruption scenario did not have disaster recovery instances or data replication.

32. Lack of a process to identify dependencies of critical ICT systems may result in unexpected outages of critical business functions.

(5) The UNJSPF Secretariat should: (i) update its configuration management database with a full inventory of hardware and software directly or indirectly linked to its critical systems; and (ii) perform periodic assessment of these dependencies as part of disaster recovery planning.

The UNJSPF secretariat accepted recommendation 5 and stated that a Configuration Management Database is being developed that, together with the Configuration Management and Change Management processes, will meet the requirements listed in this recommendation. Recommendation 5 remains open pending receipt of: (i) a full inventory of hardware and software linked to the Fund's critical systems; and (ii) evidence of periodic assessment of these dependencies.

<u>Testing of business continuity and recovery plan was incomplete</u>

33. The "Maintenance, exercise and review regime" for implementation of the United Nations Organizational Resilience Management System (ORMS) requires periodic testing of plans, procedures and systems to ensure their reliability.

34. The Fund periodically tested its business continuity and disaster recovery plan separately, with some scope limitations. OIOS noted the following in regard to test activities:

(i) The business continuity test scenarios were not adequately defined. For example, business continuity testing for a pandemic scenario would differ from a cyber-attack scenario impacting some or all production systems.

(ii) Business continuity tests assumed that all ICT systems are active and running and only focused on the Geneva team's ability to perform the monthly payroll process.

(iii) IPAS users were not involved in disaster recovery tests. During the tests, one minor user transaction was performed by the ICT staff to validate the activation of disaster recovery servers. However, complex tasks within IPAS which require interaction with other ICT components (such as shared drives) were not performed. The full functionality of the disaster recovery infrastructure cannot be verified unless the applications are fully tested by the business users.

(iv) Since business users were not involved in disaster recovery tests, there was no load test performed on the IPAS disaster recovery infrastructure to observe the maximum capacity that it could serve in the event of unavailability of the production site.

(v) There were no documented instructions describing the activation of the disaster recovery systems in the Fund's Geneva Office. Therefore, during the disaster recovery tests of IPAS, disaster recovery servers were activated remotely by the New York recovery team. Lack of documented guidance could negatively impact the achievement of expected recovery time objectives. Furthermore, in the service level agreement on provisioning of infrastructure, UNICC's role in restoration activities was not clearly defined and UNJSPF was assigned as the responsible party for the activity.

(vi) Disaster recovery tests were not performed for other critical ICT systems such as e-mail, file sharing and network infrastructure which were identified as critical in the BIA; test plans and results were not documented for these systems.

35. Complete testing of business continuity and disaster recovery plans is necessary to enable the Fund to assess the accuracy and adequacy of its plans and its disaster recovery infrastructure. Failure to do so may have an adverse impact on the Fund's business continuity in the event of a disruption.

(6) The UNJSPF secretariat should enhance the testing of its business continuity and disaster recovery plans by: (i) documenting the disaster scenarios to be tested; and (ii) including the activation of disaster recovery systems such as IPAS, e-mail and shared drives in its testing activities.

The UNJSPF secretariat did not accept recommendation 6 stating that it is not part of the United Nations Secretariat. Therefore, the United Nations Policy Statement on Business Continuity Management policy and other United Nations disaster recovery guidelines are not applicable and are not appropriate criteria to audit the Fund. The Fund should be audited against its business continuity strategy as defined and adopted by management. UNJSPF tests are aligned with the business continuity strategy which is designed to address multiple scenarios (emergency, crisis and disaster) to ensure flexibility, long-term value and the highest level of success when faced with a significant disruption. The Fund secretariat will continue to gradually expand the scope of its business continuity and recovery tests to minimize possible risks. Disaster recovery tests involve the activation of UNJSPF critical disaster recovery systems. OIOS notes that the ORMS policy and the "maintenance, exercise and review regime" states that it applies to all entities of the United Nations system. UNJSPF is a member of the ORMS Global Working Group since it is one of the entities within the United Nations system. ORMS was approved by the General Assembly in its resolution 67/254 of June 2013 as the emergency management framework for the Organization. The ORMS policy prescribed its adoption across the United Nations system. General Assembly resolution 67/254 requested the Secretary-General to submit to it a progress report on the implementation of ORMS, including information on the steps taken to expand the system to include the specialized agencies, funds and programmes. Therefore, OIOS is of the view that the ORMS policy applies to UNJSPF since it has been approved by the supreme legislative body of the United Nations to which the Fund is ultimately accountable. Even if the Fund adopts a legalistic position to argue against its applicability, OIOS maintains that the ORMS policy is a source of good practices for disaster recovery management which the Fund needs to implement to strengthen its emergency preparedness. OIOS review of the Fund's test reports showed that no disaster recovery tests were performed for e-mail, file sharing and network infrastructure which were identified as critical in the Fund's BIA report. Instead, the tests included only IPAS servers without its interfaces. End-to-end critical payroll recovery activities were never tested on the disaster recovery instance. Additionally, no business continuity tests were performed for scenarios such as epidemic/pandemic conditions requiring remote access to the Fund's critical systems through Mobile Office. OIOS therefore maintains that disaster recovery tests for all critical ICT systems are essential and test activities should be enhanced to assure continuity of operations in a disruption scenario. This unaccepted recommendation has been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risks.

Coordination between the Fund secretariat and IMD needed to be strengthened

36. In accordance with its terms of reference, the Business Continuity/Recovery Working Group of UNJSPF was composed of members from the Fund secretariat and IMD. It was responsible for: (i) coordinating the tasks required to develop a Fund-wide business continuity/recovery plan based on a complete business impact analysis; (ii) developing plans and procedures to address various emergency scenarios; (iii) providing adequate guidance and direction for the Fund's business continuity management; and (iv) monitoring the development of any business continuity management related projects.

37. The working group met every quarter. The meeting minutes showed that it did not provide guidance and direction on certain subjects which could improve and standardize the business continuity and disaster recovery planning and coordination. For example:

(i) Standard disaster or disruption scenarios were not selected to be used in the development of business continuity, disaster recovery plans and tests for the Fund secretariat and IMD.

(ii) There was no coordination or agreed procedures during the test exercises concerning the continuity and recovery of shared ICT infrastructure, the DHP data centre, emergency notification system, and shared e-mail infrastructure. IMD was informed by UNICC that the disaster recovery tests of its e-mail system could not be performed until the Fund's secretariat completed the migration project on the shared platform. However, the working group did not provide any guidance on the coordination of this activity.

38. This condition was due to the absence of effective coordination of business continuity and disaster recovery activities between the Fund's secretariat and IMD which may lead to incomplete or ineffective disaster recovery arrangements. Since an audit recommendation relating to this issue made in the OIOS audit of business continuity and disaster recovery planning in IMD (Report 2016/048) is still under implementation, no additional recommendation is made in the present report.

V. ACKNOWLEDGEMENT

39. 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.

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

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity and disaster recovery in the secretariat 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 UNJSPF secretariat should strengthen its business impact analysis process by assessing the impact of unavailability of ICT systems and internal/external service dependencies.	Important	C	This recommendation has been closed without implementation based on management's acceptance of residual risks.	Not provided
2	The UNJSPF secretariat should: (i) update its business continuity strategy taking into consideration its own assessment of the "high"/"catastrophic" impact of outage of core business processes such as client services and pension entitlements; and (ii) document the business continuity procedures to be followed for these processes in the event of an outage.	Important	C	This recommendation has been closed without implementation based on management's acceptance of residual risks.	Not provided
3	The UNJSPF secretariat should implement payroll reconciliation reports in IPAS to mitigate the risk of erroneous payroll in the event of a disruption entailing the unavailability of its New York staff to perform manual reconciliations.	Important	C	This recommendation has been closed without implementation based on management's acceptance of residual risks.	Not provided
4	The UNJSPF secretariat should: (i) document disaster recovery plans and procedures for all of its critical ICT systems; and (ii) clarify and communicate the roles and responsibilities of ICT recovery team members including vendors and service providers.	Important	O	(i) Receipt of documented disaster recovery plans and procedures for critical ICT systems; (ii) Receipt of evidence of communication of roles and responsibilities of ICT recovery team members, vendors and service providers.	31 December 2017
5	The UNJSPF Secretariat should: (i) update its configuration management database with a full inventory of hardware and software directly or	Important	O	(i) Receipt of a full inventory of hardware and software linked to the Fund's critical systems; and (ii) evidence of periodic assessment of these	31 December 2017

[1] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[3] C = closed, O = open
[4] Date provided by the UNJSPF secretariat in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity and disaster recovery in the secretariat 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]
	indirectly linked to its critical systems; and (ii) perform periodic assessment of these dependencies as part of disaster recovery planning.			dependencies.	
6	The UNJSPF secretariat should enhance the testing of its business continuity and disaster recovery plans by: (i) documenting the disaster scenarios to be tested; and (ii) including the activation of disaster recovery systems such as IPAS, e-mail and shared drives in its testing activities.	Important	C	This recommendation has been closed without implementation based on management's acceptance of residual risks.	Not provided

APPENDIX I

Management Response

UNITED NATIONS **NATIONS UNIES**

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

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

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

MEMORANDUM

Ref: New York, 5 May 2017

-OIC

To / A:	Mr. Gurpur Kumar, Director Internal Audit Division, OIOS	From / De :	Mr. Sergio B. Arvizú, Chief Executive Officer, United Nations Joint Staff Pension Fund

Subject / Objet: **UNJSPF response to draft report audit of business continuity and disaster recovery in the secretariat of the UNJSPF (Assignment No. AS2015/800/02)**

1. This is in response to your memorandum dated 21 April 2017, in which you submitted for the Fund's comments and response on the draft report on the above-mentioned audit.

2. The Fund secretariat thanks OIOS for its review of business continuity and disaster recovery conducted from April 2016 to February 2017.

3. The Fund secretariat reiterates its request that OIOS consider the comments, factual corrections and clarifications provided in memorandum dated 4 April 2017 and additional clarifications attached to this memorandum (**Annex I**). This will ensure that the final report accurately reflects the Fund's business continuity and disaster recovery strategy, which is aligned with the results of the business impact analysis.

4. In the same line, the Fund secretariat noted the draft report does not include the Fund secretariat's responses to unaccepted recommendations, and kindly requests OIOS to reflect this information in the final report. The Fund's responses explain the rationale for not accepting recommendations that are considered not appropriate or unnecessary.

5. As requested, the Fund's response to the audit recommendations is included in **Annex II**.

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

ANNEX I

AUDIT RECOMMENDATIONS

Audit of business continuity and disaster recovery in the secretariat of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	The UNJSPF secretariat should strengthen its business impact analysis process by assessing the impact of unavailability of ICT systems and internal/external service dependencies.	Important	No	N/A	N/A	In accordance with best practices (ITIL V3), the Fund conducted a business impact analysis to "identify": i) critical business processes; and ii) input-output dependencies of critical business processes. OIOS recommendation to assess the impact of **all** inputs or ICT systems for each business activity is not aligned with best practices. The recommendation also has no value added as it will not modify the list of UNJSPF critical processes. Further, the risk of unavailability of vendors during a disaster is mitigated with: i) the use of multiple banks and vendors with global operations; ii) contracts and service delivery agreements with disaster recovery clauses; iii) maintenance contracts; and iv) software support and issue resolution capability available in the Geneva Office. Accordingly, the possible risk identified by OIOS is properly mitigated.
2	The UNJSPF secretariat should: (i) update its business continuity strategy taking into consideration its own assessment of the "high"/"catastrophic" impact of outage of core business processes	Important	No	N/A	N/A	(i) The recommendation is based on an incorrect interpretation of the Fund's business impact analysis and business continuity strategy. The Geneva Office is responsible for executing UNJPSF business continuity strategy, which covers the most critical payroll processes (month-end closing of pension

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	such as client services and pension entitlements; and (ii) document the business continuity procedures to be followed for these processes in the event of an outage.					entitlements and release of approved cases; month-end closing of the payroll; cash management processes; and routing and disbursement of payments); communication to all stakeholders; and regular execution of Pension Entitlements and Client Services functions from Geneva. Therefore, the execution of Pension Entitlements and Client Services functions is already covered by UNJSPF business continuity strategy. (ii) The business continuity strategy, including Pension Entitlements and Client Services recovery tasks performed by the Geneva Office, is well-documented in the business continuity / recovery plan. There is no need to document additional procedures. Based on the above comments, the possible risk identified by OIOS is properly mitigated.
3	The UNJSPF secretariat should implement payroll reconciliation reports in IPAS to mitigate the risk of erroneous payroll in the event of a disruption entailing the unavailability of its New York staff to perform manual reconciliations.	Important	No	N/A	N/A	UNJSPF business continuity strategy specifies that payroll reconciliations will be performed, as part of return to normal operations, by the Payments Unit in New York. Payroll reconciliation are not time critical, and therefore will be performed in New York as a detective (ex-post) control on the activities performed by the Geneva Office during a disaster. Payroll reconciliations are performed using system generated reports and therefore, there are no manually produced payroll reports. Based on the above, the possible risk identified by OIOS is properly mitigated.
4	The UNJSPF secretariat should: (i) document disaster recovery plans and procedures for all of its	Important	Yes	Chief of IMSS	December 2017	A new set of disaster recovery procedures it has been drafted. After the completion of the next Disaster Recovery Readiness Test, UNJSPF disaster

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	critical ICT systems; and (ii) clarify and communicate the roles and responsibilities of ICT recovery team members including vendors and service providers.					recovery procedures will be revised and published. According to best practices, disaster recovery procedures will continue to be focused on critical ICT systems as identified in the Fund´s business impact analysis. Several ICT systems listed by OIOS are not required for the Fund's business continuity and recovery strategy (i.e. Mobile Office – remote access and call distribution systems in New York).
5	The UNJSPF Secretariat should: (i) update its configuration management database with a full inventory of hardware and software directly or indirectly linked to its critical systems; and (ii) perform periodic assessment of these dependencies as part of disaster recovery planning.	Important	Yes	Chief of IMSS	December 2017	A Configuration Management Database (CMBD) is being developed that, together with the Configuration Management and Change Management Processes, will meet the requirements listed in this recommendation.
6	The UNJSPF secretariat should enhance the testing of its business continuity and disaster recovery plans by: (i) documenting the disaster scenarios to be tested; and (ii) including the activation of disaster recovery systems such as IPAS, email and shared drives in its testing activities.	Important	No	N/A	N/A	(i) All UNJSPF business continuity and disaster recovery tests have a documented test plan with clearly defined objectives and scope. Test results are documented and evaluated. UNJPSF tests are aligned with the business continuity strategy, which is designed to address multiple scenarios (emergency, crisis and disaster) to ensure flexibility, long-term value and the highest level of success when faced with a significant disruption. (ii) The Fund secretariat will continue to gradually expand the scope of its business continuity and recovery tests to minimize possible risks. Disaster recovery tests involve the activation of UNJSPF critical disaster recovery systems. Based on the above, the possible risk identified by OIOS is properly mitigated.

ANNEX II

General Comments, Factual Corrections and Clarifications to the Draft Report on the audit of business continuity and disaster recovery in the Fund Secretariat

In light of potential risks derived from the publication of audit reports with inaccurate or incomplete information, the Fund secretariat kindly requests OIOS to consider the following general comments, factual corrections and technical clarifications:

General Comments to Draft Report

a. **Governance and Regulatory criteria:** The Fund secretariat is not part of the United Nations Secretariat. Therefore, the United Nations Policy Statement on Business Continuity Management (BCM) policy and other United Nations disaster recovery guidelines are not applicable and are not an appropriate criterium to audit the Fund. The Fund should be audited against its Business Continuity Strategy as defined and adopted by management, which is further supported by the well documented UNJSPF Business Impact Analysis and Business Continuity / Recovery Plan.

   In the same line, the Fund secretariat is not a member of the Chief Executives Board for Coordination (CEB), and it is not mandated to apply the guidelines, standards and key performance indicators of the United Nations Organizational Resilience Management System (ORMS). This needs to be accurately reflected in the report.

b.

c. **Technical criteria:** The BC/DR strategy selected by the Fund secretariat is the result of risk-based analysis and prioritization, and as such, it is focused on the most critical functions. Two key business continuity / recovery (risk management) concepts need to be clarified:

   c1. Objective of a business impact analysis: Best practice standards adopted by the Fund specify that the objective of a business impact analysis is to identify **critical business processes and their input-output dependencies** (required resources). ITIL V3: *"BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other Business Processes, IT Services, etc. BIA defines the recovery requirements for IT Services."*

   It is not the objective and it is not a standard practice to use a business impact analysis to: i) identify dependencies for each business activity; ii) assess the impact of ICT systems or services (BIA is a "business" analysis); or iii) agree recovery objectives or alternative plans with vendors or suppliers.

   c2. Scope of a business continuity / strategy: In accordance with the Fund's business impact analysis methodology, which is aligned with best practice standards, the Fund identified "critical" business processes based on their criticality, which was calculated and derived by measures of impact and complexity.
   The Fund's **business continuity / recovery strategy is therefore focused on the critical business processes** identified by management in the business impact analysis.
   By using, interchangeably, the terms "criticality" and "impact" as criteria for identifying "critical" functions, as well as the terms "critical" and "core" when referring to different business functions and ICT systems, OIOS has incorrectly recommended to the Fund to expand the business continuity / recovery strategy and documentation to cover other functions that although important are not critical.

   These two technical inaccuracies need to be corrected to avoid reaching audit conclusions and recommendations that are not aligned with best practices, and also be not implementable. Any audit recommendation that the Fund's business continuity / recovery should cover business processes that management did not identify as "critical" in its the business impact analysis, would contradict best practice recommendations to ensure alignment of BC/DR plans with business impact analysis results.

Factual Corrections and Clarifications to specific paragraphs

Paragraph 11: It is incorrect to state that the audit field work was conducted between December 2016 and February 2017. OIOS Notification memorandum IAD:-16-00159 was received on 1 April 2016, the entrance conference held on 15 April 2016 and the audit field work started in April 2016.

Paragraph 15: Best practice standards for business impact analysis require to "**<u>identify</u>**" dependencies **<u>only for critical</u>** business processes and activities, and make clear that **"<u>agreed recovery time objectives</u>"** or **"<u>alternative plans</u>"** should be prepared at a later stage only for critical processes.

Therefore, it is technically incorrect to recommend that the business impact analysis should:

- Paragraph 15 (ii): *"Identify a complete list of ICT systems needed for **<u>each</u>** business activity".*
- Paragraph 15 (iii): Include *"**<u>agreed recovery time objective or alternative plans</u>** for the input-output dependencies".*
- Paragraph 15 (iv): Analyze the impact of *"outages or unavailability of vendors".* Agreed recovery time objectives or alternative plans do not belong to a business impact analysis.

Paragraphs 13, 16, 19 and 20: It is factually incorrect to state that the Fund's business continuity / recovery strategy is limited to "payroll" or "monthly payroll" and did not include recovery plans for other processes such as client services and pension entitlements. As specified in the Fund's Business Continuity / Recovery Plan, the business continuity strategy covers: *"critical monthly payroll processes"* performed by Pension Entitlements, Payments and Cashier functions which are not properly reflected or over simplified in the audit report, including:

- *"Month-end closing of pension entitlements and release of approved cases;*
- *Month-end closing of the pension benefit payroll;*
- *Cash management processes; and*
- *Routing and disbursement of payments."*

The recovery procedures also take into account the following key areas:

- *"Safety of employees;*
- *Assessment of impact to the Fund's operations; and*
- *Communication among UNJSPF Recovery Teams (as described in Appendix F), communication to all staff and to key stakeholders."*

Paragraphs 20 and 22: As specified in Section 3 Methodology of UNJPSF Business Impact Analysis dated January 2017, *"determination of criticality of the Fund processes utilizes the measures of impact and complexity".* It is technically and factually incorrect to state that *"Notwithstanding the "high" and "catastrophic" ratings for the **<u>accumulated impact</u>** of outage of client services and pension entitlements, the Fund did not document business continuity plans and procedures for these processes":*

- The business continuity / recovery plan is built on the assumption that the Geneva Office is the primary recovery site. The Fund's BC/DR strategy relies on the Geneva Office staff, processes and infrastructure to: i) recover the critical monthly payroll processes; and ii) continue client services, pension entitlements and records management functions regularly performed by this Office.
- Actions to recover records management and client services functions performed in New York from the Geneva Office are specified in Section 5.9 "Emergency Communications" and Section 7.1 "Immediate Reaction Steps".

- Steps to recover pension entitlements functions are specified in Section 7.2 "Business Continuity / Recovery Procedures".

Tables 1 and 2: Based on the previous comments, the information contained in these tables misrepresents the results of the Fund's business impact analysis and the business continuity strategy.

Paragraph 21 and Table 2: OIOS presented partial and incorrect information on the BC/DR strategy. It is factually incorrect to state that the Fund downgraded the impact ratings of Pension Entitlements, Client Services and Records Management between 2010 and 2015 and that these *"functions were excluded from Fund's list of critical business processes"*.

The Fund's business continuity strategy continues to be focused on the recovery of the "critical payroll processes" (including month-end closing of pension entitlements and release of approved cases). Prior to June 2015, processing of all work-types and accounting functions was performed *"depending on the availability of additional time and Operations/FSS individuals to finalize critical cases"*. Moreover, due to process changes derived from IPAS implementation, after June 2015, the Geneva Office processes **all** types of benefits, recalculations and revisions, and continues to provide client services. Therefore, it is not accurate to state that the new business continuity strategy after June 2015 does not include the processing of all benefits and finance activities (death in service, children, deletions, reinstatements, etc.) as well as client servicing.

Paragraph 23: This paragraph needs to be amended to accurately reflect the payroll process. It is inaccurate to state that there are no payroll reconciliation reports in IPAS and that *"the New York payroll team produced reports manually using information in IPAS"*. Payroll reconciliations are performed using system generated reports. Payroll reconciliation is not time critical and will continue to be performed "as business as usual" by the Payments Unit in New York.

Paragraph 25: As noted above, the United Nations disaster recovery guidelines are not applicable to the Fund.

Paragraph 27: This paragraph needs to be amended since OIOS lists as "critical" or "key" ICT systems that do not support the business continuity strategy which is focused on "critical" business processes (i.e. Mobile Office, remote access systems and telephone call distribution systems). Only the ICT systems specified in the Fund's business impact analysis are critical.

Paragraph 33: As noted above, the Fund is not mandated to follow the guidelines issued by the United Nations Organizational Resilience Management System (ORMS) Working Group.

Paragraph 34 and recommendation 6. Need to be amended since all UNJSPF business continuity and recovery tests have a documented plan with defined objective and scope. Test results are documented and evaluated. Further, UNJSPF business continuity strategy is comprehensive and designed to address multiple scenarios (i.e. emergencies, crisis or disasters that may significantly affect the Fund's staff, property and processes). Issues and incidents with limited impact on business operations are handled as part of business-as-usual processes. Disaster recovery tests involve the activation of UNJSPF critical disaster recovery systems as defined in the business impact analysis.

Paragraph 37: Since its creation in 2007, the Business Continuity / Recovery Working Group (WG) has played a critical role in the definition of the Fund's business continuity and disaster recovery strategy and related infrastructure based on comprehensive risk assessments and business impact analysis studies. The Working Group also recommended the selection of the business continuity / recovery strategy, monitored the development and maintenance of the BC/DR plans, and coordinated periodic training and testing activities. The Working Group closely monitored and decided on the update of the BC/DR strategy, plan and related infrastructure in light of IPAS implementation. Most recently, to enhance coordination mechanisms between the Fund secretariat and IMD, the WG is now Co-chaired by the Deputy CEO and the IMD Director. The WG also successfully coordinated and completed at the end of 2016, a comprehensive "Crisis Management" training and test with the participation of all UNJSPF staff, and updated emergency communication procedures to enhance coordination between the Fund secretariat and IMD.

The above actions do not support OIOS statement that the Business Continuity / Recovery Working Group *"did not provide guidance and direction on certain subjects"*. It is further noted that UNJSPF business continuity strategy is multi-scenario (i.e. designed to cover multiple scenarios); it is not the role of the BC/DR Working Group to provide guidance on ICT projects such as the migration of the e-mail system; and that the Fund secretariat and IMD do not have any *"shared ICT infrastructure"*.