Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2016/048

Audit of business continuity and disaster recovery planning in the Investment Management Division of the United Nations Joint Staff Pension Fund

Overall results relating to the effective and efficient management of business continuity and disaster recovery planning were initially assessed as partially satisfactory. Implementation of six important recommendations remains in progress

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

16 May 2016
Assignment No. AT2016/801/01

CONTENTS

AUDIT REPORT

Audit of business continuity and disaster recovery in the Investment Management Division 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 planning in the Investment Management Division (IMD) of the United Nations Joint Staff Pension Fund ("UNJSPF" or "the Fund").

2. IMD is responsible for the investment of the assets of the Fund. IMD is composed of five organizational entities that report to the Representative of the Secretary-General (RSG) for the investments of the Fund. These entities include: Office of the RSG/Director, Investment Section, Risk and Compliance Section, Information Systems Section (ISS) and Operations Section.

3. Business continuity and disaster recover planning are critical components of emergency management and organizational resilience. Business continuity planning applies to the business and it concerns the ability to continue critical functions and processes during and after an emergency event, considering critical personnel, key business processes, vital records, critical suppliers, and key vendors and clients. There is an inherent relationship between an information and communications technology (ICT) system and the business process it supports. Therefore, business continuity plans are supported by ICT disaster recovery plans and include recovery strategies to ensure that the ICT systems can be recovered quickly and effectively following a disruption. ICT disaster recovery plans include detailed recovery procedures and guidance for restoring a damaged system in accordance with the estimated impact of a potential damage and recovery requirements.

4. UNJPSF established a business continuity/recovery working group in 2014. This working group was composed of members from IMD and the Fund Secretariat with the mandate to: (i) coordinate business continuity and disaster recovery activities; (ii) develop plans and procedures to address different 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, in a formal and integrated approach.

5. ISS is responsible for: (i) designing and implementing production and disaster recovery infrastructures of the business applications supporting front and back investment operation processes; (ii) providing application level support for business applications; and (iii) providing infrastructure services, including managing system interfaces, mobile devices, desktop services, database management, ICT security and incident resolution.

6. Recently, IMD implemented the first phase of the Bloomberg Assets and Investment Management (AIM) system, replacing older systems (Charles River, OMGEO and some of the functions performed by the "Society for Worldwide Interbank Financial Telecommunication", SWIFT[1] system). The new Bloomberg AIM was supported by a third party hosted service, which provided high availability and straight through processing of trade order management. With the full implementation of this project,

[1] Charles River was used as a Trade Order Management System. OMGEO was used for automated trade matching process. SWIFT was used for releasing payment messages to the custodian and master record keeper.

IMD planned to support the majority of its business functions with Bloomberg AIM, which included its own disaster recovery solution.

7. IMD used other hosted services for Risk Metrics, FX/ALL, Citi Direct, Northern Trust Passport, and Holt [2] which provided disaster recovery as part of their services. In order to establish a secure communication for some of these services, IMD operated communication interfaces hosted in its data centres.

8. IMD internally hosted and managed some of its ICT services, including Wilshire/Abacus (used for data reconciliation and cash activity reporting), file sharing, Mobile Office, database servers and data interfaces with external service providers (i.e., Bloomberg AIM data interface; and Risk Metrics data interface).

9. IMD outsourced the following ICT services to the United Nations International Computing Centre (UNICC): (i) data centre management and server hosting; (ii) first tier help desk support for the resolution of incidents and user assistance; (iii) data storage and backup services; (iv) e-Mail and messaging; (v) management of the Active Directory[3] service; and (vi) disaster recovery site hosting for SWIFT.

10. IMD received support from the Information Management Systems Service (IMSS) of the Fund Secretariat for network management and security token management.

11. The ICT infrastructure of IMD was hosted in three data centres: (i) UNICC Data Centre in New Jersey (NADC); (ii) UNICC Data Centre in Geneva; and (iii) Dag Hammarskjold Plaza (DHP) data centre.

12. Comments provided by IMD are incorporated in italics.

II. OBJECTIVE AND SCOPE

13. The audit was conducted to assess the adequacy and effectiveness of the IMD governance, risk management and control processes in providing reasonable assurance regarding the **efficient and effective management of business continuity and disaster recovery planning in IMD.**

14. This audit was included in the OIOS work plan for 2016 in view of the high risks associated with the business continuity and disaster recovery and their potential impact on IMD operations.

15. The key controls tested for the audit were: (a) business continuity and disaster recovery plans; and (b) coordinated management mechanisms. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Business continuity and disaster recovery plans -** controls that provide reasonable assurance that business continuity and disaster recovery plans are in place to ensure that the

[2] Risk Metrics is a risk assessment software for investment risks. FX/ALL is the foreign exchange trading platform. Northern Trust Passport is a web-based custodian and master record keeper application (for trade notification, cash movement, and reports) hosted by Northern Trust. Citi Web is web-based custodian application (for trade system, cash movement, and reports, etc.) hosted by Citibank; and Bloomberg PORT and Holt are online market data services.

[3] Active Directory is the system controlling the IMD domain including devices, users, group policy, authentication and authorization.

operations of IMD can withstand adverse events and continue to operate within a reasonable time frame; and

(b) **Coordinated management mechanisms -** controls that provide reasonable assurance that business continuity and disaster recovery activities are coordinated with the Fund Secretariat and any potential gaps or overlaps are identified and resolved in a timely manner.

16. The key controls were assessed for the control objectives shown in Table 1.

17. OIOS conducted the audit from January to March 2016. The audit covered the period from January 2015 to March 2016.

18. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to determine their effectiveness.

III. AUDIT RESULTS

19. The IMD governance, risk management and control processes examined were initially assessed as **partially satisfactory**[4] in providing reasonable assurance regarding the **effective and efficient management of business continuity and disaster recovery planning in IMD.** OIOS made six audit recommendations to address issues identified in the audit.

20. IMD had completed the transition of its critical ICT applications to third parties which had also provided their own disaster recovery infrastructure. Although this approach mitigated some of the main risks affecting the ICT systems operated by IMD, additional controls were required in order to: (i) strengthen risk assessment and impact analysis of business continuity and disaster recovery; (ii) identify critical ICT applications and risks arising from ICT infrastructure and system dependencies; (iii) ensure the involvement of all business units in business continuity planning; (iv) update the plans with adequate scenarios; (v) define a short and long term strategy addressing the single points of failure of critical systems; (vi) document and test recovery procedures for all ICT applications; and (vii) strengthen coordination with the Fund Secretariat to mitigate the risk of incomplete or ineffective disaster recovery arrangements.

21. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **partially satisfactory** as implementation of six important recommendations remains in progress.

[4] A rating of **"partially satisfactory"** means that important (but not critical or pervasive) deficiencies exist 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.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	**Accurate financial and operational reporting**	**Safeguarding of assets**	**Compliance with policies, mandates, regulations and rules**
Efficient and effective management of business continuity and disaster recovery planning in IMD	(a) Business continuity and disaster recovery plans	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(b) Coordinated management mechanisms	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory

A. Business continuity and disaster recovery plans

Need to strengthen risk assessment and impact analysis of business continuity and disaster recovery

22. The enterprise-wide risk management policy of UNJSPF required annual risk assessments and risk treatment plans. Additionally, the organizational resilience standard adopted by the United Nations Secretariat recommended to re-evaluate risks and their impacts in accordance with any changes made to the operating environment, procedures, functions, services, partnerships and supply chains.

23. IMD conducted its last business impact assessment in 2006. Since then, several changes were implemented in its ICT infrastructure and new service agreements were established with different external service providers. In preparation for its business continuity and disaster recovery planning, IMD did not re-assess the risks – and their impact – arising from changes that have occurred in its environment. In this regard, the following weaknesses were identified:

(i) Business continuity and disaster recovery plans, disaster recovery infrastructure and backup schedules were not developed in accordance with the requirements of the business users and business impact analysis;

(ii) The potential impact deriving from the unavailability of services provided by third parties - including discretionary investment managers, custodians and master record keeper - were not analyzed;

(iii) Recovery time objectives (the target time set for the recovery of ICT and business activities after a disaster) and recovery point objectives (the time between data backups and the amount of data that could be lost in between backups) for the systems and services were not assessed and agreed for all systems;

(iv) Risks related to the operations of critical ICT systems and their dependencies were not identified using an adequate risk assessment methodology; and

(v) IMD did not systematically analyze controls, priorities, mitigation actions (i.e., treatment plans), and associated costs, to improve its readiness in case of disruptions or

disasters. For example, data backup schedule, which was the most basic mitigation action to minimize data losses, was not defined for each system.

24. This condition was due to the absence of adequate risk assessment and impact analysis which may lead to the loss of critical data and result in long disruptions.

(1) IMD should: (i) define the recovery time and point objectives for all its outsourced business services, ICT systems, and ICT services by completing the business impact assessment; (ii) identify critical ICT assets and their dependencies; and (iii) prepare risk treatment and action plans to prioritize the implementation of controls.

IMD accepted recommendation 1 and stated that given its resources and other business needs, it has determined that the recommendation is best addressed through a work order with a consulting firm. The work order is in the final stages of approval. Recommendation 1 remains open pending receipt of the complete business impact assessment with recovery time and business objectives for outsourced business services, ICT systems and ICT services, analysis of criticality and dependencies of ICT assets, documentation of controls and priorities, and risk mitigation action plans.

Need to strengthen business continuity procedures and testing

25. According to the United Nations policy statement on business continuity management, each organizational unit should contribute to the business continuity plans by: (i) documenting risk mitigation strategies; (ii) defining clear emergency and recovery procedures, succession planning and delegation of authority; and (iii) establishing communication mechanisms. Organizational units should also be involved in training, testing and maintenance of the business continuity plans.

26. IMD had documented communication and evacuation procedures during an emergency scenario. Instructions and delegation of authority needed for paying obligations to beneficiaries were documented and signed. Additionally, the Operations Section documented procedures to be followed during emergency and recovery periods. However, the following business units did not document procedures describing the tasks and communication procedures (including those for staff, other IMD units, business partners and third party providers of specific services), that should be followed during the recovery period in any disruption scenario:

(i) Investments Section (i.e., Alternative Investments, Asia-Pacific, North America, Emerging Markets, Europe, Fixed Income, Real Estate and Trade Execution Unit);

(ii) Risk and Compliance Section (Risk Unit and Compliance Unit); and

(iii) Office of the RSG and Director.

27. Additionally, the Investment Section outsourced some of its investment activities to third party service providers, including external small cap investment management companies (i.e., discretionary investment managers) that initiated and executed trades on behalf of IMD using their own ICT systems. However, the business continuity requirements of IMD related to recovery time and point objectives for these services were not clearly defined, and the unavailability of these services was not considered in the business continuity plans and test exercises.

28. The testing exercise of business continuity and disaster recovery performed by IMD in September 2015 was limited to a narrow scope, and the scenario covered in the test was not clear. This exercise was built on several assumptions, including the availability of all ICT infrastructure and network in DHP and

NADC data centres, except for two application servers. Therefore, this exercise could not assure the continuity of IMD operations in several other disaster scenarios (i.e., unavailable third party services providers) that were not considered. Additionally, the contribution of the business units to the test planning activities was limited. Therefore, several activities and scenarios were not tested.

29. This condition was due to the absence of documented emergency and recovery procedures for each business unit and the lack of adequate tests with clear scenarios and procedures, which may lead to financial and information losses.

(2) IMD should document and test the business continuity procedures for each business unit.

IMD accepted recommendation 2 and stated that given its resources and other business needs, it has determined that the recommendation is best addressed through a work order with a consulting firm. The work order is in the final stages of approval. Recommendation 2 remains open pending receipt of business continuity procedures for each business unit and test results of each procedure.

Inadequate methodology for selecting critical applications

30. The United Nations Secretariat guidelines for disaster recovery planning defined the methodology for determining critical functions, processes, ICT services and applications for the purpose of business continuity and disaster recovery planning.

31. IMD did not follow the disaster recovery planning guidelines of the United Nations Secretariat to identify the criticality of its ICT systems. IMD determined its critical ICT services using its "ICT services risk prioritization matrix". However, this process was not based on adequate criteria and assessment of its ICT components. As a result, some of the IMD critical ICT systems (i.e., shared drives; mobile offices) were assessed as having a low criticality and, therefore, they were not considered in the disaster recovery planning. In particular, the following weaknesses were noted:

(i) IMD assessed three "likelihood factors" to identify the risk rating of its ICT assets, as follows: (a) volume of transactions processed; (b) complexity of calculations; and (c) sensitivity of data and transactions. However, these factors were not adequate for assessing the likelihood of any event.

(ii) The methodology used by IMD omitted the impact of non-transactional critical systems (i.e., mobile office, e-Mail and file sharing services) on IMD operations.

(iii) The risk assessment did not consider events associated with potential disruption caused by lack of electricity, telecommunications or Internet services in certain locations.

(iv) The risk rating methodology adopted by IMD did not consider the indirect impact of infrastructure limitations and dependencies. For example, the Mobile Office application - which was planned to be used for all disaster scenarios - was assessed as a low risk application.

32. This condition was due to the inadequacy of the IMD methodology to identify critical ICT systems, which may result in ineffective business continuity and disaster recovery.

(3) IMD should: (i) in coordination with the enterprise-wide risk management and business continuity/recovery working groups, update its methodology to identify critical ICT systems and to assess the risks related to business continuity and disaster recovery; and (ii)

include the risks arising from ICT infrastructure and system dependencies in its risk assessment methodology.

IMD accepted recommendation 3 and stated that given its resources and other business needs, it has determined that the recommendation is best addressed through a work order with a consulting firm. The work order is in the final stages of approval. Recommendation 3 remains open pending receipt of the updated methodologies.

Need to strengthen disaster recovery mitigation strategy and plans

33. The United Nations disaster recovery planning guidelines required the establishment of recovery strategies for all production systems, and defined three categories of solutions: (i) basic; (ii) local resilient infrastructure; and (iii) global resilient infrastructure. The guidelines also defined four planning scenarios to ensure an effective and consistent level of protection.

34. IMD did not use a consistent set of scenarios in preparing its business continuity and disaster recovery plans and test exercises. Some scenarios recommended by the United Nations procedures were not covered in IMD plans.

35. The business continuity plan of IMD of March 2016, described an objective for the implementation of recovery strategies to resume performance of any interrupted business functions. However, IMD did not document these strategies in its business continuity and disaster recovery plans. In order to achieve this objective, IMD recently outsourced some of its ICT systems and services, which also included support for disaster recovery and high availability of the ICT infrastructure. In January 2016, IMD implemented phase 1 of the Bloomberg AIM project, which covered the majority of front, middle and back office functions, and incorporated OMGEO and SWIFT functionalities to provide straight through processing. This platform was hosted by a third party service provider in two data centres located in New York and in New Jersey. This solution allowed IMD to operate in normal conditions, using its network and private leased lines, and in emergency situations, using the Internet. IMD mitigated the risk of unavailability of its core business applications except for the risk of a disaster impacting both data centers residing in the same geographic area. A similar risk might affect the e-Mail system of IMD hosted by UNICC in two separate data centres, both located in the same geographic area.

36. Notwithstanding the recent improvements made in its business continuity and disaster recovery planning, IMD did not identify and document the short and long term recovery strategies to mitigate the risks arising from single points of failures[5] in its ICT infrastructure. The following weaknesses in the ICT infrastructure and processes were found:

(i) IMD outsourced its data backup and restore services to UNICC. However, the frequency of backups for specific servers was not clearly communicated to UNICC. Backup status reports were not reviewed and data restoration tests were not performed. In the absence of backups, IMD might not be able to restore its critical data.

(ii) There was no disaster recovery instance for some data interface servers which were components of critical IMD applications.

(iii) The power source of one data centre was not redundant and, therefore, increased the risk of unavailability of some systems.

[5] Potential single points of failure are parts of any system that, if they occur, would stop the entire system from functioning as expected.

(iv) The uninterrupted power source (UPS) was not installed in a communication room, which connected staff members located on that floor to the IMD network. At the time of the audit, the procurement process to acquire the required UPS was not completed.

37. In order to address some of these weaknesses, IMD prepared a draft business case and work packages, which included: (i) re-designing the IMD network; (ii) installing a UPS in the communication room; (ii) relocating communication devices (i.e., Netscalers and SWIFT); and (iii) separating IMD network equipment from the Fund Secretariat. However, at the time of the audit, this business case was neither finalized nor approved by the IMD Steering Committee.

38. This condition was due to disaster recovery plans that did not include short and long term strategies to address single points of failures in the ICT infrastructure of IMD, which may lead to unavailability of systems in the event of a disruption.

(4) IMD should: (i) update its business continuity and disaster recovery plans with adequate scenarios; (ii) define a short and long term recovery strategy addressing the single points of failure of its critical systems; and (iii) document and communicate the backup schedule for all servers to UNICC.

IMD accepted recommendation 4 and stated that given its resources and other business needs, it has determined that the recommendation is best addressed through a work order with a consulting firm. The work order is in the final stages of approval. Recommendation 4 remains open pending receipt of: short term and long term recovery strategies to address the single point of failures of its critical systems; and backup schedule for all servers which is communicated to UNICC.

Need to strengthen the disaster recovery procedures for ICT systems

39. The United Nations disaster recovery planning guidelines require that recovery procedures should be documented and tested for ICT systems.

40. ISS had documented disaster recovery plans for Bloomberg Services (i.e., Bloomberg – Terminal, AIM and PORT), SWIFT, Risk Metrics and FX/ALL. However, recovery plans and procedures were not documented for some ICT systems (i.e., file sharing, Wilshire/Abacus, IMD Mobile Office, data interfaces with Bloomberg-AIM and Risk Metrics, Active Directory, e-Mail, and the interface with UNJSPF Oracle Financial System). The procedures of FX/ALL and Risk Metrics needed improvement, and the disaster recovery plans were not signed and approved.

41. The testing exercise of business continuity and disaster recovery performed in September 2015 did not cover all IMD systems. The tested scenario covered only the disaster recovery of Charles River and SWIFT.

42. This condition was due to the absence of documented recovery procedures for each application and the lack of adequate tests with clear scenarios and test procedures, which may lead to financial and information losses.

(5) IMD should document and test disaster recovery procedures for all ICT applications and services.

IMD accepted recommendation 5 and stated that given its resources and other business needs, it has determined that the recommendation is best addressed through a work order with a consulting firm. The work order is in the final stages of approval. Recommendation 5 remains open pending receipt of: disaster recovery procedures for all ICT systems and services; and disaster recovery test reports based on these procedures.

B. Coordinated management mechanisms

Coordination with the Fund Secretariat needed to be strengthened

43. In accordance with its terms of reference, the Business Continuity/Recovery Working Group of UNJSPF 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 different 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.

44. In 2015, the Business Continuity/Recovery Working Group met every quarter. The meeting minutes of the working group showed that this body operated primarily as an information sharing group on business continuity activities, rather than a decision making body focused on matters that required coordination between IMD and the Fund Secretariat. 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 of UNJSPF (for both the Fund Secretariat and IMD);

(ii) There was no coordination or agreed procedures during the test exercises related to the continuity and recovery of shared ICT infrastructure, including the shared firewall, router, DHP data centre, emergency notification system, and shared e-Mail infrastructure;

(iii) There was no coordination or agreed procedures for the services provided by the Fund Secretariat to IMD (i.e., for the security token service and shared network devices); and

(iv) IMD was informed by UNICC that the disaster recovery tests of its e-Mail system could not be performed until the Fund Secretariat completed the migration project on the shared platform. However, the working group did not decide on any procedure or timeline for this activity.

45. This condition was due to the absence of effective coordination of business continuity and disaster recovery activities between the Fund Secretariat and IMD which may lead to incomplete or ineffective disaster recovery arrangements.

(6) IMD, in coordination with the Fund Secretariat, should: (i) determine which disaster scenarios need to be used in the development of business continuity and disaster recovery plans and tests; and (ii) document common procedures to be followed during business continuity and disaster recovery tests, with clear responsibilities and roles.

IMD accepted recommendation 6 and stated that given its resources and other business needs, it has determined that the recommendation is best addressed through a work order with a

	consulting firm. The work order is in the final stages of approval. Recommendation 6 remains open pending receipt of common scenarios and procedures which will be followed during the disaster recovery and business continuity tests.

IV. ACKNOWLEDGEMENT

46. OIOS wishes to express its appreciation to the Management and staff of IMD 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 planning in the Investment Management Division of the United Nations Joint Staff Pension Fund

Recom. no.	Recommendation	Critical[6]/ Important[7]	C/ O[8]	Actions needed to close recommendation	Implementation date[9]
1	IMD should: (i) define the recovery time and point objectives for all its outsourced business services, ICT systems, and ICT services by completing the business impact assessment; (ii) identify critical ICT assets and their dependencies; and (iii) prepare risk treatment and action plans to prioritize the implementation of controls.	Important	O	Provide the business impact assessment with recovery time and business objectives for outsourced business services, ICT systems and ICT services, analysis of criticality and dependencies of ICT assets, documentation of controls and priorities, and risk mitigation action plans.	31 March 2017
2	IMD should document and test the business continuity procedures for each business unit.	Important	O	Provide the business continuity procedures for each business unit and test results of each procedure.	31 March 2017
3	IMD should: (i) in coordination with the enterprise-wide risk management and business continuity/recovery working groups, update its methodology to identify critical ICT systems and to assess the risks related to business continuity and disaster recovery; and (ii) include the risks arising from ICT infrastructure and system dependencies in its risk assessment methodology.	Important	O	Provide the updated methodologies.	31 March 2017
4	IMD should: (i) update its business continuity and disaster recovery plans with adequate scenarios; (ii) define a short and long term recovery strategy addressing the single points of failure of its critical systems; and (iii) document and communicate the backup schedule for all servers to UNICC.	Important	O	Provide the short term and long term recovery strategies to address the single point of failures of its critical systems; and backup schedule for all servers which is communicated to UNICC.	31 March 2017
5	IMD should document and test disaster recovery	Important	O	Provide the disaster recovery procedures for all	31 March 2017

[6] 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.
[7] 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.
[8] C = closed, O = open
[9] Date provided by IMD in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity and disaster recovery planning in the Investment Management Division of the United Nations Joint Staff Pension Fund

Recom. no.	Recommendation	Critical[6]/ Important[7]	C/ O[8]	Actions needed to close recommendation	Implementation date[9]
	procedures for all ICT applications and services.			ICT systems and services; and disaster recovery test reports based on these procedures.	
6	IMD, in coordination with the Fund Secretariat, should: (i) determine which disaster scenarios need to be used in the development of business continuity and disaster recovery plans and tests; and (ii) document common procedures to be followed during business continuity and disaster recovery tests, with clear responsibilities and roles.	Important	O	Provide common scenarios and procedures which will be followed during the disaster recovery and business continuity tests.	31 March 2017

APPENDIX I

Management Response

UNITED NATIONS NATIONS UNIES

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar 09 May 2016
A: Deputy Director
Internal Audit Division, OIOS

THROUGH: Ms. Carolyn Boykin
PAR: Representative of the Secretary-General
Investment Management Division
United Nations Joint Staff Pension Fund

FROM: Mr. Daniel Willey
DE: Compliance Officer
Investment Management Division
United Nations Joint Staff Pension Fund

SUBJECT: **Draft report on an audit of business continuity and disaster recovery planning in**
OBJECT: **the Investment Management Division of the United Nations Joint Staff Pension Fund (Assignment No. AT2016/801/01)**

1. Reference is made to your memorandum dated 28 April 2016 providing the report on the above-mentioned audit.

2. I am pleased to provide IMD's comments on the findings and recommendations as requested. Please find attached the Appendix I to the audit recommendations which details IMD's response to the findings.

3. I wish to thank you and OIOS for the recommendations made following the review and for the positive interaction with IMD staff regarding this matter.

cc: Ms. Zelda Tangonan-Fourcade, Acting Chief Operating Officer, IMD
Mr. Daniel Willey, Compliance Officer and Audit Focal Point, IMD
De. Kamel Kessaci, Senior Information Systems Officer, IMD
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS
Ms. Stara Khan, Senior Risk Assistant, IMD
Ms. Wasantha Jayasinghe, Senior Compliance Assistant, IMD

APPENDIX I

Management Response

Audit of business continuity and disaster recovery planning in the Investment Management Division 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	IMD should: (i) define the recovery time and point objectives for all its outsourced business services, ICT systems, and ICT services by completing the business impact assessment; (ii) identify critical ICT assets and their dependencies; and (iii) prepare risk treatment and action plans to prioritize the implementation of controls.	Important	Yes	Acting Chief Operating Officer and, Chief Compliance Officer until appointment of IMD Director	31 March 2017	The recommendations detailed require specific actions that are labor intensive and time consuming. Given the resources, and other business needs of IMD, it has been determined that the recommendations are best addressed through a Work Order within the Provision of Accounting Consultancy Services with PricewaterhouseCoopers (PwC). This Work Order would require that PwC conduct a comprehensive business impact analysis and risk assessment and within this activity address the recommendations from the audit. This Work Order is in the final stages of approval.
2	IMD should document and test the business continuity procedures for each business unit.	Important	Yes	Acting Chief Operating Officer and, Chief Compliance Officer until appointment of IMD Director	31 March 2017	-Same as above -

[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.

APPENDIX I

Management Response

Audit of business continuity and disaster recovery planning in the Investment Management Division 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
3	IMD should: (i) in coordination with the enterprise-wide risk management and business continuity/recovery working groups, update its methodology to identify critical ICT systems and to assess the risks related to business continuity and disaster recovery; and (ii) include the risks arising from ICT infrastructure and system dependencies in its risk assessment methodology.	Important	Yes	Acting Chief Operating Officer	31 March 2017	-Same as above -
4	IMD should: (i) update its business continuity and disaster recovery plans with adequate scenarios; (ii) define a short and long term recovery strategy addressing the single points of failure of its critical systems; and (iii) document and communicate the backup schedule for all servers to UNICC.	Important	Yes	IMD Director and, Acting Chief Operating Officer	31 March 2017	-Same as above -
5	IMD should document and test disaster recovery procedures for all ICT applications and services.	Important	Yes	Acting Chief Operating Officer	31 March 2017	-Same as above -
6	IMD, in coordination with the Fund Secretariat, should: (i) determine which disaster scenarios need to be used in the development of business continuity and disaster recovery plans and tests; and (ii) document common procedures to be followed during business continuity and disaster recovery tests, with clear responsibilities and roles.	Important	Yes	IMD Director	31 March 2017	-Same as above -