INTERNAL AUDIT DIVISION

REPORT 2015/010

Audit of information and communications technology strategic planning, governance and management in the Investment Management Division of the United Nations Joint Staff Pension Fund

Overall results relating to strategic planning, governance and management of information and communications technology were initially assessed as unsatisfactory. Implementation of five important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

11 February 2015
Assignment No. AT2014/800/01

CONTENTS

		Page
I.	BACKGROUND	1
II.	OBJECTIVE AND SCOPE	2
III.	AUDIT RESULTS	2-9
	A. Risk assessment and strategic planning mechanisms	3-8
	B. Project management capacity	8
	C. Performance monitoring indicators and mechanisms	8-9
IV.	ACKNOWLEDGEMENT	9

ANNEX I Status of audit recommendations

APPENDIX I Management response

AUDIT REPORT

Audit of information and communications technology strategic planning, governance and management 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 information and communications technology (ICT) strategic planning, governance and management in the Investment Management Division (IMD) of the United Nations Joint Staff Pension Fund ("UNJSPF" or "Fund").

2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure: (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations and rules.

3. UNJSPF was established by the General Assembly of the United Nations to provide retirement, death, disability and related benefits for the staff of the United Nations and other international intergovernmental organizations admitted to membership in the Fund. The UNJSPF serves about 23 member organizations, with 120,000 active participants and 63,000 beneficiaries. The Fund is internally managed, with an asset portfolio of over $52 billion as of March 2014.

4. 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; Risk and Compliance Section; Information Systems Section (ISS); Operations Section; and Investment Section.

5. ISS provides support for business applications and some infrastructure services (i.e., domain controller and email systems) for IMD users.

6. The UNJSPF Secretariat ("Secretariat") is responsible for the administration and payment of benefits to beneficiaries of the Fund.

7. The Information Management Systems Service (IMSS) of the Secretariat provided support and services for the ICT infrastructure of the Fund. IMSS outsourced some of its ICT services to the United Nations International Computing Centre (UNICC). Telephone services were provided by the Office of Information and Communications Technology (OICT) of the United Nations Secretariat.

8. An ICT consolidation initiative for the whole Fund was being implemented to establish a consolidated, secure and highly-available ICT architecture administered by IMSS staff, with the support of ISS for specific IMD business applications.

9. An Information Technology Executive Committee (ITEC) acted as a forum to discuss ICT strategic issues of the Fund.

10. Comments provided by IMD are incorporated in italics.

II. OBJECTIVE AND SCOPE

11. The audit was conducted to assess the adequacy and effectiveness of IMD governance, risk management and control processes to provide reasonable assurance regarding the **effective and efficient strategic planning, governance and management of ICT in IMD.**

12. This audit was included in the OIOS work plan for 2014 in view of the high risks associated with ICT strategic planning, governance and management in IMD.

13. The key controls tested for the audit were: (a) risk assessment and strategic planning mechanisms; (b) project management capacity; and (c) performance monitoring indicators and mechanisms. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Risk assessment and strategic planning mechanisms** – controls that provide reasonable assurance that strategic plans are in place, and risks relating to ICT operations in IMD are identified, assessed, and managed appropriately;

(b) **Project management capacity –** controls that provide reasonable assurance that IMD has sufficient ICT project management capacity to support its mandate and operations; and

(c) **Performance monitoring indicators and mechanisms** – controls that provide reasonable assurance that appropriate metrics have been established for ICT governance in IMD and are used to monitor the efficiency and effectiveness of ICT operations.

14. The key controls were assessed for the control objectives shown in Table 1. Certain control objectives (shown in Table 1 as "Not assessed") were not relevant to the scope defined for this audit.

15. OIOS conducted this audit from 4 June to 24 October 2014. The audit covered the period from January 2013 to August 2014.

16. 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. The audit methodology included interviews with the management of IMD and a review of strategic plans, project documentation, and reports.

III. AUDIT RESULTS

17. The IMD governance, risk management and control processes examined were initially assessed as **unsatisfactory**[1] in providing reasonable assurance regarding the **effective and efficient strategic planning, governance and management of ICT in IMD**. OIOS made six recommendations in the report to address issues identified in this audit. There were deficiencies in ICT strategic planning and governance due to the absence of a steering committee to assess, document, monitor and approve ICT strategies, projects and policies to effectively achieve the ICT objectives defined in the programme budget. Also, there were control weaknesses with regard to: (i) incomplete ICT consolidation; (ii)

[1] A rating of **"unsatisfactory"** means that one or more critical and/or pervasive deficiencies exist 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.

inadequate ICT risk assessment and project management; (iii) incomplete business continuity and disaster recovery plans; (iv) inadequate segregation of ICT functions; and (v) absence of service level agreements and performance indicators to monitor third party providers of ICT services.

18. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **partially satisfactory**[2] as implementation of five important recommendations remains in progress.

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**
Effective and efficient strategic planning, governance and management of ICT in IMD	(a) Risk assessment and strategic planning mechanisms	Unsatisfactory	Not assessed	Unsatisfactory	Unsatisfactory
	(b) Project management capacity	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(c) Performance monitoring indicators and mechanisms	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Risk assessment and strategic planning mechanisms

Weaknesses in ICT strategic planning and governance structure were addressed

19. The Secretary-General's bulletin on "Information and Communications Technology Boards" requires the development of ICT strategies and plans to ensure the cost effective implementation and management of ICT systems and resources in support of the Organization's activities. Accordingly, an ICT steering committee - composed of business and operational representatives - should be appointed in each office for the formulation, approval, monitoring and assessment of ICT strategies aligned with the Organization's objectives, policies and priorities. This committee should maintain and update information on departmental systems, resources and assets; review existing systems to confirm their cost-effectiveness; and ensure that standard methodologies are consistently used for ICT projects.

20. At the time of the audit there was no ICT governing body in IMD to assess, approve and monitor ICT strategies, projects and policies. The ITEC was an ICT governing body of the Fund composed of representatives of senior management responsible for the review of all ICT projects and initiatives undertaken by the Secretariat. IMD considered itself only an observer member of this body. The Chief of IMD/ISS was the only representative from IMD in the ITEC.

[2] 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.

21. Weekly ICT discussions were held in IMD in a forum comprised of Sections' Chiefs and the Director. This forum, however, did not have any terms or reference, mandate or written agenda. Minutes of the discussions were not maintained.

22. In the proposed programme budget for the biennium 2014-2015, IMD/ISS provided its resource requirements and key programme deliverables. However, IMD/ISS did not document any ICT strategic plan for the biennium 2014-2015 to support the programme budget.

23. IMD/ISS documented several ICT policies. However, due to the absence of an ICT steering committee until November 2014, no consistent procedure was followed to assess, review and approve these policies. In a few cases, policies were approved only by the Chief of ISS. In other instances, instead, they were approved jointly by the Chief of ISS and the Director of IMD. Some ICT policies (i.e., mobile device policy) were considered too restrictive by some IMD staff and managers, resulting in their partial implementation or large number of exceptions granted to specific users.

24. The absence of an ICT steering committee in IMD to assess, document, monitor and approve ICT strategies, projects and policies for the investment and management of IMD resources could lead to waste of resources and failure to effectively achieve the organizational ICT objectives defined in the programme budget for the biennium 2014-2015.

(1) IMD should: (i) establish an ICT steering committee; (ii) introduce a practice of consistently documenting ICT strategic plans and using them to propose programme budgets; and (iii) ensure that ICT policies are consistently approved and implemented.

IMD accepted recommendation 1 and stated that the terms of reference of the ICT Steering Committee have been formally issued and the Committee has met eight times. Regarding the ICT strategic plans for each biennium, the Committee has included this item in its planning/agenda. Within the terms of reference, the matter related to ICT policies has been addressed. Based on the action taken and documented evidence provided by IMD, recommendation 1 has been closed.

Incomplete ICT consolidation

25. In May 2007, in response to a request of the Pension Board, the Chief Executive Officer (CEO) of the Fund and the RSG reached an agreement whereby an ICT infrastructure consolidation of UNJSPF would take place under the responsibility of IMSS to achieve economies of scale, provide a robust and stable ICT environment, reduce risks, and improve the quality of services.

26. An ICT consolidation working group was formed in 2008 to monitor and implement the initiative. In March 2009, the working group reached an agreement in relation to the roles and responsibilities of the ICT teams of IMD and the Secretariat under the proposed consolidation. Further, this group agreed to jointly manage the ICT consolidation by establishing a project management team. This group also approved a memorandum of understanding (MOU), signed by the Secretariat and IMD, to implement the ICT consolidation. The MOU was followed by a master service delivery agreement and addenda for the ICT shared infrastructure and support of specific activities and systems (i.e., help-desk, and the SWIFT and Charles River systems). However, the working group did not meet after 2009. Roles, membership and terms of reference of the ICT consolidation working group (formed in 2008) were not available at the time of the audit, and the project team was not established. Furthermore, the following issues were noted:

(a) The MOU was revised in June 2012, with a provision requiring the review, approval and renewal of all associated ICT service delivery agreements established between IMD and the Secretariat by 31 December 2013. However, these agreements were not renewed; and

(b) A brief on ICT consolidation was provided in various fora, including ITEC and the Audit Committee, and a note was issued by the RSG to the Board of the Fund. However, the progress made in the implementation of the ICT consolidation was neither fully evaluated nor monitored against the expected benefits.

27. In June 2014, the Chief of IMD/ISS presented a report on the status of ICT initiatives to the Audit Committee. The report highlighted the risks stemming from the partial implementation of the ICT consolidation and the lack of clarity pertaining to:

(i) The responsibilities assigned to IMD, IMSS and UNICC; and

(ii) The future of the ICT consolidation including the management of key activities and services (i.e., management of the active directory, file sharing and the email system).

28. The incomplete ICT consolidation and the lack of a clear strategy for the management of ICT services in IMD may result in unclear roles and responsibilities and operational failures that could negatively impact the effectiveness and efficiency of IMD operations.

(2) IMD should, in collaboration with the Pension Fund Secretariat: (i) review the current state of the ICT consolidation against its expected objectives and document a plan of action; and (ii) present the plan for review and approval by the governing bodies of the Fund.

IMD accepted recommendation 2 and stated that in coordination with the Fund Secretariat, it will develop a paper on the results of the ICT consolidation achieved to date. This paper, including a plan for review and approval, will be presented at a future meeting of the enterprise-wide risk management working group for approval by the CEO and RSG. Recommendation 2 remains open pending receipt of evidence demonstrating that the review of the ICT consolidation has been completed and submitted to the Fund's governing bodies.

Inadequate ICT risk assessment processes

29. The enterprise-wide risk management policy of the Fund requires risks to be periodically assessed and managed in accordance with approved methodologies and models, and to follow a "bottom-up" approach in order to place accountability and ownership at all levels of the Fund.

30. The Fund established an enterprise risk management working group chaired by the CEO and the RSG. The Secretariat and IMD had dedicated risk management officers responsible for assisting in the identification and assessment of risks and reporting to senior management the risk profiles and effectiveness of mitigating measures.

31. In May 2014, IMD prepared a draft ICT risk register but this register was not derived from a risk assessment of the ICT infrastructure and systems of IMD. For example, no risk assessment had been performed for some of the critical applications in use (i.e., Exchange servers, Windows active directories, firewalls and business applications). The ICT security officer of IMD was not involved in this process. In addition, no formal communication channels were established between the ICT security and risk officers of IMD. Therefore, the reporting of ICT risks by the risk officer of IMD to the enterprise risk

management working group and senior management was not based on a "bottom-up" approach as required by the policy.

32. Since IMD relied on ICT systems to support its critical operations, the failure to appropriately address ICT risks may have a negative impact on the availability, integrity and confidentiality of data and systems.

33. OIOS has made a recommendation to address this issue in a separate audit of information security in UNJSPF, which is being finalized. Therefore, no additional recommendations were made in the present report.

Incomplete business continuity, disaster recovery planning and security controls

34. The United Nations initiative for organizational resilience recommends the establishment of procedures to ensure the continuity of critical processes in case of failure of information systems and to ensure their timely resumption. Accordingly, disaster recovery plans must include provisions for regular tests to validate the reliability of the supporting documentation and processes, and to train and prepare relevant personnel. Professional best practices (i.e., Control Objectives for Information and Related Technology and International Organization for Standardization (ISO) 27001) also recommend the definition of security controls in the business continuity and disaster recovery plans of the organization.

35. IMD updated its business continuity plan in October 2014 and documented an ICT infrastructure disaster recovery plan in May 2011. However, OIOS identified the following control weaknesses:

(i) The IMD disaster recovery plan and its invocation criteria were not referenced in the business continuity plan.

(ii) The business continuity plan was not documented in accordance with a business impact analysis of various disaster scenarios (such as unavailability of critical ICT systems due to risks related to cyber-attacks, infrastructure failures, and so on).

(iii) Recovery time and point objectives (maximum tolerable length of time that a computer, system, network, or application can be unavailable after a failure) of critical IMD systems had not been defined.

(iv) IMD had not determined its requirements for ICT security controls in the business continuity and disaster recovery plans.

36. The IMD business continuity plan and risk management manual required regular testing of business continuity and disaster recovery plans to verify their effectiveness. However, the details and frequency of the tests to be performed were not defined.

37. IMD tested its disaster recovery plan in May 2012 and documented the test results, shortcomings and corresponding mitigating actions. In 2013, IMD documented another test plan for business continuity and disaster recovery with descriptions of the steps to be followed during a test. Although the test was performed as planned, the test results were not documented. Further, the disaster recovery plan was not updated based on the result of these tests.

38. The management of the ICT infrastructure of IMD had been transferred from IMSS to UNICC in 2014. However, the disaster recovery plan of IMD was not updated to reflect the new arrangements.

39. In 2014, IMD experienced a series of significant ICT outages impacting its operations in New York (i.e., email, Bloomberg data services and other systems). During the resolution of the incidents, there was a communication breakdown among IMD, IMSS and UNICC with regard to the roles and responsibilities. The business continuity plan was not invoked during any of these incidents.

40. A business continuity plan without reference to ICT disaster recovery plan, recovery time and point objectives, unclear invocation criteria, and inadequate testing may prevent IMD from resuming its operations in case of adverse events.

41. The lack of ICT security controls in continuity and disaster recovery planning may compromise the integrity of IMD data and operations in adverse conditions.

(3) IMD should update its business continuity and disaster recovery plans with: (i) invocation criteria; (ii) business impact analysis of disaster scenarios; (iii) the new arrangements established with the United Nations International Computing Centre; and (iv) requirements for ICT security controls.

IMD accepted recommendation 3 and stated that it will update its business continuity and disaster recovery plans with the required elements related to: (i) invocation criteria; (ii) business impact analysis of disaster scenarios; (iii) new arrangements established with UNICC; and (iv) requirements for ICT security continuity. Recommendation 3 remains open pending receipt of the updated disaster recovery and business continuity plans, and the new arrangements established with UNICC.

Inadequate segregation of ICT duties

42. In the Fund's strategic framework for the period 2014-2015, IMD reported the need for skilled resources to deliver the expected level of ICT services. Professional best practices (COBIT) require ICT departments to evaluate their staffing needs on a regular basis or upon major changes to the business, their operations or ICT environment. Accordingly, the ICT function should identify key ICT personnel, minimize reliance on a single individual performing critical job functions, and ensure the segregation of potentially conflicting ICT duties.

43. In IMD, critical ICT systems were supported by a limited number of staff, leading to some staff performing incompatible duties. For example, the Information Security Officer was responsible for both the security and support of ICT systems, and the Information Systems Assistant was the sole responsible staff for the email system. IMD did not evaluate the risks arising from the inadequate segregation of ICT functions.

44. In June 2014, IMD issued a request for proposal for an ICT assessment of its infrastructure, including the corresponding staffing resources required. However, it was still not clear when this exercise would be completed. Inadequate segregation of ICT duties could have a negative impact on the effective, efficient and secure operations of critical IMD systems and operations.

(4) IMD should assess the risks arising from inadequate segregation of ICT duties and develop alternative plans to address the risks pending the completion of its ICT assessment.

IMD accepted recommendation 4 and stated that it will address the need for segregation of ICT duties in light of the implementation of new systems such as the Bloomberg Asset and Investment Manager, as well as the new arrangements with UNICC. IMD is also undertaking a comprehensive

review of the roles and responsibilities of its ICT staff and human resource requirements. Recommendation 4 remains open pending receipt of the results of the review undertaken to mitigate the risks resulting from inadequate segregation of duties.

B. Project management capacity

ICT projects were not managed in a consistent manner

45. IMD adopted the ICT project management methodology "Projects in Controlled Environments" (PRINCE II). PRINCE II defined a project as a temporary organization that is created for the purpose of delivering one or more business products according to an agreed business case. In accordance with this methodology, all ICT initiatives should be evaluated on the basis of documented criteria for classifying the eligible ones as a project. Furthermore, ICT initiatives not classified as projects should be managed based on a defined process.

46. IMD did not document criteria to evaluate its various ICT initiatives and determine which ones should be classified as a project. Several ICT initiatives were implemented by ISS but only a few of them were treated as projects. For example, the upgrade of the email system and the establishment of the Windows active directory were not considered projects. Other initiatives comprising the implementation of the Bloomberg asset and investment management system, Murex and OMGEO were considered ICT projects.

47. ICT projects were not regularly monitored, reviewed and assessed. For example, the implementation of the Bloomberg asset and investment management system and OMGEO (Phase-1) projects was not consistent with the PRINCE II methodology.

48. In the absence of documented evaluation criteria, important ICT initiatives may not be correctly classified. Thus they may not get adequate resources, attention or monitoring to achieve a successful outcome.

(5) IMD should: (i) evaluate its ICT initiatives in accordance with appropriate criteria; (ii) document a process to manage ICT initiatives not classified as a project; and (iii) monitor, review and assess the status and performance of all ICT initiatives and projects.

IMD accepted recommendation 5 and stated that the ICT Steering Committee is working on establishing a priority list of ICT initiatives and relevant performance criteria. The Committee is also monitoring all initiatives not classified as projects to ensure that necessary documentation is developed for each initiative. Recommendation 5 remains open pending receipt of the priority list of ICT initiatives and relevant performance criteria, and the monitoring report on the status and performance of all ICT initiatives and projects in IMD.

C. Performance monitoring indicators and mechanisms

Inadequate monitoring of the ICT services provided by UNICC

49. The United Nations Secretariat adopted the Information Technology Infrastructure Library (ITIL) as a standard for ICT service management. In accordance with this standard, ICT service level agreements should define the level of service expected by client organizations from their service provider (i.e., ICT offices or third party service providers). These terms should include standard definitions and

conditions for: (i) creating service requirements, delivery agreements, and guides; (ii) monitoring, assessing and aligning clients' requirements and services provided; and (iii) complementing the standard service catalogue with details about the organizational structure designed by the service provider with roles, tasks and responsibilities.

50. In June 2012, IMD established an MOU and service delivery agreements with the Secretariat of the Fund for the provision of select ICT services (e.g., help-desk). The MOU contained a provision requiring the Chief of ISS and the Chief Information Officer of the Secretariat to regularly review the service performance under the associated service delivery agreements. However, service performance indicators and formal review mechanisms were not put in practice.

51. In 2014, a service delivery agreement was established between the Fund and UNICC for the provision of IMD infrastructure support services. With regard to this agreement, OIOS noted that:

(i) Concerns were raised by IMD about the operational management of this agreement because IMD was not directly involved in the relationship and communication with UNICC; and

(ii) IMD lacked agreed upon criteria, performance indicators and metrics necessary to monitor UNICC services. In this regard, the Director of IMD intended to establish a direct relationship with UNICC for the ICT services to be provided directly and exclusively to IMD. However, a service delivery agreement for this purpose had not yet been established.

52. The absence of service level agreements and approved performance indicators and monitoring mechanisms may prevent IMD from receiving the expected level of ICT services and achieving best value for money.

(6) IMD should manage its relationship with the United Nations International Computing Centre on the basis of a formal memorandum of understanding and service delivery agreements complete with clear performance indicators.

IMD accepted recommendation 6 and stated that a business change order has been already signed with UNICC for the management and support of the IMD email system. A separate MOU between UNICC and IMD is being finalized. Once the MOU has been signed, appropriate service delivery agreements for additional services will be prepared. Recommendation 6 remains open pending receipt of the MOU and service delivery agreements signed by IMD with UNICC.

IV. ACKNOWLEDGEMENT

53. 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*) David Kanja
Assistant Secretary-General for Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology strategic planning, governance and management in the Investment Management Division of the United Nations Joint Staff Pension Fund

Recom. no.	Recommendation	Critical[3]/ Important[4]	C/ O[5]	Actions needed to close recommendation	Implementation date[6]
1	IMD should: (i) establish an ICT steering committee; (ii) introduce a practice of consistently documenting ICT strategic plans and using them to propose programme budgets; and (iii) ensure that ICT policies are consistently approved and implemented.	Critical	C	Action completed	Implemented
2	IMD should, in collaboration with the Pension Fund Secretariat: (i) review the current state of the ICT consolidation against its expected objectives and document a plan of action; and (ii) present the plan for review and approval by the governing bodies of the Fund.	Important	O	Receipt of documentation on the results of the review of ICT consolidation and their submission to the Fund's governing bodies.	30 June 2015
3	IMD should update its business continuity and disaster recovery plans with: (i) invocation criteria; (ii) business impact analysis of disaster scenarios; (iii) the new arrangements established with United Nations International Computing Centre (UNICC); and (iv) requirements for ICT security controls.	Important	O	Receipt of the updated disaster recovery and business continuity plans.	30 September 2015
4	IMD should assess the risks arising from inadequate segregation of ICT duties and develop alternative plans to address the risks pending the completion of its ICT assessment.	Important	O	Receipt of the results of the review undertaken to mitigate the risks resulting from inadequate segregation of duties.	31 December 2015
5	IMD should: (i) evaluate its ICT initiatives in accordance with appropriate criteria; (ii) document a process to manage ICT initiatives not classified as	Important	O	Receipt of the priority list of ICT initiatives and relevant performance criteria, and the monitoring report on the status and performance	31 December 2015

[3] 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.
[4] 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.
[5] C = closed, O = open
[6] Date provided by IMD in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology strategic planning, governance and management in the Investment Management Division of the United Nations Joint Staff Pension Fund

Recom. no.	Recommendation	Critical[3]/ Important[4]	C/ O[5]	Actions needed to close recommendation	Implementation date[6]
	a project; and (iii) monitor, review and assess the status and performance of all ICT initiatives and projects.			of all ICT initiatives and projects in the IMD.	
6	IMD should manage its relationship with the United Nations International Computing Centre on the basis of a formal memorandum of understanding and service delivery agreements complete with clear performance indicators.	Important	O	Receipt of the MOU and service delivery agreements signed by IMD with UNICC.	31 December 2015

APPENDIX I

Management Response

UNITED NATIONS NATIONS UNIES

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar, Deputy Director 22 January 2015
A: Internal Audit Division, OIOS

THROUGH: Ms. Carol Boykin, CFA
PAR: Representative of the Secretary General 4 Feb 2015
United Nations Joint Staff Pension Fund

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

SUBJECT: Draft report on an audit of information and communications technology strategic planning, governance and management in the Investment Management Division of UNJSPF (Assignment No. AT2014/800/01)

1. Reference is made to your memorandum dated 6 January 2015 providing the report on the above mentioned audit.

2. I am pleased to provide Investment Management Division's (IMD) comments on the findings and recommendations as requested.

3. Please find attached the Annex to the audit recommendations which details IMD's responses to the findings.

4. Specific to the "Critical" recommendation regarding the establishment of an IMD ICT Steering Committee. IMD has formally established an IMD ICT Steering Committee. OIOS nominated a representative to participate in the meetings as described in the Terms of Reference separately provided to OIOS for review. The Terms of Reference for this Committee have been formally issued. In implementing the recommendation, the Committee has addressed the need for comprehensive ICT strategic plans which will be used in the formulation of strategic frameworks and budget proposals. The Committee ensures that IMD ICT policies are aligned with the needs of the Division and approved and supported by all relevant Sections and that the implementation of the plans are continuously and appropriately monitored. The Committee has met eight times since its first meeting on 3 November 2014. At these meetings substantive matters were addressed including the decommissioning of the Murex Accounting system as well as ICT strategic plans, programme budgets, and policies (all consistent with the OIOS recommendation). The copies of the minutes were separately provided to OIOS for review.

5. 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. Suzanne Bishopric, Director, Investment Management Division, UNJSPF
Mr. Paul Dooley, Deputy Chief Executive Officer, UNJSPF
Mr. Ajit Singh, Deputy Director of Risk and Compliance, IMD
Ms. Pirjo Sinikallio, Senior Programme Officer, IMD
Ms. Kathalina Manosalvas, Risk Officer and Audit Focal Point, UNJSPF
Dr. Kamel Kessaci, Senior Information Systems Officer, IMD
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS
Mr. Fernando Salon, Chief UNJSPF Audit Section, OIOS
Mr. Dino Cataldo Dell'Accio, Chief ICT Audit Section, Internal Audit Division, OIOS

APPENDIX I

Management Response

Audit of information and communications technology strategic planning, governance and management 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) establish an ICT steering committee; (ii) introduce a practice of consistently documenting ICT strategic plans and using them to propose programme budgets; and (iii) ensure that ICT policies are consistently approved and implemented.	Critical	Yes	Chair, IMD ICT Steering Committee	Implemented.	The TOR of the IMD ICT Steering Committee has been (i) formally issued and the Committee has met eight times. (ii) Regarding the ICT strategic plans for each biennium the Steering Committee has included this item in its planning/agenda. (iii) Within the ICT TOR the matter of ICT policies is addressed.
2	IMD should, in collaboration with the Pension Fund Secretariat: (i) review the current state of the ICT consolidation against its expected objectives and document a plan of action; and (ii) present the plan for review and approval by the governing bodies of the Fund.	Important	Yes	Chair, IMD ICT Steering Committee	June 2015	IMD will in coordination with the Fund Secretariat develop a paper on the results of the ICT consolidation achieved to date. This paper including a plan for review and approval will be presented at a future meeting of the enterprise-wide Risk Management Working Group for the approval of the CEO/RSG.
3	IMD should update its business continuity and disaster recovery plans with: (i) invocation criteria; (ii) business impact analysis of disaster scenarios; (iii) the new arrangements established with United Nations International Computing Centre (UNICC); and (iv) requirements for ICT security controls.	Important	Yes	IMD Information Systems Officer and the Deputy Director, Risk and Compliance	September 2015	IMD will update its business continuity and disaster recovery plans with the required elements related to (i) invocation criteria; (ii) business impact analysis of disaster scenarios; (iii) the new arrangements established with UNICC; and (iv) requirements for ICT security continuity.

[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.

APPENDIX I

Management Response

Audit of information and communications technology strategic planning, governance and management 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
4	IMD should assess the risks arising from inadequate segregation of ICT duties and develop alternative plans to address the risks pending the completion of its ICT assessment.	Important		Chair, IMD ICT Steering Committee	December 2015	IMD will address the need for segregation of ICT duties in light of the implementation of new systems such as Bloomberg AIM as well as the new arrangements with ICC. Also under the new leadership, IMD is undertaking a comprehensive review of the roles and responsibilities of its ICT staff and human resource requirements.
5	IMD should: (i) evaluate its ICT initiatives in accordance with appropriate criteria; (ii) document a process to manage ICT initiatives not classified as a project; and (iii) monitor, review and assess the status and performance of all ICT initiatives and projects.	Important	Yes	Chair, IMD ICT Steering Committee	December 2015	IMD ICT Steering Committee is working on establishing a priority list for IMD ICT initiatives and relevant performance criteria. The Committee is also monitoring all initiatives which are not classified as projects and the necessary documentation of each such initiative.
6	IMD should manage its relationship with United Nations International Computing Centre on the basis of a formal memorandum of understanding and service delivery agreements complete with clear performance indicators.	Important	Yes	Chair, IMD ICT Steering Committee	December 2015	IMD and ICC have already signed a relevant Business Change Order for the management and support of the IMD email system. The MOU between ICC and IMD is being finalized. Once the MOU has been signed, the Service Delivery Agreements will be revised accordingly.