INTERNAL AUDIT DIVISION

REPORT 2017/015

Audit of the new trade order management system in the Investment Management Division of the United Nations Joint Staff Pension Fund

There was need to document a benefits review plan and strengthen system security

23 March 2017
Assignment No. AT2016/801/02

Audit of the new trade order management system in the Investment Management Division 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 new trade order management system in the Investment Management Division (IMD) of the United Nations Joint Staff Pension Fund (UNJSPF). The audit covered the period from December 2013 to November 2016 and included a review of the functionalities implemented in phase I of the project that went live on 18 January 2016. These included functionalities related to investment management (i.e., portfolio management and electronic equity trading), compliance, operations and electronic payment processing.

IMD needed to document a benefits review plan and strengthen system security.

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

- Update the business case for the new trade order management system; document a benefits review plan; and update the project risk register for the system.
- Complete the decommissioning plan for its old trade order management system and the related payment system.
- In consultation with the Procurement Division include an appropriate clause in future bid documents/contracts for such services to safeguard itself in situations where a cyber security breach and/or severe disruption in the system provider's information and communications technology (ICT) environment could result in financial loss to the Organization.
- Based on lessons learned during implementation of phase 1 of the new trade order management system, should strengthen user acceptance testing for phase 2 by: (i) completing user acceptance tests for all processes; (ii) ensuring that workflows are finalized before conducting the tests; (iii) ensuring independent validation of test plans and results; (iv) including ICT security test scenarios in the test plans; and (v) using a test environment for user acceptance testing.
- Update its user access forms to include additional functions and permissions relating to the new trade order management system; establish a change control procedure to ensure that brokers classified as 'non-performing/unsatisfactory' are immediately de-activated in the system; establish a process to use the system's change management functionality; evaluate both 'production test' and the 'beta' environments with respect to their functionalities and costs and choose the one best suited to its needs; and set up procedures to manage the 'beta test environment' for testing process changes and rollouts.
- Document and implement a comprehensive ICT security plan for the new trade order management system in accordance with its ICT security policy and procedures to address the identified weaknesses.
- Finalize its requirements for retention of system emails and messaging to ensure compliance with its communication practices and document retention policy.

IMD 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 United Nations Joint Staff Pension Board and the General Assembly indicating management's acceptance of residual risks.

CONTENTS

Audit of the new trade order management system 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 the new trade order management system in the Investment Management Division (IMD) of the United Nations Joint Staff Pension Fund (UNJSPF).

2. The Fund comprises of the Secretariat, with the responsibility for pension plan administration, and IMD, with the responsibility for investment of the Fund's assets. Management of the Fund's investments is the fiduciary responsibility of the Secretary-General of the United Nations. The Secretary-General has delegated this responsibility to the Representative of the Secretary-General (RSG).

3. The majority of the Fund's assets were internally managed by the staff of the IMD. As of October 2016, the market value of the Fund's assets was approximately $53.8 billion with global equities comprising 61.8 per cent and the global fixed income comprising 28.2 per cent of the total portfolio. The remaining 10 per cent was spread across real assets, alternative investments, cash and short-term investments.

4. IMD had implemented its legacy trade order management system in 2010. However, in 2014, IMD determined that this system did not fully meet its requirements. Further, the system was deemed to be at risk of failure due to its obsolete underlying information and communications technology (ICT) infrastructure. IMD determined that upgrading the existing system required major changes to its underlying ICT infrastructure. IMD conducted a cost-benefit analysis between upgrading the legacy system and purchasing a new trade order management system. Based on this analysis, IMD proposed to procure the new system (premium version with enhanced features) as a stop-gap measure for a period of three years with a comprehensive request for proposal being issued in future that will allow IMD to select the most suitable platform available then.

5. Accordingly, in April 2015 the Headquarters Committee on Contracts (HCC) recommended approval of the case pursuant to United Nations Financial Rule 105.16 (a) (i) which states that the Under-Secretary-General for Management may determine for a particular procurement action that using formal methods of solicitation is not in the best interest of the United Nations when there is no competitive marketplace for the requirement. Based on the HCC recommendation, IMD established a contract with system provider for an initial period of two years with the option to extend for one additional year in the total not-to-exceed amount of $2.6 million.

6. The new trade order system was implemented in two phases. The first phase was initiated in August 2015 and implemented in January 2016. It included functionalities related to investment management (i.e., portfolio management and electronic equity trading), compliance, operations and electronic payment processing. The second phase was planned to be implemented by end 2016 and included the remaining functionalities: (i) electronic fixed income trading; (ii) electronic foreign exchange trading; and (iii) transaction cost analysis.

7. System contracts for phase 1 were signed in July 2016 and those for phase 2 were signed in April 2016. The system license purchased by IMD included on-site assistance, premium trade-desk support, customized training, and invitation to knowledge-sharing events.

8. The new trade order management system was offered as "Software as a Service" (SaaS) – a delivery model in which software and its associated data are hosted centrally by the system provider and accessed remotely as a web-based service by IMD staff. The subscription fee for this service was charged to IMD on a monthly basis. SaaS offered several advantages such as: (i) ease of use; (ii) scalability; (iii) managed maintenance and upgrades; (iv) customer service and helpdesk; and (v) in-built disaster recovery. However, SaaS could also give rise to concerns related to privacy and ICT security.

9. The total cost of ownership for the new trade order management system over a three-year period was estimated to be approximately $3.1 million plus a one-time cost of $183,000. The project was expected to remain within the estimated costs.

10. From February to October 2016, equity purchases worth approximately $4.5 billion and equity sales worth $4.3 billion had been transacted in the new system through 1,774 trades.

11. IMD adopted the United Nations ICT project management framework "Projects in Controlled Environments" (PRINCE 2) for implementing the new system.

12. Comments provided by IMD are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

13. 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 new trade order management system.

14. This audit was included in the 2016 risk-based work plan of OIOS due to the risk that potential weaknesses in implementing the new system may have an adverse impact on the management of investments in IMD.

15. OIOS conducted this audit from August to November 2016. The audit covered the period from December 2013 to November 2016. Based on an activity-level risk assessment, the audit covered higher and medium risks of the processes implemented in phase I of the project that went live on 18 January 2016.

16. The audit methodology included: (a) interviews with key IMD staff; (b) review of relevant documentation, contracts, policies and procedures; (c) analytical review of data; (d) sample testing/review of failed trades, reconciliation statements, compliance rules, payment messages and Standard Settlement Instructions[1]; and (e) ICT security tests using the system terminal.

III. OVERALL CONCLUSION

17. The new system has enabled transparent trade order processing with integrated compliance review. Portfolio holdings were electronically linked to market data, custodian banks and the master record keeper. User log-on process to the system was secure and required a combination of a password and the user's finger imprint. However, IMD needed to document and implement a comprehensive ICT security plan for the system. IMD also needed to strengthen controls in some areas relating to project management, user acceptance testing, change management, and finalizing the requirements for retention of the system's emails and instant messages.

[1] Standard Settlement Instructions are agreements between two financial institutions.

IV. AUDIT RESULTS

A. Project management

Project management controls needed to be strengthened

18. The United Nations ICT project management framework defines an ICT project as a one-time effort undertaken to produce major products, services or results for the Organization for a specified period of time, and within defined resource constraints. The project lifecycle consists of project initiation, project execution and project closing. Project management controls require that a valid business case, which provides the rationale and business justification for the project, should be reviewed and updated throughout the project life-cycle. Further, the project initiation documentation (PID) should contain: (i) information security requirements to ensure confidentiality and integrity of the data; and (ii) benefits review plan, to define and measure achievement of the project's benefits. Additionally, the project risk register should be updated with important risks that could impact the project.

19. Implementation of the new trade order management system was generally managed in accordance with the United Nations project management framework. However:

(i) The approved business case was not updated at various stages of the project. For example, it was not updated with the revision in project cost elements (e.g., number and type of system terminals) and changes in business requirements.

(ii) High-level information security requirements were specified in the PID; however, a comprehensive ICT security plan to define and implement these requirements in alignment with the IMD ICT security policy and procedures (e.g., ICT security policy, managing user rights to the IMD systems) was not documented. Though detailed information security requirements were not defined yet, OIOS conducted ICT security tests to check the extent of ICT security weaknesses in the new system. ICT security weaknesses were found, as explained in Section B of the present report.

(iii) A benefits review plan to define how and when measurement of the achievement of the project's intended benefits could be made was not documented.

(iv) The project risk register did not document the risk that the new system had been implemented only as a stop-gap arrangement for a period of three years. Its continuation after three years remains uncertain. This uncertainty could have a significant impact on IMD operations and needs to be appropriately managed.

20. This condition was caused because the above aspects were not considered in project planning and execution. This may prevent IMD from: (i) continuously evaluating the validity and relevance of the business case for the new system; (ii) reviewing the benefits of its implementation; and (iii) monitoring important project risks.

(1) IMD should: (i) update the business case for the new trade order management system for cost elements and business requirements; (ii) document a benefits review plan; and (iii) update the project risk register for the system.

IMD did not accept recommendation 1 stating that it does not see the need or benefit of updating this documentation post facto. But looking forward, IMD will perform an ex ante study and lessons

learned documentation for business cases. Additionally, a consultant firm is assisting IMD with a full ICT target operating model assessment which includes all systems, processes and ICT risks. OIOS is of the view that: (i) failure to update the business case weakened the ability of IMD to evaluate its validity, track costs, and monitor the changes made to business requirements; (ii) the absence of a benefits review plan was a hindrance to assessing the benefits expected from the new system; and (iii) an outdated project risk register significantly diminished its utility to manage risks effectively. OIOS is of the opinion that these conditions reflect significant weaknesses in project governance and if left unaddressed, they may be considered to be acceptable practices for future ICT initiatives. Particularly, the lack of a benefits review plan is a matter of concern because it is one of the basic requirements of ICT project management. Allowing such a requirement to be disregarded may reflect adversely on the control environment in IMD. This unaccepted recommendation has been closed without implementation and may be reported to the United Nations Joint Staff Pension Board (UNJSPB) and the General Assembly indicating management's acceptance of residual risks.

Plans for decommissioning old applications needed to be updated

21. The Office of Information and Communications Technology of the United Nations Secretariat has published a technical procedure to decommission the obsolete ICT applications. This procedure recommends the documentation of: (i) business impact analysis; (ii) legal and financial review of licenses, contractual obligations, and costs associated with decommissioning; (iii) review of ICT security implications; (iv) ICT asset disposal, deployment, reuse or retirement; (v) disposal or retention of data, in accordance with the organizational data retention and information security policies; and (vi) a communication strategy to keep all impacted parties informed.

22. In view of implementation of the new trade order management system, IMD had decided to decommission some of its important ICT applications, system and functionalities that would become obsolete or irrelevant with the implementation of the new trade order management system. These included old (legacy) trade order management system and the payment system.

23. IMD documented plans to decommission these old systems after the implementation of phase I of the new system. The decision to decommission the legacy trade order management system was made before the implementation of the new system, while the decision to the payment system was made in May 2016.

24. The decommissioning plans were not updated with reference to communication strategy and ICT security implications. Additionally, the decommissioning plan for the legacy trade order management system did not include any associated costs while the decommissioning plan for the payment system was not updated with reference to asset disposal, deployment, reuse or retirement.

25. Lack of a comprehensive plan for decommissioning of old ICT applications could result in additional costs, ICT security vulnerabilities, and lack of communication to the affected parties.

(2) IMD should complete the decommissioning plan for its old trade order management system and the related payment system.

IMD did not accept recommendation 2 stating that it has fully decommissioned the legacy trade order management and related systems. The Information Systems Section in collaboration with IMD users is working on the archiving of this information system data. The archiving is required as per the IMD retention policy (seven years). Given the time and human resources constraints, IMD considered the implementation of the new trade order management system had a much higher priority than archiving this data already saved. The archiving activity has already started and expected to be completed in

the third quarter of 2017. OIOS notes that the audit identified control deficiencies in decommissioning plans which exposed IMD to additional costs, ICT security vulnerabilities, loss of data, errors and lack of information to the concerned parties. This unaccepted recommendation has been closed without implementation and may be reported to UNJSPB and the General Assembly indicating management's acceptance of residual risks.

Need to protect IMD from financial loss in the event of security breaches and disruptions

26. ICT best practice "Control Objectives for Information and Related Technologies" (COBIT) recommends that commercial contracts for an ICT system contain clauses on non-disclosure, ICT security requirements, and liabilities.

27. The contract signed by IMD for the new trade order management system contained a liability provision which limited the legal damages potentially recoverable from the system provider in the event of the breach of contract to a monetary cap of $432,000 (excluding third party claims, bodily injury and fraudulent data claims). It also included a waiver of liability clause which did not cover situations where a cyber security breach and/or severe disruption in the system provider's ICT environment could result in a financial loss to IMD. The absence of adequate contractual protection may expose IMD to unexpected financial loss. OIOS recognizes that it may not be feasible to renegotiate the contract with the system provider at this stage in view of the stop-gap nature of the arrangement but is of the view that IMD should revisit this issue and include appropriate provisions in the request for proposal/contract that may be awarded after a competitive bidding process in future.

(3) IMD, in consultation with the Procurement Division, should include an appropriate clause in future bid documents/contracts for such services to safeguard itself in situations where a cyber security breach and/or severe disruption in the system provider's ICT environment could result in financial loss to the Organization.

IMD did not accept recommendation 3 but stated that it agrees with the importance of safeguarding against cyber security breaches and/or severe disruptions in the system provider's ICT environment. Therefore, IMD is launching an overall security assessment which will assess all of IMD's ICT vendors relative to best industry practices. Due to concern that this could delay or prevent contract finalization, IMD does not accept this recommendation. To the extent possible, IMD will add security/disruption clauses to contracts with service providers. OIOS maintains that appropriate safeguards against cyber security breaches and/or severe disruption in services are essential to protect the interests of the Organization. Therefore, OIOS will continue to review IMD's future contracts for such ICT services and report any failures to include appropriate safeguards against these risks. This unaccepted recommendation has been closed without implementation and may be reported to UNJSPB and the General Assembly indicating management's acceptance of residual risks.

Procedure manuals were being updated

28. COBIT recommends that detailed user reference and manuals to support the implementation of an ICT system.

29. IMD documented quick reference notes (cheat-sheet) in January 2016, detailing basic steps and system functions required by the Front, Middle and Back Office users to process transactions in the new trade order management system. These were supplemented with the generic help manuals downloadable from the system application. Furthermore, some stand-alone processes related to broker setup and watch

list for corporate actions[2] were created. However, this cheat-sheet did not consider all scenarios such as setting up/modifying new standard settlement instructions, errors in payment messages, and impact on reconciliation statements in case of any cancellation/correction to the trade data. For example, OIOS review of the Reconciliation module in the new system showed that any change in the trade data would also change the corresponding reconciliation statements. However such changes could not be easily detected as the system did not place any identifier on the modified data/reconciliation statement. Absence of a process to handle such a scenario could result in errors or delays in reconciliation.

30. OIOS is of the view that the cheat-sheet does not replace the need to update IMD procedure manuals for the Middle and Back Offices. IMD procedures for the legacy trade order management system contained detailed information on operational risks, controls and accountability, which was not documented in the cheat-sheet for the new system. IMD stated that it will continue to update all its procedure manuals. In view of the action being taken by IMD, OIOS did not make a recommendation in this area.

User acceptance testing procedures needed to be strengthened for phase 2

31. COBIT recommends establishing a test plan based on enterprise standards and approved workflow that defines roles, responsibilities, and criteria. It recommends: (i) testing of all functional and technical requirements including those for ICT security; (ii) confirming that all test plans are approved by stakeholders, including business process owners and ICT, as appropriate and independently validated; and (iii) defining and establishing a secure test environment representative of the planned business process.

32. IMD had conducted user acceptance tests for all processes except the reconciliation process and the cash management process. The user acceptance tests conducted were not based on approved documented workflow. The tests were completed in December 2015, while workflow was documented and approved in January 2016. The workflow should have been finalized before the conduct of user acceptance tests to ensure completeness of the test plans and scenarios.

33. The user acceptance test plans did not consider the ICT security scenarios for system functionality and user access to measure security weakness or loopholes. For example: (i) user acceptance test for the payment module did not test whether the users could copy/edit the messages or create any unauthorized messages; and (ii) no test scenarios were included to check whether users could perform conflicting roles (for example, if traders could access the 'business decision support' functionality which is reserved for the investment officers).

34. Reviewers and approvers for the user acceptance tests were the same set of users; an independent validation of the test plans and results was not done to ensure their completeness.

35. IMD was not provided a separate test database for the user acceptance tests on the new trade order management system. The pre-production database set up in August 2015 by the system provider was used for workflow configuration as well as user acceptance testing. The pre-production database was converted into the production database on 18 January 2016. Consequently, some test data was mixed up with the production data. The system provider had installed a test environment (beta environment) on 19 January 2016 after the implementation of the phase 1 of the system.

[2] A "corporate action" is an event (such as stock split, change or name, merger) initiated by a public company that affects the securities issued by the company. It may have a direct impact on the shareholders of the security. Failure to correctly process a corporate action can result in substantial loss to the company.

36. This condition was due to inadequacies in planning for user acceptance testing. Weaknesses in user acceptance testing may result in problems in product quality and integrity of data. OIOS is of the view that user acceptance testing for phase 2 of the system needs to be improved based on the lessons learned during phase 1.

(4) IMD, based on lessons learned during implementation of phase 1 of the new trade order management system, should strengthen user acceptance testing for phase 2 by: (i) completing user acceptance tests for all processes; (ii) ensuring that workflows are finalized before conducting the tests; (iii) ensuring independent validation of test plans and results; (iv) including ICT security test scenarios in the test plans; and (v) using a test environment for user acceptance testing.

IMD did not accept recommendation 4 stating that this recommendation might best be placed under "opportunities for improvement". IMD is continuing to perform user acceptance tests. All tests are performed in a testing environment (beta). OIOS maintains that recommendation 4 addresses control weaknesses that occurred during phase 1 which need to be prevented from re-occurring in phase 2. These are not just "opportunities for improvement" but essential control processes based on industry practices. This unaccepted recommendation has been closed without implementation and may be reported to UNJSPB and the General Assembly indicating management's acceptance of residual risks.

B. ICT support systems

Roles and responsibilities of ICT staff were being clarified

37. COBIT recommends organizations to define the focus, roles and responsibilities of each function within the ICT-related organizational structure.

38. IMD had not updated the job descriptions with respect to focus, roles and responsibilities of the ICT function with respect to the management/maintenance of the new trade order management system. For example, two ICT staff had been designated as 'Primary Admin' and 'Secondary Admin' in the system but their focus, roles and responsibilities were not documented. The lack of clear roles and responsibilities may lead to inefficiencies and errors in the administration of the new system.

39. IMD stated that it would document the new roles and responsibilities for the ICT staff. IMD has recently issued a request for proposal for the review of its operating model. Job descriptions and workflows would be reviewed in this study. OIOS therefore did not make any recommendation in this area.

Change management needed to be strengthened

40. COBIT recommends a formal change management procedure to handle requests for changes to applications.

41. IMD had not established a change management procedure to support the new system. The following weaknesses were noted:

(i) All changes to the backend of the system were controlled by the system provider. These changes included addition or removal of system administrators, enabling/ disabling super users, switching on/off the "4-eye principle" for various system functionalities. These changes were communicated to the system provider by IMD through e-mails and/or the

system relationship manager. However, there was no change management process in place to identify, describe, evaluate, classify (as 'normal' or 'emergency'), approve, and track these change requests.

(ii) Changes to user access and privileges were controlled by IMD system administrators. The forms used to control user access to the new system did not contain enough information on the special functions that could be provisioned to the user. Furthermore, this form did not include user provision with respect to system sub-modules. Inappropriate assignment of access could result in potential role conflicts.

(iii) IMD did not implement a change control procedure to timely deactivate brokers in the system, who were evaluated as 'non-performing/unsatisfactory' by the broker evaluation committee. Three 'non-performing/unsatisfactory' cases in the broker evaluation report for the first quarter of 2016 were marked as active in the new system.

(iv) The system used a change control functionality to provide information to its users on the future features, updates and/or changes to the existing work-flows, and complex corporate actions. IMD had not yet established a process to use this functionality. Users were not yet trained in this functionality. OIOS noted one incident where delay was caused in the processing of a corporate action due to lack of monitoring. This resulted in a variance between the positions shown as held by IMD's custodian[3] and the new trade order management system. The variance was subsequently resolved after the portfolio manager pointed the error to the operations team. IMD stated that it would regulate the use of the change control functionality during phase 2 of the project.

(v) OIOS brought to the attention of IMD that the system provider offered two types of test environment – "production test environment" and "beta test environment" – to test the process changes and rollouts before implementing them in the production environment. These two test environments were different in terms of their configuration, cost, and functionality. For example, the "production test environment" closely replicated the production environment, unlike the 'beta environment'. IMD had not yet evaluated which test environment is best suited to its need and was currently subscribed to the 'beta test environment'. IMD stated that it could not evaluate different test environments as this information was not available in the system provider's initial proposal.

(vi) IMD had not established a process to manage the 'beta test environment'.

42. The absence of change management procedures requiring analysis and impact of changes may result in unauthorized changes, weak ICT security, system malfunctions/disruptions and inefficiencies.

(5) IMD should: (i) update its user access forms to include additional functions and permissions relating to the new trade order management system; (ii) establish a change control procedure to ensure that brokers classified as 'non-performing/unsatisfactory' are immediately de-activated in the system; (iii) establish a process to use the system's change management functionality; (iv) evaluate both 'production test' and the 'beta' environments with respect to their functionalities and costs and choose the one best suited to its needs; and (v) set up procedures to manage the 'beta test environment' for testing

[3] An agent appointed by the United Nations to act as a global custodian for the assets deposited with the bank and held by the bank in the name of the United Nations on behalf of the participants and beneficiaries of the Fund in various parts of the world.

process changes and rollouts.

IMD accepted recommendation 5 and stated that it has included these tasks in the phase 2 of the project. IMD recently updated its user access forms to include additional functions and permissions. Any other procedures will be revised under the ICT strategy study, also known as Target Operating Model Assessment. Recommendation 5 remains open pending: (i) receipt of updated IMD user access forms; (ii) establishment of a change control procedure to ensure that brokers classified as non-performing/unsatisfactory are immediately de-activated in the system; (iii) establishment of a process to use the system's change management functionality; (iv) evaluation results for both production test environment and the beta environment; and (v) procedure to manage the 'beta test environment' for testing process changes and rollouts.

Business continuity and disaster recovery plans needed to be improved

43. 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 recommends re-evaluation of risks and their impact in accordance with any changes to the operating environment, procedures, functions, services, partnerships, and supply chains.

44. As the new trade order management system is a managed service, the disaster recovery for the application is managed by the system provider who had submitted: (i) a statement on its business continuity programme; (ii) a service organization control (SOC) 3 report from independent accountants; (iii) Data Centre Resilience Study; and (iv) confirmation on the daily back-up procedures. The SOC 3 report shared by the provider stated that in April 2015 it experienced a significant outage impacting many clients globally. Remedial actions were implemented by the system provider soon thereafter to prevent future incidents.

45. IMD had documented a disaster recovery plan for the new system in February 2016. It also successfully tested the plan in June 2016 for two scenarios. However, IMD did not test a scenario where users with expired remote access to the system would need to reactivate it before using the system. Remote access to the system expires after 30 days of no user activity and needs to be reactivated before users could remotely access the system again. Such a scenario is important to provide assurance that in the event of disaster, users could reactivate their remote access in a timely manner through any of the approved channels.

46. Additionally, IMD updated its business continuity plan in October 2016 and designated three senior investment officers as backup traders who would be granted "Trader Role" access to the global equity trading platform in the system in case of a severe business interruption. However, this scenario was yet to be tested.

47. IMD had not conducted a business impact assessment with respect to non-availability of the new system. No service level agreement was signed with the system provider agreeing upon 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).

48. Since OIOS had made related recommendations in its audit of business continuity and disaster recovery planning in IMD (AT2016/801/01), no additional recommendations were made in this area.

Weaknesses in ICT security of the new system needed to be addressed

49. The new trade order management system was offered as 'Software as a Service'. The system provider was responsible for the security of its environment as well as the application database and infrastructure. The system provider provided several documents and explanations on its internal ICT security practices. OIOS could not independently verify these practices as the system provider's environment was restricted for visit by its customers. OIOS therefore relied on the statement of internal control report prepared by the independent accountants for the system provider.

50. IMD had documented user access to the production environment in January 2016. This document contained details only on end-user roles but did not contain details on roles configured in the new system's sub-modules. This document had not been updated. Additionally, the IMD ICT security officer prepared a document on network architecture, system administration and information security officer roles and responsibilities in August 2016 but this document was not comprehensive enough to cover all ICT security requirements such as log management and security of the IMD File Transfer Protocol (FTP) site, and storage of data feeds from the system. IMD stated that it would review and update the user access document in phase 2 of the project.

51. While an ICT security plan was yet to be prepared for the new system, OIOS review of the post-implementation ICT security showed a number of weaknesses as detailed below.

(i) Log management

52. Log management and review process for the system was inadequate. Logs were reviewed only on a monthly basis by comparing the log file generated on the first day of the month with the log file generated on the last day of the month. Thus, all within month changes were left out of the review. Furthermore, log review was restricted to the activities performed by the system administrators of IMD.

53. The logs were reviewed on a standalone basis for the new system without considering interfaced systems. Since administrators of the new system are also administrators of a related interfaced system, the review of logs for the new system alone would not generate alerts for any anomaly or conflicting actions performed in the related interfaced system.

54. Logs of changes to user permissions within the new system's sub-modules were not reviewed. No process was established to signoff the reviewed logs (electronically or otherwise) so as to assure their integrity.

55. IMD did not assess and document the logs it required and the logs that were actually available from the system. For example, no logs were available to: (i) track changes in broker commissions/ details; and (ii) track the activity of users on mandatory leave (who could log in through the remote log-in facility of the system).

(ii) User access and the '4-eyes[4] principle'

56. Conflicting roles were assigned to some users. Further, clean-up was required on the user permissions to various sub-modules of the new system. Instances noted during the audit were communicated to IMD for corrective action.

[4] The '4-eyes principle' is a requirement that two individuals approve some action before it can be taken.

57. Several important sub-modules of the new system had their own user permission systems. IMD did not establish a process to assign user permissions to these sub-modules. The need to implement the '4-eyes principle' was not comprehensively evaluated across the new system in accordance with the procedure on managing user access rights, and the regulations of UNJSPF. The '4-eyes principle' was implemented for some functionalities such as Standard Settlement Instructions and investment order approvals but was not enabled for many other modules. Additionally, the '4-eyes principle' was not available in the new system for some other important functionalities such as cancel/correct trade and commissions for which compensatory controls could be put in place.

(iii) Security of IMD FTP site

58. Permissions to the FTP folder which stores the system logs were not adequately assigned. System administrators had full permission to the FTP folder and therefore could modify the logs. IMD subsequently took corrective action to change FTP folder permissions.

59. The integrity of data feeds extracted from the new system and dumped into the IMD FTP folder was not verified as no data validation controls were put in place. The data stored in the FTP folder was not encrypted and was available in plain text which could result in breach of data confidentiality.

(iv) Controls over the payment module

60. IMD had not established any compensating controls to verify the payment messages exchanged through the new system. OIOS shared with IMD the daily validation reports rolled out by payment system as part of its customer security programme to detect unusual payments and minimize the risk of fraud.

(v) Other ICT security issues

61. Incident management and configuration management procedures were not developed with reference to the new system. In absence of same, IMD may be unable to respond in a timely manner to any ICT security incidents relating to the system.

62. System terminals did not have a set time-out procedure and the user could remain logged in for several hours. This weakness could be exploited as IMD had not yet implemented desktop policies to logout users after a defined period of inactivity.

63. Public storage websites such as drop-box and one-drive were accessible from the IMD network, thereby allowing users to upload private organizational data into public cloud. IMD stated that it was evaluating web-filtering solutions to prevent loss of confidential data.

64. IMD laptops were not encrypted. Since the full functionality of the new trade order management system could be accessed directly on these devices, confidential data was at risk in case of theft or loss of these devices.

65. The above-mentioned issues had arisen because IMD did not document and implement a comprehensive ICT security plan for the new system.

(6) IMD should document and implement a comprehensive ICT security plan for the new trade order management system in accordance with its ICT security policy and procedures to address the identified weaknesses.

IMD accepted recommendation 6 and stated that as a top priority it is currently implementing this recommendation to address the weaknesses found. Additionally, IMD is in the process of launching an overall ICT security assessment. The goal is to design a comprehensive information security system. Recommendation 6 remains open pending receipt of evidence that a comprehensive ICT security plan has been implemented for the new trade order management system in accordance with IMD's ICT security policy and procedures.

Requirements for retention of system emails and messages needed to be finalized

66. IMD established a communication and document retention policy in 2011 which applies to all types of electronic communications such as but not limited to electronic mail (email), third parties' messaging mail, instant messaging (IM), social networks and blogs. This policy covers electronic communications for IMD, to or from other United Nations entities, brokers, vendors, or any personal email communications within IMD and social networking sites. The policy required retention of all electronic communications and records for official use for a period of seven years (two years on-site and five years off-site). The policy also requires that all electronic communications will be maintained and monitored by the compliance function through appropriate software programming or sampling of email, as appropriate.

67. The system provider published a document which provides explanation of its electronic communication services and policies. According to this document, all system messages are retained for a period of five years, unless customers have specified a longer retention period by subscribing to its 'vault' service. Alternatively, the system provider allows its customers use its message extraction services.

68. IMD had not finalized its requirements for the retention or extraction of email and IM exchanged on the new system's platform to comply with its communication and retention policy.

69. This condition was due to inadequate planning and resulted in non-compliance with the IMD communication and document retention policy. If not addressed, any information required for compliance review and/or investigation purposes may become unavailable. IMD had initiated an evaluation of its requirements in this regard.

(7) IMD should finalize its requirements for retention of system emails and messaging to ensure compliance with its communication practices and document retention policy.

IMD accepted recommendation 7 and stated that in addition to finalizing its requirements, it started the request to the Procurement Division to add a 'vault' service which will assist with this activity. Recommendation 7 remains open pending receipt of finalized requirements and an implementation plan for ensuring the retention of system emails and messaging in accordance with the communication practices and document retention policy of IMD.

V. ACKNOWLEDGEMENT

70. 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 the new trade order management system in the Investment Management Division of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[5]/ Important[6]	C/ O[7]	Actions needed to close recommendation	Implementation date[8]
1	IMD should: (i) update the business case for the new trade order management system for cost elements and business requirements; (ii) document a benefits review plan; and (iii) update the project risk register for the system.	Important	C	Closed without implementation based on management's acceptance of residual risks.	Not applicable
2	IMD should complete the decommissioning plan for its old trade order management system and the related payment system.	Important	C	Closed without implementation based on management's acceptance of residual risks.	Not applicable
3	IMD, in consultation with the Procurement Division, should include an appropriate clause in future bid documents/contracts for such services to safeguard itself in situations where a cyber security breach and/or severe disruption in the system provider's ICT environment could result in financial loss to the Organization.	Important	C	Closed without implementation based on management's acceptance of residual risks.	Not applicable
4	IMD, based on lessons learned during implementation of phase 1 of the new trade order management system, should strengthen user acceptance testing for phase 2 by: (i) completing user acceptance tests for all processes; (ii) ensuring that workflows are finalized before conducting the tests; (iii) ensuring independent validation of test plans and results; (iv) including ICT security test scenarios in the test plans; and (v) using a test environment for user acceptance testing.	Important	C	Closed without implementation based on management's acceptance of residual risks.	Not applicable

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

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of the new trade order management system in the Investment Management Division of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[5]/ Important[6]	C/ O[7]	Actions needed to close recommendation	Implementation date[8]
5	IMD should: (i) update its user access forms to include additional functions and permissions relating to the new trade order management system; (ii) establish a change control procedure to ensure that brokers classified as 'non-performing/ unsatisfactory' are immediately de-activated in the system; (iii) establish a process to use the system's change management functionality; (iv) evaluate both 'production test' and the 'beta' environments with respect to their functionalities and costs and choose the one best suited to its needs; and (v) set up procedures to manage the 'beta test environment' for testing process changes and rollouts.	Important	O	(i) Receipt of updated IMD user access forms; (ii) establishment of a change control procedure to ensure that brokers classified as non-performing/unsatisfactory are immediately de-activated in the system; (iii) establishment of a process to use the system's change management functionality; (iv) evaluation results for both production test environment and the beta environment; and (v) procedure to manage the 'beta test environment' for testing process changes and rollouts.	31 December 2017
6	IMD should document and implement a comprehensive ICT security plan for the new trade order management system in accordance with its ICT security policy and procedures to address the identified weaknesses.	Important	O	Receipt of evidence that a comprehensive ICT security plan has been implemented for the new trade order management system in accordance with IMD's ICT security policy and procedures.	31 December 2017
7	IMD should finalize its requirements for retention of system emails and messaging to ensure compliance with its communication practices and document retention policy.	Important	O	Receipt of finalized requirements and an implementation plan for ensuring the retention of system emails and messaging in accordance with the communication practices and document retention policy of IMD.	31 December 2018

APPENDIX I

Management Response

UNITED NATIONS NATIONS UNIES

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar 16 March 2017
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: Chief Compliance Officer
Investment Management Division
United Nations Joint Staff Pension Fund

SUBJECT: **Draft report on an audit of the new trade order management system in the**
OBJECT: **Investment Management Division of the United Nations Joint Staff Pension Fund (Assignment No. AT2016/801/02)**

1. Reference is made to your memorandum dated 21 February 2017 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 Annex I to the audit recommendations which details IMD's response to the findings.

3. I wish to thank you and OIOS for the positive interaction with IMD staff during this audit.

cc: Mr. Herman Bril, Director, IMD
Mr. Toru Shindo, Deputy Director, IMD
Mr. Daniel Willey, Chief Compliance Officer and Audit Focal Point, IMD
Mr. Eduardo Hilzinger, Information Systems Officer, IMD
Dr. 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 the new trade order management system 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) update the business case for the new trade order management system for cost elements and business requirements; (ii) document a benefits review plan; and (iii) update the project risk register for the system.	Important	No			IMD takes note. IMD does not see the need or benefit of updating this documentation post-facto. But looking forward, IMD will perform an ex ante study and lessons learned documentation for business cases. Additionally, a consultant firm is assisting IMD with a full ICT target operating model assessment which includes all systems, processes, and ICT risks.
2	IMD should complete the decommissioning plan for its old trade order management system and the related payment system.	Important	No			IMD has fully decommissioned SWIFT Alliance, Charles River and Abacus. ISS in collaboration with IMD users is working on the archiving of this information system data. The archiving is required as per the IMD retention policy (seven years). Given the time and human resources constraints, IMD considered the implementation of Bloomberg AIM had a much higher priority than archiving this data already saved. The archiving activity has already started and expected to be completed in the end of 2017.
3	IMD, in consultation with the Procurement	Important	No			IMD agrees with the importance of

[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 the new trade order management system 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
	Division, should include an appropriate clause in future bid documents/contracts for such services to safeguard itself in situations where a cyber security breach and/or severe disruption in the system provider's ICT environment could result in financial loss to the Organization.					safeguarding against cyber security breaches and/or severe disruptions in the system provider's ICT environment. Therefore, IMD is launching an overall ICT security assessment, which will assess all of IMD's ICT vendors relative to best industry practices. Due to concern that this could delay or prevent contract finalization, we do not accept this recommendation. To the extent possible, IMD will add cyber security/disruption clauses to contracts with service providers.
4	IMD, based on lessons learned during implementation of phase 1 of the new trade order management system, should strengthen user acceptance testing for phase 2 by: (i) completing user acceptance tests for all processes; (ii) ensuring that workflows are finalized before conducting the tests; (iii) ensuring independent validation of test plans and results; (iv) including ICT security test scenarios in the test plans; and (v) using a test environment for user acceptance testing.	Important	No			Recognizing that the audit took place while Bloomberg AIM is being implemented, this recommendation might best be placed under "opportunities for improvement." IMD is continuing to perform UATs. All tests are performed in a testing environment (BETA).
5	IMD should: (i) update its user access forms to include additional functions and permissions relating to the new trade order management system; (ii) establish a change control procedure to ensure that brokers classified as 'non-performing/	Important	Yes	COO and Deputy-Director for Investments (item ii)	December 2017	IMD has included these tasks in the phase 2 of Bloomberg AIM implementation. IMD recently updated its user access forms to include additional functions and permissions relating to the new trade

APPENDIX I

Management Response

Audit of the new trade order management system 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
	unsatisfactory' are immediately de-activated in the system; (iii) establish a process to use the system's change management functionality; (iv) evaluate both 'production test' and the 'beta' environments with respect to their functionalities and costs and choose the one best suited to its needs; and (v) set up procedures to manage the 'beta test environment' for testing process changes and rollouts.					order management system. The item (ii) is under the Investment Section. Any other procedures will be revised under the ICT Strategy study, or also known as Target Operating Model Assessment.
6	IMD should document and implement a comprehensive ICT security plan for the new trade order management system in accordance with its ICT security policy and procedures to address the identified weaknesses.	Important	Yes	COO	December 2017	As a top priority IMD is currently implementing this recommendation to address the weaknesses found. Additionally, IMD is in the process of launching an overall ICT security assessment which will include the assessment of all external ICT provider (including Bloomberg). The goal is to design a comprehensive information security system. IMD will review and test these controls whilst re-assessing its information security and building a stronger information security system.
7	IMD should finalize its requirements for retention of system emails and messaging to ensure compliance with its communication practices and document retention policy.	Important	Yes	COO	December 2018	In addition to finalizing the requirements, IMD started the request to UN Procurement Division to add a Bloomberg Service, i.e. Bloomberg Vault which will assist with this activity.