INTERNAL AUDIT DIVISION

REPORT 2015/057

Audit of the Omgeo system in the Investment Management Division of the United Nations Joint Staff Pension Fund

Overall results relating to the effective and efficient management of the Omgeo system were initially assessed as partially satisfactory. Implementation of three important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

22 June 2015
Assignment No. AT2014/800/03

CONTENTS

AUDIT REPORT

Audit of the Omgeo 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 Omgeo system in the Investment Management Division (IMD) of the United Nations Joint Staff Pension Fund (UNJSPF).

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. 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.

4. ISS provides support for business applications and some infrastructure services for IMD users.

5. Omgeo is a software system that supports the automated management of trade matching. According to the budget performance report of 2012-2013, IMD allocated $100,000 for the implementation of Omgeo with a reported expenditure of $86,200.

6. Omgeo consisted of the following separate components:

(i) Omgeo-CTM, which supported the management of global equities and fixed income securities;

(ii) Omgeo-OASYS, which supported the management of domestic equities and fixed income securities; and

(iii) Omgeo Network, which was the central hub provided by the vendor to connect brokers and investment offices.

7. Omgeo-CTM operated as an internal module in the trade order management process managed with the Charles River system. Omgeo-OASYS was a stand-alone system interfaced with Charles River. Omgeo-CTM and Omgeo-OASYS communicated with the Omgeo Network separately.

8. Charles River was the trade order management system used by IMD for order management, execution, allocation and trade processing.

9. Trade matching is a stage in the straight through processing of a trade, during which details of a submitted trade order (i.e., quantity, price, broker data, and security type) are matched against the information confirmed by the broker. When a match is established, the trade automatically flows to the next phase of its execution. When there is a mismatch in the values provided, the front office addresses the cause of the mismatch to proceed with the next phase. Before the implementation of Omgeo, IMD performed trade matching manually using faxes and emails. This process, however, exposed IMD to risks

associated with potential mistakes deriving from the manual matching (described as failed trades) associated with penalties and charges. To address these risks and enable a straight through processing of trades, IMD decided to implement the Omgeo system, which automatically connects and communicates trade and allocation details to external brokers.

10. Implementation of the Omgeo project started in 2012 and included three main activities:

(i) Amending the workflow of the front and back offices to include electronic trade confirmation affirmation;

(ii) Configuring the trade order management system Charles River to interface with Omgeo-CTM and Omgeo-OASYS, including the corresponding workflow; and

(iii) Establishing a secure communication link between Charles River and Omgeo.

11. The project initiation document included the following key benefits expected from the implementation of Omgeo:

(i) Creation of a single reference point for the trade blotter data across all IMD sections;

(ii) Automation of tolerance checking and maintenance of routing rules allowing staff to focus on key risks and reducing errors of manual processing;

(iii) Fast forwarding of the trade settlement with real-time routing, instead of traditional end-of-day processing;

(iv) Reduction of risks and costs through an early detection of errors and failed trades; and

(v) Centralization of post-trade activities with the Charles River integration.

12. IMD adopted the information and communications technology (ICT) project management methodology PRINCE II (i.e., Projects in Controlled Environments) for the implementation of Omgeo.

13. Comments provided by IMD are incorporated in italics.

II. OBJECTIVE AND SCOPE

14. The audit was conducted to assess the adequacy and effectiveness of IMD governance, risk management and control processes in providing reasonable assurance regarding **the effective and efficient management of the Omgeo system**.

15. This audit was included in the OIOS work plan for 2014 in view of the high risks associated with the Omgeo system.

16. The key controls tested for the audit were: (a) project management; (b) change management; and (c) ICT support systems. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Project management –** controls that provide reasonable assurance that there is sufficient ICT project management capacity to support the implementation and support of the Omgeo system;

(b) **Change management –** controls that provide reasonable assurance that there is a systematic approach to dealing with changes and issues associated with the implementation of Omgeo; and

(c) **ICT support systems –** controls that provide reasonable assurance that the Omgeo system addresses the operational needs of IMD in an efficient, effective and secure manner.

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

18. OIOS conducted this audit from December 2014 to March 2015. The audit covered the period from June 2014 to January 2015.

19. 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 assess their effectiveness. In particular, OIOS: (a) analyzed project documents; (b) interviewed responsible staff; (c) conducted walkthroughs of Omgeo processes and procedures; (d) tested the effectiveness of, project management, system development, system analysis, design and testing; and (e) tested the user access and back-end security controls.

III. AUDIT RESULTS

20. The IMD governance, risk management and control processes examined were initially assessed as **partially satisfactory**[1] in providing reasonable assurance regarding the **effective and efficient management of the Omgeo system.**

21. OIOS made three audit recommendations to address issues identified in the audit. IMD implemented some good controls for project management, user training and technical documentation. However, there were control weaknesses in the preparation of the business case, change management procedures and ICT strategic plans.

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

[1] A rating of **"partially satisfactory"** means that important (but not critical or pervasive) deficiencies exist in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	**Accurate financial and operational reporting**	**Safeguarding of assets**	**Compliance with policies, mandates, regulations and rules**
Effective and efficient management of the Omgeo system	(a) Project management	Partially satisfactory	Satisfactory	Partially satisfactory	Partially satisfactory
	(b) Change management	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(c) ICT support systems	Satisfactory	Satisfactory	Satisfactory	Satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Project management

Inadequate business case

23. PRINCE II defines 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. A business case should be documented to describe the reasons, options, expected benefits, time, costs and major risks of a project. It should be used to judge whether the project remains desirable, viable and achievable.

24. In June 2012, IMD prepared a project initiation document and project plan which described the project objectives, expected key benefits, completion date, project organization and risks. However, the following weaknesses were identified in the project initiation phase:

(i) IMD did not document the justification behind the selection of Omgeo to automate the matching process. IMD explained that informal research was performed and the results showed that Omgeo was the most commonly used trade matching platform among the brokers community. However, an adequate study was not conducted to compare it with alternative options available in the market in terms of costs, coverage of security types managed, and number of brokers automatically connected to the Omgeo system.

(ii) The expected total cost of the project was not established at the beginning of the project. Software licences and service fees, and costs related to hardware, project implementation (internal resources and vendors), ongoing operations and maintenance as well as their funding arrangements were not documented as part of the project planning and business case preparation. In December 2012, IMD prepared a high level expenditure report which included only the cost of internal staff and some external fees related to the system integrators (i.e., Charles River and Omgeo). This report was not in alignment with the relevant purchase orders and did not include enough details.

(iii) The Omgeo business case did not contain an assessment of the potential impact of other ICT projects and organizational changes (i.e., creation of a Middle Office) being implemented in IMD. For example, impacts pertaining to the implementation of a major project such as Bloomberg AIM - which will replace the existing trading platform

(Charles River) in IMD - was not assessed and documented. Similarly, the impact of delays in the establishment of a Middle Office was not assessed as part of the Omgeo business case.

25. The lack of a business case prevented IMD from having a documented justification of the proposed solution, supported by a cost-benefit analysis, and its impact on the existing ICT portfolio and projects. This could lead to the implementation of inefficient and uneconomical ICT solutions.

(1) IMD should develop a business case template to be used for current and future ICT projects and initiatives requiring: (i) justification of proposed solution; (ii) cost-benefit analysis with estimated project cost; and (iii) impact to the current ICT portfolio and projects.

IMD accepted recommendation 1 and stated that as recommended by the IMD ICT Steering Committee, the IMD business case template for ICT projects is pending approval by the RSG. The IMD business case template applies to the on-going IMD projects as well as future projects. IMD shall provide OIOS with the copy of the instructions from IMD management to project managers. Recommendation 1 remains open pending receipt of the business case template approved by the RSG and instructions to project managers to update the business cases of ongoing projects using the new business case template.

Project management controls

26. PRINCE II requires project management controls for planning, delegating, monitoring and controlling all aspects of projects to achieve the objectives within expected timelines and targets for time, costs, quality, scope, benefits and risks.

27. Initially, several aspects of the Omgeo project had not been adequately managed, resulting in two years delay in completion of the project. The following weaknesses were identified in the practices followed during the implementation of the Omgeo project from June 2012 to October 2014:

(i) Project roles and responsibilities were not adequately assigned;

(ii) The total cost of the implementation of the Omgeo project was not estimated and monitored. Software licences and service fees, hardware requirements, implementation costs (internal resources and vendors), ongoing operations and maintenance costs were not documented as part of the project planning and business case preparation;

(iii) The business case was not reviewed and updated during the project;

(iv) Although an issue register was created, project issues were not adequately logged and escalated to IMD management; and

28. The technical implementation of the Omgeo project was completed as planned in December 2012. The system was successfully moved to production environment with four brokers instead of the initially identified 180 brokers. IMD continued to operate Omgeo with this limited capacity from December 2012 to December 2014. The reason for this limited usage (i.e. suspension of full coverage) was reported as the lack of middle office resources to operate Omgeo.

29. In October 2014, IMD started a new phase (second phase) of implementation of Omgeo and documented a lessons learned report of the project and decided to configure the system with all 180 brokers as initially planned. During this new phase:

(i) IMD prepared a new project initiation document;

(ii) Established a new project board and assigned the project roles and responsibilities,

(iii) Monitored the progress of the project, risk and issues through periodic status reports.

30. IMD completed the configuration of the system in accordance with the revised project plan following PRINCE II practices. In view of the actions already taken during this phase of the project, OIOS did not make any recommendations in this area.

Project risks

31. PRINCE II requires the establishment of a formal project risk management process to identify, analyze, respond, mitigate and monitor the risks of the project.

32. Although, during the project initiation phase, IMD documented its project risk management strategy, created a risk register and assessed the risks of Omgeo, adequate mitigating controls were not implemented as expected. However, during the second phase of the implementation (started in October 2014), IMD monitored risks periodically and started to implement adequate mitigating controls. Several project risks were beyond the scope of Omgeo and, therefore, had been appropriately escalated to the ICT Steering Committee of IMD (i.e., Omgeo full disaster recovery implementation; expiration of Charles River support; and emergency changes to the system after Murex decommissioning) for management decision. Given the actions taken by IMD, OIOS did not make recommendations in this area.

Adequate data verification and testing

33. The control practices recommended by the industry standard “Control Objectives for Information and Related Technology” (COBIT), require testing the functionalities of ICT systems and their interoperability with existing applications and infrastructure, to verify the efficiency of system performance and the integrity of data.

34. IMD followed adequate practices during the test phase including:

(i) Documenting test scenarios;

(ii) Testing data samples;

(iii) Establishing separate production and test environments;

(iv) Logging and managing issues identified during the testing; and

(v) Documenting the user acceptance sign-off completed with senior users.

35. OIOS therefore concluded that the data verification and testing processes were satisfactorily performed.

Adequate user training and technical documentation

36. COBIT requires the transfer of adequate knowledge and skills to enable end-users to effectively and efficiently use the system with the support of instructions, training materials and technical documentation.

37. IMD documented training material for Omgeo-CTM and Omgeo-OASYS and trained end-users. Additionally, detailed technical documentation for the administration and configuration of the system was prepared. Therefore, OIOS concluded that user training and technical documentation were adequately performed.

Adequate project closure

38. PRINCE II requires projects to be completed on the basis of activities that include closure of issues, maintenance of a risk register and a log of lessons learned.

39. IMD documented an end-project report including:

(i) Descriptions of project deliverables;

(ii) Results, accomplishments, benefits and changes in the business work flow;

(iii) Escalation of issues and risks; and

(iv) Lessons learned.

40. In view of the actions taken by IMD, OIOS concluded that the project closure was adequately documented.

B. Change management

Inadequate change management procedures for emergency changes

41. COBIT requires that any proposed change to ICT systems should be supported by an assessment of the impact on other ICT systems and applications. Changes should be formally managed, including those related to emergency maintenance tasks affecting the infrastructure and applications within the production environment.

42. IMD established adequate procedures for managing changes to Omgeo with requirements for approving modifications to master data, including:

(i) Broker registration forms were used to add new brokers in Omgeo;

(ii) User request/change control forms were adopted to manage changes associated to system configurations related to fixed income matching profile forms, currency tolerance lists, and settlement currency lists; and

(iii) User registration forms were used to grant/revoke user access to Omgeo.

43. However, IMD used multiple systems to automate the life-cycle of trades (i.e., Charles River, Omgeo, SWIFT, Murex, etc.). These systems were either directly integrated or depended on each other to support the data and work flows of IMD operations. However, IMD did not have a change management procedure to manage the impact of emergency changes to its ICT systems. The consequences of this condition were evident during the recent decommissioning of the Murex system when IMD implemented emergency changes to its operations (i.e., changes implemented on Charles River) and invoked its business continuity plan. During the implementation of this emergency change, the unavailability of Omgeo system was reported as an incident.

44. This condition was due to the absence of emergency change management procedures which prevented IMD from identifying the dependencies and impact of changes between ICT systems, and may expose to the systems to malfunctions, business disruptions and inefficiencies.

(2) IMD should implement a comprehensive change management procedure to address normal and emergency conditions which includes an assessment of the impact of changes on other ICT systems.

IMD accepted recommendation 2 and stated that the procedure will be developed as recommended. It will be submitted to the IMD ICT Steering Committee for review and approval. The target date for implementation is 31 August 2015. Recommendation 2 remains open pending receipt of the approved change management procedure with an assessment of the impact of changes on other ICT systems.

Absence of ICT alignment and strategic plan

45. COBIT requires alignment between business and ICT strategic plans and an assessment of current and future needs. This alignment should take into consideration the current ICT capabilities and the business objectives defined for the medium and long term periods.

46. IMD had not conducted an assessment of its current and future business requirements and did not document an ICT strategic plan to achieve these requirements. IMD was in the process of making several changes in its ICT landscape with the decommissioning of Murex and the replacement of Charles River system with the Bloomberg AIM that will both impact the configuration and operations of Omgeo.

47. The IMD ICT Steering Committee recently decided and proposed to engage subject matter experts for each line of business to work in conjunction with IMD representatives for the study of its ICT systems and roadmap. At the time of this audit, however, this activity was not yet started.

48. This condition was caused by the misaligned and outdated ICT strategic plans which may prevent IMD from achieving the expected value and benefits of its ICT investments.

(3) IMD should update its ICT strategy and roadmap with the definition of the future desired status of its ICT landscape.

IMD accepted recommendation 3 and stated that ISS will prepare an ICT strategic proposal which will be submitted to the IMD ICT Steering Committee for review and approval by 31 December 2015. Recommendation 3 remains open pending receipt of the strategic proposal documenting the alignment of ICT systems with core business processes, an estimate of future ICT requirements, and the future desired status of the IMD ICT landscape.

C. ICT support systems

Incomplete disaster recovery infrastructure and planning

49. 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 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.

50. Two of three components of the Omgeo system were under the control of IMD (Omgeo administered its own network hub). However, while IMD implemented the disaster recovery instance and test of Omgeo-CTM in the data centre of the United Nations International Computing Centre (UNICC) located in Geneva, it did not have a disaster recovery instance for Omgeo OASYS. IMD documented its hardware and software configuration, network requirements and proposed architecture for the implementation of Omgeo disaster recovery instances in Geneva and proposed the solution to the ICT Steering Committee. The ICT Steering Committee approved the proposed implementation in February 2015. Accordingly, the change request for the implementation of the full disaster recovery solution was sent to UNICC.

51. The IMD disaster recovery and business continuity plan did not include specific instructions related to the Omgeo system. Additionally, the backup schedule of Omgeo-OASYS was not documented. OIOS already addressed this control weakness in the 2015 audit of ICT strategic planning, governance and management in IMD. Given that IMD has been addressing the recommendation that was issued by this audit, no further recommendations were made in this area.

Application access controls were generally adequate

52. The control best practices recommended by the international standard for ICT security management (ISO-27001) adopted by UNJSPF, require that access to systems and applications should be controlled by a secure log-on procedure and strong passwords.

53. The following access controls were configured and implemented in Omgeo-CTM:

(i) The application was accessed through uniquely assigned user accounts;

(ii) Access to the application access was restricted to five users with granular role assignments;

(iii) Strong passwords were enforced;

(iv) Multiple unsuccessful login attempts caused the lockdown of user accounts;

(v) User accounts that were not used for 90 days were automatically locked; and

(vi) User account audit logs were stored by the service provider and were available upon request of IMD.

54. However, there was one Omgeo-CTM service system account for which the password was stored in clear text in a system configuration file. Audit tests showed that this account could not be used to

access any user interface. OIOS assessed this risk as low because only the Omgeo administrator had access to this configuration file and there was continuous monitoring of the system. Therefore, OIOS did not make a recommendation in this area.

Inadequate access request forms

55. The control best practices issued in the international standard for ICT security management (ISO-27001) require that users should be provided access only to systems that they have been specifically authorized to use.

56. OIOS reviewed the access request forms of users having access to Omgeo and noted that an access request form was not signed and authorized for one user with the role of system administrator. This role provided him with privileged access to the Omgeo system, allowing: (i) changes to Omgeo system parameters; (ii) update of broker accounts settlement instructions, bank identifier code, and post trading rules; and (iii) shut down of the trade gateway and the engine of the financial information exchange protocol.

57. In response to the results of this audit, IMD amended the access request forms and revoked the access granted to the user who was not authorized to have the role of system administrator. Therefore, OIOS did not make any recommendation in this area.

IV. ACKNOWLEDGEMENT

58. 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 the Omgeo system in the Investment Management Division of the United Nations Joint Staff Pension Fund

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	IMD should develop a business case template to be used for current and future ICT projects and initiatives requiring: (i) justification of proposed solution; (ii) cost-benefit analysis with estimated project cost; and (iii) impact to the current ICT portfolio and projects.	Important	O	Provide copy of the business case template approved by the RSG and the instructions issued to project managers to update the business cases of ongoing projects using the new business case template.	30 June 2015
2	IMD should implement a comprehensive change management procedure to address normal and emergency conditions which includes an assessment of the impact of changes on other ICT systems.	Important	O	Provide copy of the approved change management procedure with an assessment of the impact of changes on other ICT systems.	31 August 2015
3	IMD should update its ICT strategy and roadmap with the definition of the future desired status of its ICT landscape.	Important	O	Provide copy of strategic proposal documenting the alignment of ICT systems with core business processes, an estimate of future ICT requirements, and the future desired status of IMD ICT landscape.	31 December 2015

[2] 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.
[3] 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.
[4] C = closed, O = open
[5] Date provided by IMD in response to recommendations.

APPENDIX I

Management Response

UNITED NATIONS | NATIONS UNIES

INTEROFFICE MEMORANDUM | MEMORANDUM INTERIEUR

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

01 June 2015

THROUGH: Daniel Willey / Daniel Willey 5 June 2015
PAR:

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

5 June 2015

SUBJECT: **Draft report on an audit of the OMGEO system in the Investment Management**
OBJECT: **Division of the United Nations Joint Staff Pension Fund (Assignment No. AT2014/800/03)**

1. Reference is made to your memorandum dated 21 May 2015 providing the report on the above-mentioned audit.

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

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

cc: Mr. Ajit Singh, Deputy Director Risk and Compliance, IMD
Mr. Daniel Willey, Compliance Officer and Audit Focal Point, IMD
Dr. Kamel Kessaci, Senior Information Systems Officer, IMD
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS
Ms. Wasantha Jayasinghe, Senior Compliance Assistant, IMD
Ms. Stara Khan, Senior Risk Assistant, IMD

APPENDIX I

Management Response

Audit of the Omgeo 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 develop a business case template to be used for current and future ICT projects and initiatives requiring: (i) justification of proposed solution; (ii) cost-benefit analysis with estimated project cost; and (iii) impact to the current ICT portfolio and projects.	Important	Yes	TBD	30 June, 2015	As recommended by the IMD ICT Steering Committee, the IMD business case template for ICT projects is pending for approval by the RSG. As recommended by OIOS, the IMD business case template applies to the on-going IMD projects as well as future projects. IMD shall provide OIOS with the copy of the instruction from IMD management to project managers.
2	IMD should implement a comprehensive change management procedure to address normal and emergency conditions which includes an assessment of the impact of changes on other ICT systems.	Important	Yes	TBD	31 August, 2015	The procedure will be developed as recommended. It will be submitted to the IMD ICT Steering Committee for review and approval. The target date to implement this recommendation is 31 August 2015.
3	IMD should update its ICT strategy and roadmap with the definition of the future desired status of its ICT landscape.	Important	Yes	TBD	31 December, 2015	ISS will prepare an ICT strategic proposal which will be submitted to the IMD ICT Steering Committee for review and approval. The target date to implement this recommendation is 31 December 2015.

[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.