



INTERNAL AUDIT DIVISION

AUDIT REPORT

Audit of the Riskmetrics system in the Investment Management Division of UNJSPF

**Overall results relating to the effective
implementation of the Riskmetrics system
were initially assessed as satisfactory**

FINAL OVERALL RATING: SATISFACTORY

26 July 2012

Assignment No. AT2011/801/01

CONTENTS

	<i>Page</i>
I. BACKGROUND	1
II. OBJECTIVE AND SCOPE	2-3
III. AUDIT RESULTS	2-6
A. Project management	3-4
B. ICT support systems	4-6
IV. ACKNOWLEDGEMENT	6
APPENDIX 1 Management response	

AUDIT REPORT

Audit of the Riskmetrics system in the Investment Management Division of UNJSPF

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the Riskmetrics 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. In the past, IMD lacked relevant and reliable tools to effectively monitor its investment portfolios and attribute performance, as well as understand the sources of risk and how they impact the portfolio's performance. The Risk/Compliance Officer used to monitor the asset allocation against the approved instructions. Investment officers used Excel spreadsheets to calculate impact on their respective regional portfolios, and risk reports were obtained from the master record keeper Northern Trust.
4. In March 2010, to address the limitations of the previous approach, IMD acquired a portfolio risk analysis and performance attribution from the company Riskmetrics (developer of the Riskmetrics system). After the contract was signed, Riskmetrics merged with Morgan Stanley Capital International (MSCI).
5. The Riskmetrics system is composed of two modules (Risk Manager, and Performance Manager for Equity and Fixed Income) and generates daily absolute and relative risk reports, allowing the investment officers to review the risk-adjusted performance of equity and bond portfolios in relation to the respective benchmarks.
6. The Riskmetrics system is provided by MSCI as a managed service. The software is physically hosted by MSCI in its data centre and it is accessed remotely by IMD via secure connection. IMD transmits on a daily basis to MSCI a position file containing the list of its holdings. MSCI uploads the position file sent by IMD into Riskmetrics. Based on MSCI proprietary market data and algorithms, risk assessment reports are generated in Riskmetrics. IMD accesses Riskmetrics via Internet for viewing/downloading the risk reports or simulating potential risk scenarios and their impact on its holdings.
7. IMD had completed the testing of the Risk Manager module, which was released into production in October 2011.
8. As a result of the merger between Riskmetrics and MSCI, the release of the Performance Manager module for Equity and Fixed Income was delayed. IMD completed the test of the Performance Manager module for Equity. Testing of the Performance Manager for Fixed Income is still in progress and is expected to be released into production by December 2012.

9. The total price of the software acquisition was \$3,802,000, of which \$3,352,000 was for software license fees and \$450,000 for implementation fees. The total expenditure incurred by IMD as of December 2011 was \$693,333.

II. OBJECTIVE AND SCOPE

10. The audit was conducted to assess the adequacy and effectiveness of IMD's governance, risk management and control processes in providing reasonable assurance regarding **effective implementation of the Riskmetrics system**.

11. This audit was selected because of the potential risks to which IMD would be exposed as a consequence of ineffective implementation of the Riskmetrics system supporting the risk management function.

12. The key controls tested for the audit were: (a) project management; and (b) information and communications technology (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 project management capacity deployed to achieve the objectives defined by IMD with the acquisition of Riskmetrics, including: (a) adequate financial resources; (b) adequate and competent human resources; and (c) appropriate project management tools, methodology and systems; and

(b) **ICT support systems** - controls that provide reasonable assurance that Riskmetrics supports the risk management function and delivers the intended benefits to IMD.

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

14. OIOS conducted this audit from 15 November 2011 to 8 May 2012. The audit covered the period from 1 January 2010 to 30 April 2012.

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

III. AUDIT RESULTS

16. In OIOS' opinion, IMD's governance, risk management and control processes were **satisfactory** in providing reasonable assurance regarding the **effective implementation of the Riskmetrics system**.

17. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **satisfactory**.

Table 1: Assessment of key controls

Business objective(s)	Key controls	Control objectives			
		Efficient and effective operations	Accurate financial and operational reporting	Safeguarding of assets	Compliance with mandates, regulations and rules
Effective implementation of the Riskmetrics system	(a) Project management	Satisfactory	Satisfactory	Satisfactory	Satisfactory
	(b) ICT support systems	Satisfactory	Satisfactory	Satisfactory	Satisfactory
FINAL OVERALL RATING: SATISFACTORY					

A. Project management

Statement of work

18. IMD defined its requirements for a portfolio risk analysis and performance attribution system. The terms of reference were adequate and based on detailed functional and technical requirements, computing environment and corresponding functions.

Contract management

19. The contract included specific provisions for MSCI to manage the technology, data and analytics used to produce and deliver risk and performance reports, and ensure constant monitoring and quality control on the basis of a service level agreement. In accordance with the contract, IMD in collaboration with MSCI developed a project plan, service level agreement and operating documents with specifications for the implementation and use of the Riskmetrics system.

20. OIOS reviewed the system, project documents and reports, and also interviewed both technical staff and end-users. The results confirmed the adequacy of the mechanisms implemented for: (i) the security of data transmission; (ii) the use of the required file types and structure; (iii) naming conventions; (iv) workflows; (v) reporting services; (vi) customizations; and (vii) scoping, testing and processing the services.

21. OIOS also reviewed the payments made by IMD to MSCI, and confirmed that they were appropriate.

Assignment of roles and responsibilities

22. In accordance with the terms of the contract, IMD and MSCI developed a service specification document for the implementation of the Riskmetrics system, with detailed definition of the roles and responsibilities of each party.

23. OIOS reviewed the service specification document, weekly meeting notes and issue log maintained by IMD. Tasks performed by IMD and MSCI during the period March 2010 – March 2012 were in accordance with the roles and responsibilities defined in the service specification document.

Service level agreement and specifications

24. A service level agreement between IMD and MSCI was detailed in the contract. In addition, details pertaining to the managed services had been defined in a service specification document developed by IMD and MSCI in accordance with the terms of the contract.

25. OIOS reviewed the service specification document in conjunction with the project plan and the issue log developed by IMD for monitoring the implementation of the Riskmetrics system. This log included details of the issues identified, resolved and tested during the course of the contract execution.

26. All the services defined in the service level agreement for the Risk Manager module were adequately configured and implemented in accordance with the terms of the contract. The following controls were in place: (i) automated and documented scripts for the transmission of the position file; (ii) an hierarchy structure documented the details of asset class, regions, markets, country portfolios and benchmarks; (iii) monitoring procedures and responsibilities for the review of the file logging Riskmetrics transactions; and (iv) exceptions were verified and resolved with MSCI.

Change management procedures

27. The contract provided IMD the right to obtain all enhancements, modifications, extensions and other changes to the software system. Terms of reference for requesting changes and customizations to the reports were defined in the service specification document.

28. Requests for changes followed the terms of reference for managing changes. Most these changes pertained to report customizations requested by IMD.

Training

29. IMD staff was trained on the use of the Riskmetrics system by MSCI. Training sessions were adequately delivered through hands-on simulations of the system's functionalities. In addition, IMD staff confirmed their positive assessment of the training and support received from MSCI.

B. ICT support systems

Reports

30. IMD officers provided positive feedback and assessments on the quality of the Riskmetrics reports and stated that, with increased amount of users, the system could provide significant benefits to their daily analysis.

Simulation and testing

31. Testing conducted by IMD was adequately documented and performed. Acceptance tests were organized by the Risk Management Office with the Director and the Portfolio Managers of IMD. The tests were supported by an issue log complete with all relevant details, including weekly status report logs of project implementation.

32. As of March 2012, IMD completed the tests and sign-off sessions with the Director and Portfolio Managers of IMD for the acceptance of Risk Manager and Performance Manager for Equity.

Security mechanisms for generation/transmission of the position file and access to Riskmetrics

33. OIOS reviewed the policies, procedures and technical configurations established by IMD for controlling the generation and transmission of the position files and access to Riskmetrics.

34. IMD has a general policy regulating staff access to systems and compliance procedures, although the policy was not dated and did not indicate a version number.

35. The position files transmitted by IMD to MSCI were based on the file provided daily by the global custodian Northern Trust. This process was adequately controlled on the basis of the following mechanisms in place: (i) use of secure transfer protocols (SFTP); (ii) limited and controlled access granted to the IMD/IT staff to the file and hosting servers for performing the actions associated with this function; (iii) pre-identification and configuration of the computers (gateways) from which IMD staff can access Riskmetrics; (iv) remote access allowed only through secure connection to IMD servers; and (v) access to the Riskmetrics system limited to read-only and/or simulations of risk scenarios that do not alter the composition of the original position file. The current list of users authorized to access the Riskmetrics system was adequately controlled.

Logging and audit trails

36. The processing of the position file uploaded in Riskmetrics was logged. The logs contained a limited number of exception cases associated with positions that did not fully map with those defined in the Riskmetrics model. Logs were reviewed by IMD on a daily basis for monitoring and reconciliation; and exception cases were explained and addressed with MSCI.

37. "Process summary log records" recorded the success and/or failure of the report production processes and additional statistics summarizing the automated workflow processing. The content of these records was adequate and did not show any critical issues. Access to the log file was controlled and limited to the Senior Compliance Assistant.

Security mechanisms to ensure the confidentiality, integrity and availability of data

38. According to the terms of the contract, MSCI has full responsibility for hosting and managing the technical infrastructure processing and storing IMD data. OIOS conducted a physical inspection of this technical infrastructure and checked the controls pertaining to physical security, servers siting and connection, power supply, cooling mechanisms, fire suppression, and backup and continuity.

39. The MSCI data centre was protected with adequate control mechanisms in accordance with professional industry standards. The data centre was protected by armed guards constantly on-site. Server racks were segregated and isolated in separate zones and metal cages. Electrical power was adequate and redundant, with guaranteed 100% uptime. The facility was equipped with the required support of uninterruptible power supply devices and environmental controls (i.e. temperature, humidity and fire suppression). Each section of the data centre was isolated and had dedicated cooling inlets.

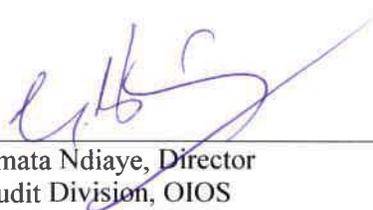
40. However, in the area of business continuity and disaster recovery, although the primary data centre was supported by a redundant site (secondary data centre), the two locations were only 40 miles apart. This condition potentially exposes MSCI and IMD to the risk of losing data in case of a disastrous event extending to both locations simultaneously. MSCI indicated that while they have a processing facility in Switzerland, data was not yet replicated to this site for business continuity and disaster recovery purposes.

41. In OIOS' opinion, given that IMD is using the Riskmetrics system only for risk analysis and reporting purposes, the potential unavailability of the service from MSCI would not have a significant impact on its critical operations.

42. In addition, a SAS 70 examination (step II) report issued by Deloitte & Touche LLP on MSCI operations as of 31 December 2010 (a similar report for 2011 was being finalized) provided additional assurance with regard to internal controls implemented by MSCI for restricting logical access to operating systems, databases and applications to authorized personnel, and ensuring that programs and modifications to production systems are tested prior to their implementation.

IV. ACKNOWLEDGEMENT

43. 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.



Ms. Fatoumata Ndiaye, Director
Internal Audit Division, OIOS