

**FOR
INFORMATION**

EBAP/15/49

June 4, 2015

To: Members of the Executive Board
From: The Secretary
Subject: **Office of Internal Audit and Inspection—FY 2015 Activity Report**

Board Action: Executive Directors' **information**

Publication: No (this paper is intended for the use of the Executive Board only).

Additional Information: Ahead of the visit of the External Audit Committee, OIA will be available in the Board Committee room on June 9, 2015 to answer questions on this Activity Report, particularly the recently posted audits/reviews completed in FY 2015.

Questions: Ms. Brady, OIA (ext. 39532)



OFFICE OF INTERNAL AUDIT FY 2015 ACTIVITY REPORT

June 3, 2015

EXECUTIVE SUMMARY

This report, which provides an overview of OIA's activities in FY 2015, fulfills management's commitment to keep the Executive Board regularly informed on control and audit related items.

In FY 2015, OIA completed 12 assurance and advisory engagements (audits and reviews), and prepared the 2014 Report on Risk Management issued by the Advisory Committee on Risk Management (ACRM). Ten of these engagements assessed the adequacy of controls and procedures in order to mitigate risks to the achievement of the Fund's institutional and departmental goals. OIA also completed two additional internal projects: a review of OIA's annual planning methodology, to align it with leading practices; and a review of OIA's recommendation follow-up process, to improve OIA's root cause analysis, follow-up and escalation process.

Also, as approved by the Executive Board, OIA produced its first, and the Fund's sixth, Periodic Monitoring Report (PMR). The PMR assessed the extent to which Board-endorsed IEO recommendations have either been implemented or are in progress. The report was issued and discussed in July 2014.

Approved By
Clare Brady

Prepared by the Office of Internal Audit and Inspection

CONTENTS

| | |
|--|----------|
| INTRODUCTION | 3 |
| OFFICE OF INTERNAL AUDIT AND INSPECTION (OIA) | 3 |
| A. Mandate | 3 |
| SUMMARY OF FY 2015 ENGAGEMENT RESULTS | 3 |
| OIA INTERNAL PROJECTS | 6 |
| STATUS OF FY 2015 WORK PLAN | 7 |
| A. Audits and Reviews | 7 |
| B. Risk Management | 7 |
| C. Periodic Monitoring Report (PMR) | 7 |
| ADMINISTRATIVE MATTERS | 7 |
| TABLE | |
| 1. OIA's Work Plan, FY 2015 | 8 |

INTRODUCTION

1. **This report fulfills the Managing Director’s commitment to regularly share information with the Board on control and audit related matters, and provides an overview of OIA’s activities in FY 2015.** The report includes the results of FY 2015 assurance and advisory engagements (audits and reviews), an overview of two internal projects, and the status of the FY 2015 work plan.
2. **On June 9, 2015, a question and answer (Q&A) session with OIA is scheduled for Executive Directors and their offices.** This session will help Executive Directors to prepare for the upcoming visit of the External Audit Committee (EAC) by providing an opportunity to discuss the results of FY 2015 work with the OIA team.

OFFICE OF INTERNAL AUDIT AND INSPECTION (OIA)

A. Mandate

3. **OIA is an independent and objective assurance and advisory function that adds value to the Fund by improving its operations.** OIA assists the Fund in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organization’s governance, risk management, and internal control process. OIA’s work is carried out in accordance with the Institute of Internal Auditors’ (IIA) International Professional Practices Framework (IPPF). In line with leading practices, OIA reports to Fund management, and its activities are overseen by the EAC, thus ensuring its objectivity and independence. OIA’s authority and responsibility are defined in the General Administrative Order (GAO) No. 14 and Executive Board Decision, DEC/14892-(11/41).

SUMMARY OF FY 2015 ENGAGEMENT RESULTS

4. The scope of the **Audit of the Investment Account (IA)** included: oversight of the work of FIN and the IA’s asset custodian and external managers; the conflict of interest framework; the monitoring of the IA managers’ compliance with the Fund’s investment guidelines; the reporting of the performance and risks to the Investment Oversight Committee and the Board; and risk mitigation measures in place to protect Fund assets, including information assets, and to segregate access to information and systems. Overall, OIA found that the controls supporting IA operations are well designed and operating effectively.
5. The **Audit of the Financial Transactions Related to the HQ1 Renewal Project** assessed the operating effectiveness of budgetary and financial controls supporting the HQ1 renewal program. In designing controls for the renovation, the HQ1 renewal project team established a low tolerance for cost and schedule overruns and assessed financial risks as high. The audit found that the controls supporting financial and budget administration for the HQ1 renewal program are operating effectively. However, the project has encountered challenges that require continued

vigilance with respect to the schedule and the budget for the remainder of the project. The audit made recommendations to help the project management team minimize cost uncertainties (associated with amendments to the construction contract), and to promote the effective use of schedule management tools.

6. The scope of the **Audit of the Administration of Salaries and Benefits** covered the salaries and benefits of Fund employees (including contractual employees and long-term experts), and employees of the IEO and OEDs, including Executive Directors, their advisors, and assistants. The control gaps identified in this audit, when considered in the aggregate and in the context of the financial resources involved, represented significant weaknesses in the design and operating effectiveness of controls. Certain elements, such as the processing of payments for salaries and benefits in FIN, were well controlled and supervised. However, there were a number of deficiencies in the design and operating effectiveness of controls supporting the administration of benefits, as well as the oversight, accountability, and assurance processes within HRD for detecting errors and policy non-compliance. The lack of capacity in HRD to implement robust internal controls has persisted for several years. HRD management has made efforts, within the past two years, to build capacity through the hiring of new staff with knowledge and experience in designing and implementing internal controls. However, it was agreed that a fully effective control framework may not be achievable without additional resources, or by diverting resources from other activities.

7. The **Audit of the Administration of the Staff Financial Disclosure Program** examined the design of the Program's controls, but did not perform detailed testing of the operating effectiveness of the controls due to confidentiality restrictions on individual staff financial disclosure submissions. The audit made two recommendations covering: (i) the review methodology developed by KPMG—the external compliance advisor—to analyze financial holdings and transactions submitted by staff for possible financial conflicts of interest; and (ii) the follow-up process to ensure that staff have taken the agreed upon actions to remediate financial conflicts of interest.

8. The **Audit of the Voluntary Savings Plan (VSP)** assessed the adequacy of controls within the process flow for transactions, including the updates of the VSP business rules in the Fund's Information Technology (IT) systems. The audit found that generally, controls are operating effectively, and that the VSP business rules have been properly updated in the IT systems. OIA found opportunities to strengthen certain aspects of VSP operations, in particular, the audit recommended that HRD, FIN, and TGS improve: (i) the monitoring of Wells Fargo's annual financial statements and internal controls; (ii) the monitoring of the IT security provisions of the Fund's contract with Wells Fargo; and (iii) user access controls for VSP systems.

9. The **Audit of the Fund's Data Centers** assessed the design and operating effectiveness of the controls that protect and safeguard the confidentiality, integrity, and availability of the Fund's information assets. The scope included the HQ1 and HQ2 data centers, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) facilities and equipment, the offsite data recovery center, and the communication links between all the data centers. The audit examined management oversight of the data centers, the data centers' key operating controls, physical and environmental security, construction risks due to ongoing renovations to the HQ1 building, and data center-related

business continuity management. The audit is substantially complete and the draft report will be issued in early June

10. The Audit of Software License Management assessed whether the processes to manage software licenses in the Fund are effective in ensuring that legal and business risks associated with the ownership and use of software licenses are mitigated. The Fund relies on software installed on over 6000 computers and 2200 servers to support its core business capabilities. Annual spending on software (purchase and maintenance) is approximately \$20 million. The scope of the audit included software installed on Fund workstations and servers, and the home-use software program. Since OIA's last audit of software licenses (FY 2009), which identified a number of significant weaknesses, some progress has been made by TGSIT to strengthen controls. There are still weaknesses that need to be addressed before management can be confident that the associated legal risks are properly managed, and that Fund resources are used efficiently. OIA made recommendations to strengthen the approach to the management of software licenses in the following four areas: (i) policy; (ii) software lifecycle management; (iii) the inventory of Fund software; and (iv) the home-use software program.

11. The Audit of the IT Controls of the SWIFT System assessed the effectiveness of the confidentiality, integrity, and availability controls in the SWIFT system as implemented in the Fund. SWIFT is a secure communications channel used to exchange standardized financial messages for communicating payment instructions and other sensitive data. The Fund uses the SWIFT system to send and receive requests for transfers of funds among various organizations worldwide. While the processes for the logging and monitoring of SWIFT messages are effective, the audit identified a number of weaknesses in the way the SWIFT system is managed. Weaknesses existed in the areas of configuration management; the maintenance and support of the SWIFT system; and user administration. The ownership of the SWIFT system, and the corresponding roles and responsibilities were also unclear. The audit made recommendations to address these gaps, with the aim of strengthening the overall, and sustained, management of the SWIFT system. Since the report was issued, progress has been made in the areas of configuration management, maintenance and support of the SWIFT system, and coordination of roles and responsibilities between FIN and TGSIT.

12. The Advisory Work on the Preparation of ICD's Regional Technical Assistance Centers (RTAC) Handbook. The work was initiated following discussion with ICD leadership, to provide early input and assistance in support of the design of a comprehensive procedural Handbook for the RTACs, partly as a response to a previous OIA recommendation. OIA provided comments and feedback to ICD during the drafting of the Handbook chapters, focusing on financial and budgetary controls, and the mitigation of financial, operational and reputational risks to the Fund. ICD has incorporated OIA's comments in the final version of the Handbook that will be circulated Fund-wide in FY 2016.

13. This targeted Advisory Review of the Application of the Rules for Correction (under the Fund's Transparency Policy) to Article IV Consultation Staff Papers focused on the application of the rules for correction, and the internal controls designed to minimize errors in Article IV consultation staff papers during their production stages. The review added to the periodic Board

review of the transparency policy (conducted by SPR). The processes designed for the application of the rules for correction and to minimize errors in Article IV consultation staff papers are operating as designed. However, there are opportunities to strengthen related controls. The elements of the process that could be improved include: (i) the completeness of data on rejected correction requests; (ii) the documentation trail supporting the confirmation of authorities' views during consultations; (iii) the validation and compliance monitoring tools for country desk data; (iv) certain quality aspects of the review process; and (v) the outreach to country authorities on the transparency policy. The report proposed ways to strengthen the processes that underpin the transparency of the decision-making process for correction requests, and also made some practical suggestions for improving the management of the incidence of corrections across departments. The suggestions were advisory in nature, designed to feed into management's consideration of process improvements, and should be weighed against institutional risk tolerance and the associated implementation costs.

OIA INTERNAL PROJECTS

14. The Review of OIA's Recommendation Follow-up Process analyzed more than 300 control issues that have been raised by OIA between FY 2009 and FY 2014, to assess the extent to which risk themes from this population could be constructively derived and addressed, and to identify areas of improvement in OIA's follow-up process. OIA also reviewed the population of 72 unique outstanding recommendations from 27 audits open in its tracking database as of January 2015. The objectives were to: retire or rewrite superseded issues; recalibrate ratings based on risk; analyze common risk themes; and identify ways to improve OIA's recommendation follow up process. This review has been largely completed and delivered several useful results. The review concluded that two-thirds of the recommendations could be closed at year end FY 2015, either because updated information has been provided by client departments, or issues are now out of date, or the residual risks to the Fund are minimal.

15. As a result of this work, the database of remaining recommendations forms a more solid and risk-focused baseline in support of OIA's work and reporting to management. Several risk themes were identified which informed the preparation of OIA's FY 2016 risk assessment and proposed program of work (e.g., management of third party service providers and identity access management). From an internal perspective, the review highlighted areas that need to be strengthened in OIA's approach to follow up. The intention is that a paper proposing changes to OIA's follow up practices will be circulated to departmental Directors for consideration, and subsequently sent to management for approval.

16. The Review of OIA's Annual Planning Methodology was designed to promote increased collaboration with clients (including the institutional risk function), and to include appropriate consideration of the institution's key goals and priorities. The Fund's Accountability Framework serves as the main tool for understanding the Fund's priorities. The consideration of top down priorities is supplemented with ongoing dialogue with departments to better understand their day-to-day operations and the practical challenges to the achievement of their goals. OIA launched a

stakeholder relationship management framework in early FY 15. The aim was to start to build closer working relationships between OIA staff and Fund colleagues at the working level, and also to understand departmental priorities, and the potential risks to the achievement of departmental goals. The revised approach supports OIA's ambition of taking on, over time, a more strategically-relevant role in the Fund.

STATUS OF FY 2015 WORK PLAN

A. Audits and Reviews

17. In compliance with OIA's accountability framework, all audits and reviews planned for FY 2015 have been completed, or are in the reporting phase (see table 1).

B. Risk Management

18. In FY 2015, OIA assisted the Advisory Committee on Risk Management (ACRM) in the preparation of the 2014 Report on Risk Management. The final report produced by OIA was issued in June 2014 (SM/14/172, 6/20/14). Just prior to this, in May 2014, the Managing Director established the new Risk Management Unit (RMU) within OMD, effective June 2014, with the objective of fostering a strong risk culture throughout the institution. OIA is working collaboratively with the RMU as it develops a risk management framework for the Fund. At a practical level, OIA now (i) shares all its audit reports with the RMU, and (ii) is categorizing its findings into risk areas or systematic risk themes to feed into the RMU's overall picture of risks to the institution.

C. Periodic Monitoring Report (PMR)

19. The Executive Board, endorsed by the Managing Director, and supported by the External Audit Committee, approved the transfer of responsibility for the preparation of PMRs to OIA (EBAP/14/10, 2/30/14). OIA issued its first and the Fund's Sixth PMR in July 2014 (SM/14/194, Supplement 1, 7/31/14), covering four endorsed Management Implementation Plans (MIPs). It also presented an update of progress on previously raised MIPs.

ADMINISTRATIVE MATTERS

20. OIA's budget for FY 2015 was \$4.4 million; the outturn was \$4.3 million. The budgeted cost for supporting OIA's operations corresponds to about 0.46 percent of the Fund's net administrative budget.

**Table 1. OIA’s Work Plan, FY 2015
As of April 30, 2015**

| Project Title | Project Status |
|---|------------------------|
| Audits and Reviews | |
| Operational and Financial Audits and Reviews | |
| 1. Audit of the Investment Account (IA) | Completed |
| 2. Audit of the Financial Transactions Related to the HQ1 Renewal Project | Completed |
| 3. Audit of the Administration of Salaries and Benefits | Completed |
| 4. Audit of the Financial Disclosure Program | Completed |
| 5. Audit of the Voluntary Savings Plan (VSP) | Completed |
| Technology Audits | |
| 5. Audit of the Fund’s Data Centers | Reporting phase |
| 6. Audit of Software License Management | Completed ¹ |
| 7. Audit of the IT Controls of the SWIFT System | Completed |
| Advisory Reviews | |
| 8. Advisory Work on the Preparation of the Control Framework for Regional Technical Assistance Centers (RTACS) Handbook | Completed |
| 9. Advisory Review of the Application of the Corrections Policy to the Article IV Consultation Staff Papers | Completed |
| OIA Internal Projects | |
| 10. Review of OIA’s Recommendation Follow-up Process | Reporting phase |
| 12. Review of OIA’s Annual Planning Methodology | Completed |
| Risk Management | |
| 1. 2014 Report on Risk Management | Completed |
| Periodic Monitoring Reports (PMR) | |
| 1. Sixth PMR | Completed |

Source: Office of Internal Audit and Inspection

¹ Report issued May 22, 2015