FOR INFORMATION

EBAP/17/4

January 11, 2017

To: Members of the Executive Board

From: The Secretary

Subject: **Office of Internal Audit and Inspection—FY 2017 Interim 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 January 17, 2017, to answer questions on this Interim Activity Report.
Questions:	Ms. Brady, OIA (ext. 39532) Mr. Murugan, OIA (ext. 38132)

INTERNATIONAL MONETARY FUND

OFFICE OF INTERNAL AUDIT AND INSPECTION (OIA)—FY 2017 INTERIM ACTIVITY REPORT

January 10, 2017

EXECUTIVE SUMMARY

This report provides an overview of OIA's activities in FY 2017 to date. The report fulfills management's commitment to keep the Executive Board regularly informed on audit and control-related items.

In the first part of the year, two reports that had been issued in draft at the time of OIA's 2016 Activity Report were finalized: (i) the advisory review of the cost-recovery model for externally-funded capacity development; and (ii) the audit of the contracting process for third party service providers. OIA completed its work on three audits that were in progress at the beginning of FY 2017: (i) the audit of the quota increase payments under the 14th general review; (ii) the audit of the Fund's business continuity management program (report issued to client departments); and (iii) the audit of the Fund's approach to identify and access management (report issued to client departments). In addition to its approved Program of Work, OIA conducted an independent evaluation of the prototype of the Fund's Economic Data Registry at the request of the Chair of the Economic Data Steering Committee.

OIA also issued its third Periodic Monitoring Report (PMR) in December 2016. The PMR assesses the extent to which Board endorsed IEO recommendations have either been implemented or are in progress. The Evaluation Committee (EVC) will meet to discuss the report's findings on January 25, 2017.

In November 2016, OIA concluded its annual planning exercise to formulate a new Program of Work for FY 17/18. OIA's planning cycle has been shifted to align with the Fund's strategic planning cycle and now also systematically considers the Fund's risk profile. Management approved the Program of Work in December 2016.

In the first half of the year, OIA completed changes to its staffing model to bring about a more robust delivery structure, strengthen professional practices, foster teamwork and collaboration, and build pipeline talent and sustainability for the function. The staffing of three new managerial positions was completed in the second quarter of 2017. Updates to OIA's job ladder were finalized in November 2016 to align with the Fund's job standards and best practices in the internal audit profession.

Approved By
Clare Brady

Prepared by the Office of Internal Audit and Inspection

CONTENTS

INTRODUCTION

1. This report fulfills the Managing Director's commitment to regularly share information with the Board on audit and control-related matters, and provides an overview of the Office of Internal Audit's (OIA) activities in FY 2017 to date. The report includes a summary of the work completed and underway in the first half of FY 2017; a summary of the outcome of OIA's follow up of IEO recommendations captured in the Eighth Periodic Monitoring Report; and an overview of the FY 2017 follow up work on outstanding internal control issues.

2. On January 17, 2017, 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 visit of the External Audit Committee (EAC) by providing an opportunity to discuss FY 2017 audit coverage with OIA team members.

OFFICE OF INTERNAL AUDIT AND INSPECTION (OIA)

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 WORK COMPLETED TO DATE IN FY 2017

A. Advisory Review of the Cost-Recovery Model for Externally-Funded Capacity Development (finalized June 2016)

4. The review assessed the design and implementation of the cost recovery model for externally-funded capacity development (CD). CD accounts for 27 percent of the Fund's total output, or $310 million of total spending, of which $140 million represents funding through external contributions. While the scope of this review covered all elements of the approach to cost recovery (direct costs, indirect costs, and trust fund management fees), the most significant gap, in terms of overall financial impact, was in the area of indirect costs.

5. While many comparators have found themselves in a similar position of under-recovering indirect costs, a few institutions have made the strategic shift towards an approach that recognizes external resources as integral to the institutions' overall financing portfolio. Drawing on these comparator practices, this review suggested various areas in which the Fund's cost recovery model could be strengthened. The report noted that these options

should be considered in conjunction with the broader strategic questions on the direction, management, and financing of externally-funded CD in the longer term.

6. The output from OIA's review is being considered by ICD and OBP in the context of options for strengthening the cost recovery model. In addition to the broader strategic discussions about the cost recovery model, management also asked departments to address the opportunities for process improvement that were noted in the report. These included: (i) a review of the standard cost approach used to charge most personnel costs; (ii) the implementation of measures to budget for and capture eligible costs that are generated outside the core CD delivery teams or departments; (iii) the improvement of departmental review processes; (iv) streamlining time reporting; and, (v) sharing knowledge and good practices. Departments have already started taking action in a number of these areas.

B. Audit of the Quota Increase Payments Under the 14th General Review (issued June 2016)

7. In response to a request from Board members during the January 2016 EAC visit, OIA performed audit procedures with respect to the collection and recording of the 14th review quota payments. Quota payments were made pursuant to the adoption by the Board of Governors of Resolution 66-2, in December 2010, that became effective January 26, 2016. OIA's overall objective was to provide additional assurance, relative to the audit work conducted by PwC, that quota increase payments, and NAB rollbacks, had been accurately processed and recorded in the Fund's FY 2016 financial statements.

8. OIA concluded that controls for the processing of payment of quotas and NAB rollbacks were appropriately designed and operated effectively, and that transactions were processed and recorded in accordance with Board decisions. OIA's audit procedures, liaising with FIN and PwC, included a review of the control framework designed by FIN, and testing of the operating effectiveness of controls based on a sample of transactions.

C. Audit of the Contracting Process for Third Party Service Providers (finalized July 2016)

9. The overall objective of this audit was to evaluate the design and operating effectiveness of the process for contracting with third parties. The audit specifically focused on: the achievement of value for money; the governance framework; the controls to mitigate financial, operational and reputational risks; and fraud mitigation measures. The audit concluded that, since the last audit in FY 2008, CSF Procurement (PB) has successfully shifted its focus away from transactional controls, towards a more strategic, value and service oriented approach.

10. Opportunities to strengthen controls were highlighted in three areas: (i) delegated procurement activities; (ii) the vendor risk assessment process, and; (iii) the payment process. Action plans were designed by client departments to mitigate the risks. Specifically: (i) PB agreed to develop outreach and training to departments with delegated authority, along with monitoring of delegated contracts meeting certain criteria; (ii) the vendor risk assessment process

will be expanded to include an assessment of the vendors' operations and internal controls before they are hired; and, (iii) PB and FIN will work together to redesign the payment process and strengthen segregation of duties control. OIA's forthcoming audit of the management of third party vendors will complement the results of this audit, and will assess the Fund's framework for managing the ongoing risks associated with use of third party service providers, including cloud and other managed service solutions.

D. Evaluation of the Economic Data Registry (EDR) Prototype (issued November 2016)

11. The aim of the Economic Data Registry (EDR) project is to address the Fund's need for a single access point to economic data in internal and external databases. The EDR project has two main phases: (i) delivery of the prototype, and (ii) full implementation (inclusion of additional functionality, finalization of the user interface, improvement of usability and search results, and ingestion of additional databases). The Fund's selected software vendor delivered a prototype of the EDR solution in early September 2016.

12. At the request of the Chair of the Economic Data Steering Committee (EDSC), OIA conducted an independent evaluation of the prototype to objectively inform the EDSC's decision on whether to proceed with the full implementation of the EDR project. The main components of the evaluation were to: (i) assess the delivery of the technical requirements; (ii) review the results of the "use cases", and data owner and user feedback; (iii) assess the design of the system architecture and system security; and (iv) review a sample of customized code.

13. OIA concluded that the business requirements, as identified in the vendor contract, had largely been implemented in the prototype. Further, there were no significant vulnerabilities in the system security, architecture or customized code. The report highlighted that user adoption of the final EDR product should not be assumed solely based on the technical implementation of the business requirements, and stressed the importance of user engagement and expectation management as the project progresses. The report also flagged some important forward looking considerations in the areas of: clarity of roles and responsibilities; vendor and contract management; the complexity of Fund data; and technical system documentation. The next phase of the EDR project will focus on improving usability, and implementing user interfaces and additional functionality.

E. Audit of the Fund's Business Continuity Management (BCM) Program (report issued to client departments in December 2016)

14. The objective of this audit was to assess the design and operating effectiveness of the Fund's BCM program. The audit also assessed the phases of the Fund's BCM program against industry leading practices. The scope of the audit, including the nature and depth of testing for each of the phases of the BCM program, took into consideration: (i) remedial actions, in response to the 2012 OIA audit; and (ii) the relatively recent creation of both the Chief Administrative Officer role, and the RMU, and their potential impact on the governance and design of the program.

15. The audit concluded that incremental improvements have been made to the BCM arrangements over the last decade, but further progress needs to be made to improve the effectiveness of the overall program. A lack of clarity about the approach that should be taken to risk mitigation, and gaps in the governance arrangements, have contributed to some weaknesses in the design and potential effectiveness of the Fund's BCM program. A draft report has been issued, and departments are in the process of formulating action plans.

16. The recent establishment of the Fund Risk Committee provides an opportunity for an institutional discussion on the BCM program gaps. In particular, it may be beneficial to reconsider the appropriate risk acceptance level for the Fund, given the gap between the Fund's implied risk acceptance level (now explicit) and the approach that has been taken, to date, to mitigate BCM-related risks.

F. Audit of the Fund's Approach to Identity and Access Management (IAM) (report issued to client departments in December 2016)

17. IAM is the framework for managing and using identities that allows individuals to access information assets. This framework includes the strategy, the business processes, the technical solutions, and the data needed to identify (i.e., who you are), authenticate (i.e., you are who you say you are), and authorize (i.e., what you are allowed to do) individuals to access physical and logical assets. The Information Technology Department (ITD) has been working on improving IAM processes at the Fund, including performing an IAM gap analysis in the context of the Enterprise Information Security Program (EISP). Booz Allen Hamilton was engaged to conduct the gap analysis.

18. OIA's audit assessed Booz Allen Hamilton's high-level recommendations in the context of the Fund environment. The main objective of this additional piece of work was to assess current practices, challenges, operating effectiveness of controls, and support management by identifying pragmatic next steps in terms of strengthening IAM practices. The audit assessed: (i) the design of the IAM framework to meet the current and future needs of the Fund; (ii) the translation of the framework into processes and practices; (iii) the processes for identifying, and responding to risks related to IAM; and (iv) the processes for measuring the effectiveness of IAM**.**

19. The Fund's approach to IAM should, in the first instance, be guided by the Board's low risk acceptance for information security. Against that backdrop, the audit highlighted certain areas that should be prioritized to improve governance, streamline processes and improve controls. These areas include cross-functional IAM program governance, privileged access, training, and recertification processes. A draft report has been issued, and departments are in the process of compiling action plans to address the issues raised in the report.

PERIODIC MONITORING REPORT (PMR)

20. OIA completed the annual follow up work for Board-endorsed IEO recommendations during the first half of FY 2017 and issued the PMR in December 2016. The report assessed the progress made over the last year on actions contained in the four MIPs arising from recent

IEO evaluations, and another four for which individual management actions were classified as still "in progress" in the Seventh PMR. Overall, 43 of the 77 actions included in the eight MIPs covered in this PMR have been implemented.

21. The Eighth PMR concluded that progress on implementing management actions has been somewhat uneven. Management actions associated with the four recently issued management implementation plans (MIPs) are progressing well. In contrast, actions included in older MIPs are progressing more slowly. Many of the older management actions are more broadly worded and in many instances have no clear timetable.

22. The Evaluation Committee (EVC) will meet to discuss the report's findings on January 25, 2017.

OUTSTANDING AUDIT ISSUES

23. OIA has now issued two 'snapshot' reports on outstanding and overdue audit issues and a six-monthly reporting cycle has been agreed with management (see the last report attached as Appendix I). The next report to management will be issued at the end of January 2017, and will represent the situation at the end of the 2016 calendar year. Over the last year the heightened sensitivity to open audit issues has resulted in an overall reduction of outstanding issues from 72 to 20. In addition, since the issuance of the last six-monthly report in July 2016, one "high" impact rated issue on HQ1 financial transactions has been closed (October 2016).

24. Now that the discipline of regular follow up has been established, OIA will reconsider the timing of the reporting cycle to maximize the value of the updates for management, the EAC and the Board.

OIA INTERNAL ACTIVITIES

A. Program of Work for FY 17/18

25. In November 2016, OIA concluded its annual planning exercise to formulate its Program of Work for FY 17/18. The formulation of the Program of Work is underpinned by two key improvements to OIA's risk-based planning approach: (i) a closer alignment of OIA's work plan with the Fund's strategic planning cycle; and (ii) a systematic consideration of the RMU's assessment of the Fund's risk profile. As required by professional auditing standards, OIA's planning approach takes into account the institution's view of risk, including the risk acceptance levels determined by Board and Management.

26. The FY 17/18 Program of Work is designed to align with key institutional focus areas and risk mitigation themes (see illustrative overview in Appendix II). The Program includes a balanced mix of audits and advisory reviews and incorporates coverage of key areas such as Results-Based Monitoring of Capacity Development (RBM), Modernization of HR Systems, Third-party Vendor Management, and Network Security.

B. FY 2018 Accountability Framework Deliverables

27. In addition to the execution of its Program of Work, in FY 2018 OIA will develop and publish its first Annual Report. The aim of the report will be to provide insight by drawing on OIA's body of work and distilling broader qualitative messages on the state of the Fund's risk management, governance, and controls processes.

28. OIA is also upgrading its Quality Assurance and Improvement Program (QAIP), to anchor audit procedures to professional standards, and support the continuous improvement of work practices. In FY 2018, OIA will undertake an External Quality Assessment (EQA) by an external independent team of qualified audit professionals to validate OIA's commitment to quality and accountability.

29. In terms of its methodological approach, OIA will integrate data analytics into the planning phase of its engagement-level procedures. This approach is intended to increase the institutional impact of OIA's work through data-driven insights and analysis.

ADMINISTRATIVE MATTERS

A. OIA Target Operating Model

30. OIA successfully completed the staffing of three new managerial positions in the summer of 2016. The changes were in part designed to bring about a more robust delivery structure, strengthen OIA's professional practices, foster teamwork and collaboration, and build pipeline talent and sustainability for the function.

31. OIA completed a redesign of the Auditing Job Ladder (clustering of professional jobs into grade bands) in November 2016, by working closely with HRD. The proposed model better differentiates the responsibilities of senior-level internal audit professionals from those of mid-level and entry-level professionals, and clarifies accountabilities. It also allows for a streamlined description of job standards, within the context of the Fund's grade structure, that are better aligned with OIA's operating model, and with industry practices.

B. FY 2017 Budget Outlook

32. OIA expects to end FY 2017 at or above 98 percent of its overall budget allocation of $4.6 million. OIA made internal budget reallocations as part of its FY 2017 mid-year reallocation, to support optimal deployment of its overall resource envelope.

Appendix I. Report on Outstanding Audit Issues as at June 30, 2016

Key Messages

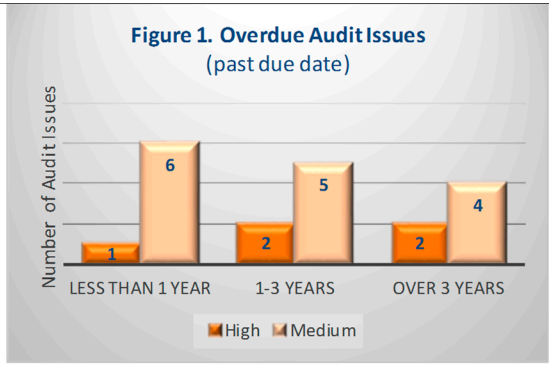
This report presents an overview of outstanding and overdue audit issues. The total number of outstanding issues has been reduced from 31 at end-December 2015, to 20 as of June 30, 2016. All the open issues are now overdue.

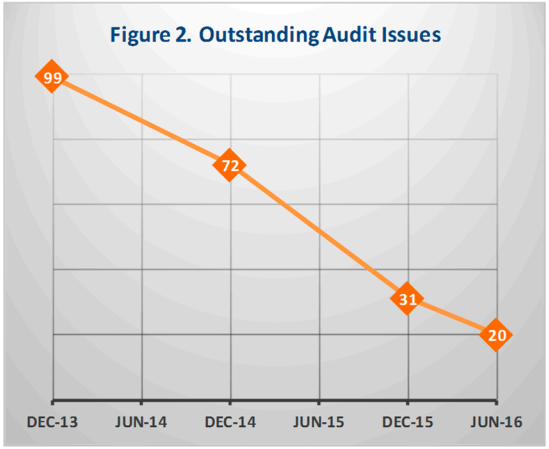
Five of the overdue issues were rated as 'High' impact. Since the last report, one High rated issue covering access controls for the data centers has been closed, and a risk management issue from the same data center audit is now overdue. These issues stem from four audits: Business Continuity Planning (BCP) (2012); Financial Transactions related to the HQ1 Renewal Program (2014); Administration of Salaries and Benefits (2014); and, Data Centers (2015).

- **BCP:** Issues remained unresolved following the last audit in 2012. In addition, the 2016 Spring Update of the Risk Report flagged business continuity as an area in which risk levels are deemed to be higher than the acceptable risk level implied by Fund policy and processes. These two drivers triggered the current audit of the BCM program, to include an assessment of the associated risks. The high-level objectives of the audit are to flag those issues that require decisions at the institutional level, and to create momentum for closing the remaining control gaps.
- **Financial Transactions related to the HQ1 Renewal Program:** The risks relating to schedule (and related cost) uncertainty have largely been mitigated. A new cost loaded schedule ensures that progress is reported to all key stakeholders, including the Board. The completed global settlement with contractors substantially eliminated the backlog of construction change requests (CCRs) and provides greater certainty on the project's budget exposure. To sustain this progress, new procedures to improve the change order process are being developed. These procedures will be completed by the HQ1 team and reviewed before OIA's next monitoring report.
- **Administration of Salaries and Benefits:** Steady progress continues to be made by HRD to mitigate control risks. Given recent departmental changes, including to the Division that is responsible for developing the control framework, it will be important for HRD to focus on (i) capacity issues in terms of the skills required to design and maintain processes and controls, and (ii) key person dependencies.
- **Data Centers**: ITD has now completed a comprehensive review of all access lists, and stronger requirements for managing and monitoring of access rights have been implemented. ITD has also implemented an Information Security Governance, Risk and Compliance framework (ISGRC) to facilitate risk-based decision making and escalation of security-related matters. Discussions on the development of a similar framework for data center-related business continuity are ongoing.

There are four Medium-rated issues that are more than three years overdue. Two are related to Business Continuity (discussed above). The remaining two are nearing completion:

- To address issues with the **accuracy of local employee information** (report issued in April 2011), a capital project is in the final stages of software development, following approval in FY16. The development phase of the project was delayed due to the more urgent PeopleSoft upgrade. The project is expected to be completed in August 2016.
- Risks related to policies governing the designation of depositories and concentration of **gold holdings** have not been reviewed by the Board for fifty years (report issued in 2012). FIN is in the latter stages of preparing a report to management on a re-assessment of the concentration risks and the custodial arrangements, including guarantees.





International Standards for the Professional Practice of Internal Auditing

2500 – Monitoring Progress: The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 - The chief audit executive must ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

Appendix II. Alignment of OIA's Coverage with MKGs