

**FOR
INFORMATION**

EBAP/18/1*

January 10, 2018

To: Members of the Executive Board

From: The Secretary

Subject: **Office of Internal Audit—FY 2018 Interim Activity Report**

Board Action: Executive Directors' **information**

Publication: No, due to content sensitivity.

Additional Information: Ahead of the visit of the External Audit Committee, OIA will be available in the Board Committee room on January 24, 2018 to answer questions on this Interim Activity Report.

Questions: Mr. Murugan, OIA (ext. 38132)

*Subject line amended to provide correct name of the Office of Internal Audit.



January 2, 2018

OFFICE OF INTERNAL AUDIT (OIA) – FY 2018 INTERIM ACTIVITY REPORT

EXECUTIVE SUMMARY

This report provides an overview of OIA's activities in FY 2018 to date. The report fulfills management's commitment to keep the Executive Board regularly informed of audit and control-related items.

In the first part of the year, OIA completed two audits: (i) the audit of third party vendor management; and (ii) the audit of systems development and maintenance processes. Advisory reviews are underway in the areas of: (i) the results-based management for capacity development; (ii) committee structure for risk management; and (iii) talent acquisition. OIA continued to provide ongoing advisory support to the 1HR program team. OIA has also begun planning for an advisory engagement covering the Fund's overseas presence.

OIA introduced, during the first half of the year, two new approaches to reporting (Insight Notes and Good Practice Series) to complement its traditional outputs. These new products are designed to deliver timely insights on governance, risk, and control matters and promote greater risk and control awareness within the organization. OIA's first Insight Note covered the Fund's approach to issuing, updating, and enforcing its administrative policies. The maiden edition of OIA's Good Practice Series covered the "Three Lines of Defense" (3LOD) model and the delineation of risk management roles and responsibilities in the context of the Fund's governance framework.

OIA has commenced its preparation and review activities leading to the production of the Ninth Periodic Monitoring Report (PMR). Building on process improvements effected in prior years, OIA published an online repository of the population of IEO recommendations and related management actions.

OIA has also begun its planning exercise to formulate its Program of Work for FY 2019, which is expected to be presented to the External Audit Committee (EAC) and Management by end-March 2018.

During the second half of FY 2018, OIA will undertake an External Quality Assessment (EQA). The EQA is designed to assess OIA's conformance with professional auditing standards.

Approved By
Packiaraj Murugan

Prepared by OIA

CONTENTS

INTRODUCTION	3
OIA'S MANDATE	3
SUMMARY OF WORK COMPLETED TO DATE IN FY 2018	3
A. Insight Note on Fund's Administrative Policies and Procedures (issued July 2017)	3
B. Audit of Third Party Vendor Management (issued September 2017)	4
C. Good Practice Series (GPS) on the Three Lines of Defense (3LOD) Model (issued October 2017)	4
D. Audit of the Fund Systems Development and Maintenance Processes (issued November 2017)	5
E. Informal Advisory Work	6
SUMMARY OF WORK UNDERWAY IN FY 2018	6
A. Review of the Results Based Management (RBM) Initiative for Capacity Development (in progress)	6
B. Review of Talent Acquisition (in progress)	7
C. Review of the Committee Structure for Risk Management (in progress)	7
D. Review of the Fund's Overseas Presence (planning underway)	7
NINTH PERIODIC MONITORING REPORT	8
OVERDUE ISSUES	8
OIA INTERNAL ACTIVITIES	8
A. Program of Work for FY 2019	8
B. FY 2019 Accountability Framework Deliverables	8
C. Quality Assurance	9
ADMINISTRATIVE MATTER	9
APPENDIX	
I. Report on Overdue Audit Issues as at October 31, 2017	10

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 2018 to date.** The report includes a summary of the work completed and underway in the first half of FY 2018; results of OIA’s follow up work on outstanding internal control issues; and an overview of key internal OIA activities.
2. **On January 24, 2018, 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 2018 audit coverage with OIA staff.

OIA’S MANDATE

3. **OIA is an independent assurance and advisory function designed to protect and strengthen the Fund.** The mission of OIA is to: (i) bring a systematic and disciplined approach to assess and improve the effectiveness of the Fund’s governance, risk management processes, and internal controls; and (ii) act as a consultant and catalyst for the improvement of the Fund’s business processes by advising on best practice and the development of cost-effective control solutions.
4. **OIA’s work is carried out in accordance with the Institute of Internal Auditors’ (IIA) International Professional Practices Framework (IPPF).** To provide for the independence of OIA, the Director of OIA reports to Fund management, and maintains a functional reporting relationship with the EAC.

SUMMARY OF WORK COMPLETED TO DATE IN FY 2018

A. Insight Note on Fund’s Administrative Policies and Procedures (issued July 2017)

5. **OIA’s first “Insight Note” - a new reporting format designed to contribute to institutional problem-solving – covered the Fund’s approach to issuing, documenting, updating, and enforcing administrative policies.** The Insight Note, produced with the full support of LEG, identified areas of weaknesses in the Fund’s handling of administrative policy, procedure, and guidance documents and suggested certain improvements for management consideration.
6. **The systemic weaknesses identified covered: (i) hierarchy and level of authority underpinning Fund administrative policies and procedures; (ii) documentation, communication, and access; and (iii) accountability and ownership.** These weaknesses collectively undermine: (i) consistent interpretation by staff of the applicability or level of authority of different policy and procedure documents; (ii) timely and effective access to and communication about the relevant administrative policies and procedures; (iii) ownership of policies; and

(iv) awareness of policies and monitoring of compliance, making it difficult to effectively escalate and manage policy exceptions or waivers.

7. LEG has developed a detailed work plan to address the identified issues in the OIA

Insight Note. The work plan will be undertaken in two phases: (i) the first phase will comprise the development and publication of a Fund-wide administrative manual (covering areas not codified in the Staff Handbook); and (ii) the second phase will look to define, standardize and streamline the processes for issuing, monitoring, and updating administrative policies.

B. Audit of Third Party Vendor Management (issued September 2017)

8. The overall objective of this audit was to assess the robustness of the Fund’s approach to managing risks associated with third party vendors throughout the lifecycle of the vendors’ engagement with the Fund.

9. Despite improvements made in recent years to processes and controls at the point of signing contracts with vendors, the audit concluded that there are foundational weaknesses in the Fund’s approach to managing third party risks after contracts have been awarded. The Fund is increasingly reliant on third parties, and the monitoring of risks associated with managing vendor services warrants an improved and more consistent approach. Specifically: (i) there are no clearly defined governance arrangements in place; (ii) weaknesses exist in the risk assessment methodology used to assess and prioritize vendor-related risks for monitoring; (iii) there are limitations in the coverage and design of current monitoring processes; and, (iv) the Fund’s ability to holistically analyze third party risk information and performance is limited. The audit also included a benchmarking against industry practices which revealed that Fund’s third party vendor management practices are at an early stage of maturity, lagging practices in the Financial Services Industry (FSI) but quite comparable to the practices of other MDBs/IFIs. Forward-looking suggestions for strengthening processes have been provided to the procurement team for their consideration.

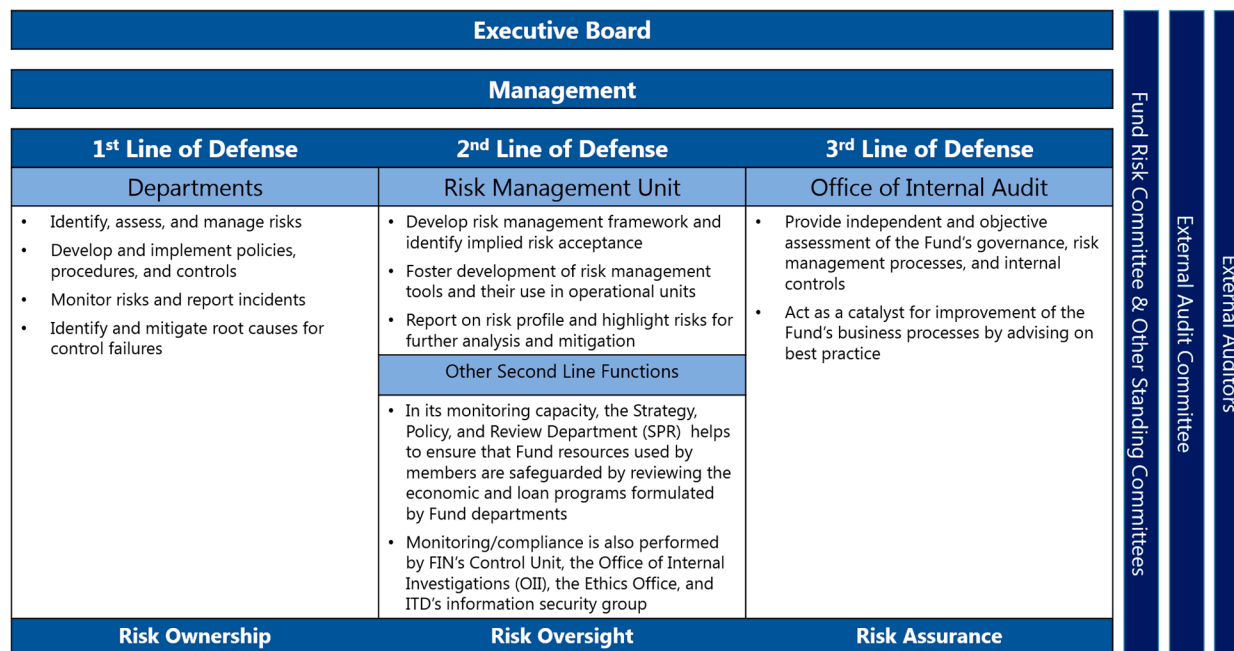
10. While there is a clear need to address weaknesses identified in the report, it is important that the improvement efforts be guided by a risk assessment exercise that balances the required level of risk mitigation against the associated costs. In this context, CSF is pursuing a sound approach for remediation of the identified issues, and is working on establishing a holistic third-party risk management framework that is suitably informed by the Fund’s risk acceptance and resource availability. Once this overarching framework is established, the subsequent implementation efforts will be suitably guided by the principles set out in the framework.

C. Good Practice Series (GPS) on the Three Lines of Defense (3LOD) Model (issued October 2017)

11. With a view to supporting the institutional goal of integrating risk management into the Fund’s operational fabric, OIA also published the first edition of its “Good Practice Series” (GPS) – covering the “Three Lines of Defense” (3LOD) model. The model is a well-established governance framework for risk management (used by global and domestic regulators) that is

predicated on defining clear roles and responsibilities, and on maintaining separation of roles among the various groups involved in risk management.

12. The coverage of the 3 LOD model, in OIA's maiden edition of the GPS, was intended to reinforce the ongoing institutional efforts to strengthen greater risk ownership.



13. The GPS provided an overview of the distinct roles played by the three “lines” within the Fund’s governance framework (as depicted above), with the Board and Management being the primary stakeholders served by the lines. The GPS also outlined the benefits of the model, its key foundational elements, efforts underway within the Fund to promote greater risk accountability, and some key indicators for assessing effective operationalization of the model. There has been positive response from client departments on OIA’s new product, particularly in context of reinforcing ownership within departments for risk management and internal controls.

D. Audit of the Fund Systems Development and Maintenance Processes (issued November 2017)

14. The Systems Development Life Cycle (SDLC) is a broadly used term for the framework that defines tasks to be performed at each step in the development and maintenance of software. Successful SDLC processes aim at implementing quality information system solutions within cost and time constraints. The need for robust SDLC processes is particularly important given the multitude of IT systems in the Fund, the emergence of business-led software development activities, the transition to cloud-based solutions, and the implementation of major technology solutions such as the 1HR program.

15. The objective of this audit was to assess the design and effectiveness of the Fund’s SDLC processes for managing risks that impact the overall quality of the software solution, the total cost of delivery, and the security of the Fund’s information.

16. The lack of clearly articulated risk-based requirements for SDLC activities at the institutional level has resulted in significant weaknesses in the Fund’s software development approach. Further, the absence of a management-approved software development and maintenance policy that applies across the organization and inadequate enforcement of software development standards have led to variable quality in SDLC practices.

17. The audit noted that urgent attention should be given towards mandating and enforcing improved SDLC controls across the Fund. These control improvements should be designed and implemented in a risk-differentiated manner, to consciously apply greater rigor in higher risk areas, while considering cost and efficiency aspects. ITD has provided a combination of near-term and medium-term measures to address the issues highlighted in this report.

E. Informal Advisory Work

18. As part of informal advice to the Director of HRD and the Deputy Managing Director and Chief Administrative Officer, OIA completed a health-check of the 1HR program. The health-check was designed to provide a quick and effective means for management to check on the program’s progress at an early stage. The results indicated that the program has had challenges in this preliminary stage; however, the shared commitment of all stakeholders to the success of the program, and the lessons learned to date have provided an opportunity to “reset”. OIA suggested improvements, including in the areas of governance and accountability, business case development, and project planning – some of which have been already implemented. OIA continues to provide ongoing advisory support to the 1HR program team on these actions.

SUMMARY OF WORK UNDERWAY IN FY 2018

A. Review of the Results Based Management (RBM) Initiative for Capacity Development (in progress)

19. The operationalization of Results-Based Management (RBM) is an integral component of the broader Capacity Development (CD) reform effort in the Fund. The implementation of RBM is intended to help the Fund: (i) monitor and evaluate the successes and failures of CD more effectively; and (ii) set priorities for resource allocation by firmly focusing CD on results.

20. The advisory review aims to support the Fund’s ongoing RBM implementation efforts. The overall objective of this advisory review is to draw lessons from the implementation experience to date - covering program governance, and systems aspects of the RBM effort, specifically for TA, which is the focus of the initial implementation – and highlight key considerations for the successful roll-out of RBM.

B. Review of Talent Acquisition (in progress)

21. As a knowledge-based institution, the Fund’s human capital remains its biggest asset, with an agile workforce central to the institution’s AIM agenda. At the request of HRD management, this advisory review supports the upcoming redesign of the Fund’s talent acquisition program in the context of the HR strategy and the modernization of HR processes and technology (1HR).

22. The objective of this advisory engagement is to review the effectiveness and efficiency of the Fund’s talent acquisition program in meeting the Fund’s needs as well as enhancing candidate experience, and to provide forward-looking recommendations based on leading practices. To support this objective, the review will examine various aspects of the talent acquisition program including governance, branding and sourcing, diversity, job posting, screening, selection, onboarding, and use of technology and analytics. The engagement will also review separately the governance, oversight, and working practices for the engagement of field-based capacity development experts, as well as short-term scholars and speakers.

C. Review of the Committee Structure for Risk Management (in progress)

23. A key priority for the Fund Risk Committee (FRC) and the Risk Management Unit (RMU) is to foster a stronger risk culture within the organization and facilitate further integration of risk management into the Fund’s operational fabric. With the establishment of the FRC, it will be important to clarify the roles and responsibilities of the various standing committees across the Fund (such as the Security Policy Group, Committee on Business and Information Technology) including vis-à-vis the FRC – to facilitate systematic, coordinated, and holistic risk oversight.

24. OIA’s advisory engagement is designed to support the efforts of the FRC and RMU - by undertaking a “stock-take” of the key management or staff-led standing committees and providing tailored recommendations to enhance the robustness of the overall risk architecture.

D. Review of the Fund’s Overseas Presence (planning underway)

25. The Fund’s overseas footprint is an important part of the member engagement strategy. The Fund’s primary business model for engaging members is to travel from HQ to conduct surveillance activities, negotiate Fund-supported programs, and deliver capacity development (CD). This model is supplemented by resident representatives and regional offices in selected countries, and technical assistance and training centers to bring the delivery of CD closer to the users.

26. This advisory engagement will cover the effectiveness of the operational and administrative mechanisms in place for supporting the Fund’s overseas presence. Likely areas of coverage include staffing and overseas mobility considerations, budget and financial administration, information technology support, physical security, and real estate arrangements.

NINTH PERIODIC MONITORING REPORT

27. OIA has commenced its preparation and review activities leading to the production of the Ninth Periodic Monitoring Report (PMR) on the Status of Management Implementation Plans (MIPs) in Response to Board-Endorsed IEO Recommendations. This will be OIA's fourth report, since it assumed responsibility (in 2014) to independently assess the progress of open management actions to implement IEO recommendations. The work is expected to be completed by end-February, and a final report is expected to be issued to the Evaluation Committee by end-March, 2018.

28. OIA has also published, on its website, an online repository of the population of IEO recommendations and related management actions. The repository is intended to provide Executive Directors and staff with a full view of the population of past IEO recommendations and their eventual disposition.

OVERDUE ISSUES

29. OIA issued its six-monthly "snapshot" report on overdue audit issues as at October 31, 2017 (see Appendix I). The snapshot report is designed to reinforce ownership of risk mitigation actions by client departments and heighten sensitivity to unmitigated risks and long overdue issues.

OIA INTERNAL ACTIVITIES

A. Program of Work for FY 2019

30. OIA has commenced its planning exercise to formulate its Program of Work for FY 2019, which is expected to be presented to the External Audit Committee (EAC) and Management by end-March 2018. The FY 2019 Program of Work, leveraging improvements to OIA's risk-based planning approach, will mark the first occasion where OIA's work plan will be fully aligned with the Fund's budget and strategic planning cycle. This will also enable OIA to more fully consider RMU's assessment of the Fund's risk profile and the priority risk mitigation directions endorsed by the FRC.

31. OIA will partner closely with client departments in delivering a body of work that is aligned with key institutional focus areas and priority risk mitigation themes. OIA will particularly focus on providing a more proactive and consultative perspective on risks with regard to operationalization of key strategic initiatives with a view to delivering timely and actionable insights.

B. FY 2019 Accountability Framework Deliverables

32. During FY 2019, OIA will continue the roll-out of its new reporting products (Insight Notes and Good Practice Series) by interspersing their issuance with OIA's traditional outputs. The new products are designed to promote greater risk awareness and support risk-informed decision-making.

33. Building on the momentum achieved in successfully leveraging data analytics to provide sharper insights, OIA will continue to focus on integrating data analytics into end-to-end engagement-level procedures.

C. Quality Assurance

34. During the second half of FY 2018, OIA will undertake an External Quality Assessment (EQA). International Standards for the Professional Practice of Internal Auditing stipulate that, “External assessments must be conducted at least every five years by a qualified, independent assessor or assessment team from outside the organization”. The EQA is designed to assess OIA’s conformance with professional auditing standards. The results of the EQA will be shared with the External Audit Committee (EAC) and summarized in OIA’s year-end Activity Report.

35. OIA has also focused on enhancing its Quality Assurance and Improvement Program (QAIP) to support operational efficiency and alignment with best practices. In this context, OIA has recently revamped its QAIP adopting a program-based approach to embedding quality into its operational processes and audit methodology.

ADMINISTRATIVE MATTERS

36. OIA expects to end FY 2018 at or above 98 percent of its overall budget allocation of \$5.0 million.

Appendix I. Report on Overdue Audit Issues as at October 31, 2017

Key Messages

This report presents an overview of outstanding and overdue audit issues. Since the issuance of the last report, OIA has closed one issue, and raised seven new issues, bringing the number of outstanding issues to 31 as of October 31, 2017. Of these 31 outstanding audit issues, 9 are overdue, representing a slight drop in the number of overdue issues since OIA's last report. Only one of the overdue issues is rated as "High" impact.

- Three new High impact issues have been raised in the audit of **Third Party Vendor Administration** covering: (i) the institutional governance for vendor management, (ii) risk assessment methodology and, (iii) monitoring and oversight of vendors.
- Three new High impact issues have been raised in the audit of **Fund System Development and Maintenance Processes** covering (i) institutional governance and mandate, (ii) design and enforcement of software development and maintenance standards and (iii) operational weakness in systems development life cycle processes.
- The High impact issue on the development of a holistic control framework to support the **administration of salaries and benefits** is significantly overdue. After several delays, due to capacity constraints and turnover in leadership, HRD management is now making progress on the foundational underpinnings for an effective solution. Early actions have focused on: the education of HRD leadership and line managers to create the right tone at the top, the development of interactive learning sessions to facilitate internal control conversations with HRD staff, and the appointment of internal control liaisons in divisions. Work is underway to: define delegated authorities, establish roles and responsibilities, and create awareness about the importance of reporting and escalating risk events. The longer-term sustainability of the Controls Program will require broad-based infusion of controls expertise and changes to culture, awareness, and work practices. The modernization of HR technology (1HR Program) should bring significant additional improvements.

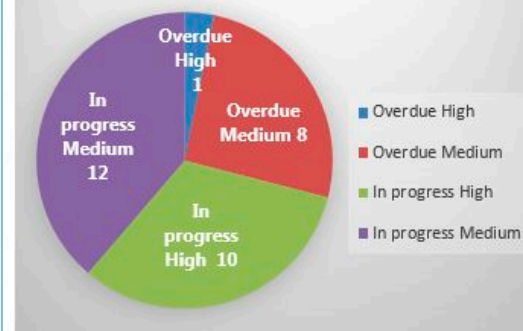
The following issues, rated as Medium impact, are flagged because they are long overdue.

- ITD has designed a risk-based plan for identifying, prioritizing and monitoring **Fund databases**, drawing upon the outcomes of the Information Categorization Pilot and leveraging existing risk-ranking mechanisms within ITD. While this issue is significantly overdue, work is currently underway to implement these measures by the end of FY 2018.
- ITD is in the process of operationalizing its detailed plans for holistically strengthening **software license management**. Comprehensive reviews have been conducted for specific licenses, and a funding request has also been submitted as part of the FY19 budget cycle to support implementation. Focus on timely execution of these plans will be crucial to avoid further slippage.

Figure 1. Overdue Audit Issues (past due date)



Figure 2. Outstanding Audit Issues



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.