FOR INFORMATION

EBAP/20/43

May 29, 2020

To: Members of the Executive Board

From: The Secretary

Subject: **Office of Internal Audit—FY 2020 Activity Report**

Board Action: Executive Directors' **information**

Publication: No, due to content sensitivity.

Additional Information: Ahead of the meetings with the External Audit Committee, OIA will be available on Tuesday, June 9, 2020 to answer questions on this Activity Report.

Questions: Ms. Onyango, OIA (ext. 30511)
Mr. Murugan, OIA (ext. 38132)

May 29, 2020

OFFICE OF INTERNAL AUDIT (OIA)—FY 2020 ACTIVITY REPORT

EXECUTIVE SUMMARY

This report provides an overview of OIA's activities in FY 2020. The report fulfills management's commitment to keep the Executive Board regularly informed on audit and control-related items.

In FY 2020, OIA has issued ten reports (including two draft reports) – four advisory reviews, five audits, and a Periodic Monitoring Report (PMR). The finalized reports cover: (i) Talent Acquisition; (ii) the Cost-Benefit Analysis (CBA) of the 1HR Program; (iii) the CBA of the Capacity Development Management and Administration Program (CDMAP); (iv) the Total Remuneration Analysis (TRA) methodology of the Comprehensive Compensation and Benefits Review (CCBR); (v) an audit of IT Infrastructure Managed Services, (vi) an audit of the HQ1 Renewal Program's Financial Management; and (vii) an audit of Quality Control Practices for CD Outputs. The Tenth Periodic Monitoring Report (PMR) was discussed by the Board in February 2020. The draft reports of two audits - the Fund's Overseas Presence, and the audit of SWIFT-related payment processes and systems – have been issued for departmental comments and are expected to be finalized by early June 2020.

Fieldwork is largely complete for an audit of the Fund's Enterprise Risk Management Framework, and preliminary findings and recommendations will be formulated by mid-June 2020. Field work for an audit of the Fund's Administration of the G-5 Program is in an advanced stage; work is also progressing on OIA's review of specific 1HR Program components (data migration, security & internal controls configuration).

OIA is adopting deliberate measures to align its FY 2021 work program and approach, in the context of the Fund's crisis response. As was the case in FY 2020, the modernization projects are expected to feature prominently in OIA's coverage for FY 2021. OIA is shortening its planning horizon to a 6-month timeframe - with a heavier proportion of advisory assignments - which will enable a more dynamic refresh of OIA's work program pipeline. OIA's semi-annual reports on overdue audit issues have continued to highlight the need for a sharper institutional focus on risk mitigation (currently there are thirty-two outstanding audit issues of which fifteen are overdue). The adoption of a revamped delivery model in FY 2019 has yielded significant productivity gains. OIA is completing the staffing of its vacant positions shortly, so that the Office can operate with a full staffing complement by the end of Q1 of FY 2021.

Approved By Nancy Onyango	Prepared by Office of Internal Audit

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 2020. The report includes a summary of the work completed during FY 2020; results of OIA's follow up work on outstanding internal control issues; and an overview of key internal OIA activities.

2.   On June 9, 2020, 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 2020 audit coverage to date with OIA staff.

OIA'S MANDATE

3.   OIA is an independent assurance and advisory function designed to protect and strengthen the Fund. The mission[1] 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 an advisor 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 IN FY 2020

A. Review of Cost-Benefit Analysis (CBA) of the 1HR Program (issued May 2019)

5.   OIA's FY 2020 Program of Work included scheduled reviews of the CBAs of the Fund's key business and digital modernization projects. The first such review covered the 1HR Program. OIA noted that the 1HR team had taken a systematic approach to factor in estimates of one-time and recurring costs, capturable benefits, and non-capturable benefits based on the best available information. OIA's memo outlined some considerations and key assumptions underpinning the 1HR CBA. Given that changes to the assumptions could have an impact on the estimated costs and benefits over the life of the 1HR program, OIA stressed the importance of updating the CBA on

---

[1] Source: OIA Charter (Approved in May 2017).

an ongoing basis, and to inform ongoing decision-making by the 1HR Steering Committee and the Committee on Business Information and Technology (CBIT).

B.   Advisory Review of Talent Acquisition (issued June 2019)

6.   **The review noted that the Fund's talent acquisition program has been broadly effective in meeting departmental hiring needs, but also identified several opportunities to enhance talent acquisition into the Fund**. The review provided forward-looking recommendations based on leading practices, and in the context of the HR modernization efforts. HRD is taking the findings of this review into account in configuring the redesigned talent acquisition processes for Workday in the 1HR Program. An important consideration, going forward, would be to fully leverage the capabilities and functionality of technology solutions so that the organization derives commensurate value from these investments.

C.   Review of Cost-Benefit Analysis (CBA) of the Capacity Development Management and Administration Program (CDMAP) (issued September 2019)

7.   **OIA's second CBA review covered the Capacity Development Management and Administration Program (CDMAP).** CDMAP aims to provide better information for strategic decision making and implementation in CD resource allocation; and strengthen integration of CD with surveillance and lending activities.

8.   **OIA concluded that the CDMAP team had adopted an inclusive and consultative approach in preparing the CBA**. The team budgeted for major program costs, including backfilled contractual resources and a small contingency for minor IT solution customization. Given the activity cost data limitations, the CDMAP team also adopted a reasonable approach in estimating capturable benefits from the program. OIA emphasized the importance of adequate data quality controls and sound data governance practices when designing the IT solution, to realize the intended strategic benefits of the program.

D.   Audit of IT Infrastructure Managed Services (issued September 2019)

9.   **This audit assessed the governance arrangements, processes, and controls over the transition of IT Infrastructure Managed Services to Larsen & Toubro Infotech (LTI), a key vendor for the Fund.**

10.   **While the audit found good control practices, the review also highlighted areas that needed to be strengthened to more robustly manage and measure service delivery, and to hold the vendor accountable**. Good control practices included strong contractual clauses, upfront security controls identification and design work, and the identification of Service Level Agreements (SLAs) upfront as part of the contract. The MSP arrangement has also yielded cost efficiencies (budget and staff reduction) for ITD, which was one of the key objectives of the transition. However,

the audit also noted specific areas of improvement: (i) change management; (ii) governance arrangements; (iii) service delivery metrics and controls around computation and validation of SLAs; (iv) the MSP's processes to identify root causes and implement risk mitigation measures for information security incidents, and issues pertaining to Identity and Access Management (IAM) raised in past OIA audits; and (v) monitoring of the MSP's obligations and commitments in a timely and effective manner. ITD provided detailed and time-bound action plans to address the issues noted in the report, with remedial actions that were targeted to be completed by end of FY 2020. These actions included: (i) missions to LTI's Extended Delivery Center (EDC), (ii) refresher training sessions on vendor management and monitoring, (iii) identification of quality metrics in addition to the SLAs, (iv) clarification of roles and responsibilities for information security risk management activities, and (v) formal sign-off from the Fund's Service Owners on a monthly basis for SLA breaches. Implementation actions, while significantly overdue, are also underway to address the IAM issues raised in past OIA audits, including: (i) the implementation of systematic IAM governance processes to review and address issues with current IAM processes and business rules; (ii) improving Privileged Access Management (PAM) controls; and (iii) the implementation of a new IAM solution to replace the current "home-grown" provisioning tool.

E. Review of CCBR Total Remuneration Analysis Methodology (issued November 2019)

11.   OIA's review of the Total Remuneration Analysis (TRA) component of the Comprehensive Compensation and Benefits Review (CCBR) was initiated in response to management's request for an independent validation of specific methodology questions related to the CCBR.

12.   OIA's overall conclusion was that the TRA methodology assumptions proposed and used by the CCBR external consultants provided a robust basis for benchmarking. This request was made in the context of the Staff Association Committee's concerns regarding the CCBR methodology. The TRA exercise is a quantitative comparison of the value of a portfolio of the "Fund's main salary and benefit programs" against a portfolio of the same or similar programs for the comparators. The review assessed the robustness of key methodology aspects used to develop the TRA. OIA also considered the results of additional "what-if" analyses, executed by the CCBR external consultants in response to OIA's requests, to specifically assess the impact of city-specific cost-of-living adjustments and childcare benefits on the TRA aggregate rollups for the comparator International Financial Institutions (IFIs). The results of these specific "what-if" analyses based on the assumptions made by the CCBR external consultants, indicated that there were no changes to the previously presented relative ranking of the Fund in the overall TRA comparison.

F. Tenth Periodic Monitoring Report (issued December 2019)

13.   The Tenth Periodic Monitoring Report (PMR) on the Status of Management Implementation Plans (MIPs) in Response to Board-Endorsed Independent Evaluation Office (IEO) Recommendations was issued in December 2019 and discussed by the Executive Board

in February 2020. The Tenth PMR covered ten MIPs. A companion paper to the PMR ("Categorization Paper") contained proposals for Board consideration for actions facing implementation challenges. Directors appreciated the accelerated pace of implementing management action plans in recent years and welcomed the proposal to categorize actions and the increased traction of IEO recommendations following the categorization process. In response to Directors' feedback, OIA will work with SPR and ORM, and in consultation with the IEO, to provide some proposals for consideration by the Evaluation Committee of the Board, on a framework for assessing the institutional impact of potential slippages in individual MIPs.

G.   Audit of the HQ1 Renewal Program's Financial Management (issued February 2020)

14.   **The audit assessed whether financial management controls implemented for the HQ1 Renewal Program were in place and functioned well through the course of the program**. The scope of the audit included all financial transactions through the end of FY 2019. The audit excluded an assessment of the technical aspects and quality of design, construction, and office fit-out work.

15.   **The construction phase of the HQ1 Renewal Program started on May 1, 2013 and reached substantial completion in September 2019, ahead of the Board-approved revised schedule and budget.** The Executive Board approved a budget of $563 million in two instalments in 2011 and 2015, to complete the renovation of the HQ1 building, as many building systems had exceeded their expected life after 40 years of use. Despite concerted efforts to minimize unexpected site conditions and events, the project ran into significant implementation challenges within its first two years and progress was significantly hampered. Those early challenges included: (i) The choice of implementation strategy did not take into full account major downside risk scenarios, especially for schedule and design changes; (ii) Inaccurate cost estimation, based on incomplete design drawings and accelerated planning, resulted in insufficient budget allocation; (iii) Unexpected (behind-the-wall) conditions and a flawed construction design led to design coordination issues; (iv) Improved asbestos protocols ordered by management at the start of construction and unexpected asbestos findings significantly impacted the schedule; (v) External lease space significantly exceeded the programmed estimates; (vi) Failures in the governance arrangements regarding delegation of operational responsibilities and escalation of issues.

16.   **By early 2015, the challenges had collectively reached a critical mass, triggering specific actions by the leadership to strengthen project management and enhance project oversight by establishing a new Task Force (HQT).** These organizational changes, accompanied by significant personal investment by the leadership, were largely responsible for ensuring that the project was completed within the revised schedule and budget.

17.   **The audit found that the financial management controls implemented for the Program were broadly adequate and functioned as designed, especially following the restructuring of the governance in 2015.** The audit found some control gaps in financial controls over contract management and invoice approvals, but also noted that the HQ1 Renewal Task Force's focus on

higher risk areas was appropriate – such as ensuring that the Task Force's resources were allocated towards efforts to minimize unwarranted large financial exposures to the Fund. Due to differences in interpretation of mandates, some large commitments (totaling $59.6 million) did not receive secondary reviews and approvals by the Task Force Review Team (TFRT), the body charged to provide secondary review of commitments above prescribed thresholds. The TFRT interpreted its role as a safeguard against unwarranted scope creep in contracted services, and in that context, did not consistently review certain large contracts exceeding established thresholds because they were not considered a significant variation in the scope of existing agreements. The lack of clarity around the use of task orders (as supplements to existing contracts) resulted in some procurement activities that were not aligned with the delegation of procurement authority that was established for the program. Controls over disbursements to the General Contractor, representing almost 70 percent of the cost of the program, worked well with minor exceptions. Similarly, the controls were effective in ensuring that costs were properly recorded, reconciled, and reported, in accordance with applicable accounting standards. While no corrective actions were necessary, the audit provided a few lessons that could be usefully applied to other large projects in the Fund.

H.   Audit of Quality Control Practices for Capacity Development (CD) Outputs (issued March 2020)

18.   **The objective of this audit was to assess the adequacy of administrative practices, processes, and procedures underpinning quality control of Fund Capacity Development (CD) mission outputs**. CD is a core activity of the Fund, representing slightly over 30 percent (or $306 million) of the Fund's total spending in FY 2019. Unlike the Fund's other core activities, CD is funded by Fund and donor resources, with donors financing over half of the CD spending. With wider dissemination, effective quality control of CD outputs is essential in safeguarding the Fund's reputation. The audit scope included CD mission outputs (both written and non-written) for CD delivery from HQ or Regional Capacity Development Centers (RCDCs), as well as on-line and face-to-face training. The audit excluded processes and outputs related to CD prioritization, Resource Allocation Planning, ex-post Evaluation, and Results-Based Management, as these processes have only recently been reformed.

19.   **The existing governance arrangements are largely adequate to ensure quality of CD outputs, and good practices exist in all CD departments.** While current policies and procedures for CD quality control are adequate for the majority of CD activities, they are mainly designed for the post-mission review of formal written outputs and do not take into full account the growing volume of non-traditional CD outputs. A quality control policy calls for all CD activities to be subjected to quality control and makes CD delivery departments responsible for the quality control of all CD services they deliver. However, quality control processes as currently designed are insufficient for handling the growing trend away from traditional CD outputs. CD is increasingly moving away from traditional post-mission reports (focused on "the what") to more of country-tailored advice on implementation (focused on "the how") with hands-on delivery through other innovative approaches rather than long-narrative reports. While no major concerns were observed, the audit found the

quality of review of written outputs to be uneven, especially for standalone expert-delivered CDs from RCDCs.

20.   **The audit identified four high-level recommendations to improve processes.** One, CD delivery departments should review the design of existing quality control processes, including the assignment of responsibilities and accountabilities, to include non-traditional outputs delivered from HQ and RCDCs. Two, CD delivery departments should review the design of existing quality control processes, including the assignment of responsibilities and accountabilities, to include non-traditional outputs delivered from HQ and RCDCs. Three, CD delivery departments should develop guidance, (e.g., training, templates, written guidelines, etc.) for experts on expected quality standards for CD outputs. Four, CD departments, in consultation with Area Departments, should clarify the roles and responsibilities of Area Departments in the quality control process for CD outputs. In response, CD departments will develop detailed implementation plans, with corresponding due dates in the next six months.

I.   Informal Advisory Work[2]

21.   **ICD management requested that OIA conduct a high-level advisory review to provide insights into the gaps between ICD Global Partnership's current and future business needs and the Capacity Development Information Management Systems (CDIMS), focusing on current capabilities.** OIA's advisory insights, shared with ICD in April 2020, stressed the need for business process harmonization and enhanced technology support for fundraising, budgeting, and reporting processes for externally funded CD. OIA also suggested sequential steps in the areas of governance improvements, business process redesign, and information technology optimization, as useful preparation to ensure that CDIMS is well placed for optimal technology enhancement and support in the long term.

22.   **In response to an ITD management request, OIA provided high-level insights on IT vendor management control practices across the lifecycle of the vendor's relationship with the Fund**. OIA's advice was intended to serve as an input to ITD in strengthening the role and activities of the Vendor Management Office (VMO). OIA's advisory inputs, provided in March 2020, covered all areas of the IT vendor management lifecycle - sourcing, procurement, contracting, on-boarding, monitoring, relationship management, and off-boarding. Also, as part of supporting ITD with the transition of a departing vendor, OIA has reviewed trends in monthly SLA reports and key personnel attrition metrics.

---

[2] OIA, in response to department requests, provides informal advice on specific areas, and the outputs are usually shared in the form of a short memo or a presentation – these interventions are designed to be quick, and not resource-intensive.

ENGAGEMENTS IN REPORTING PHASE

A. Audit of SWIFT-related Payment Processes and Systems (draft report issued May 2020)

23.   **The Fund has been using the SWIFT system since 2002 to send and receive requests for transfers of funds among various organizations worldwide.** SWIFT (Society for Worldwide Interbank Financial Telecommunication) provides a global network for financial institutions and other members to send and receive information about financial transactions in a secure, reliable environment. The SWIFT network does not process any transactions but rather relays formatted messages between its members with instructions regarding financial transactions or other business communications. Over 80 percent of Fund members use SWIFT to manage financial transactions with the Fund (approximately 22,000 messages annually).

24.   **This audit aimed to assess the governance, risk management, and controls over Fund payments made using the SWIFT infrastructure.** The audit covered related business processes at the point of creation of SWIFT messages and after release of messages, and the associated Information Technology (IT) systems. Fieldwork for the audit has been completed and draft conclusions are being validated with departments. A final report is scheduled for issuance in Q1 2021.

25.   **Several governance arrangements and controls are currently in place and have been strengthened since OIA's last audit of the SWIFT system, in particular through the addition of the service bureau, and the SWIFT Customer Security Program (CSP).** However, the SWIFT-related payment processes and systems should be subjected to the highest control standards, particularly recognizing that SWIFT has been identified as one of the Fund's Crown Jewels. Also, leading industry practices around SWIFT have been significantly upgraded in recent years reflecting a series of attacks on SWIFT systems around the world, and the heightened information security risks that organizations are facing; the Fund's ability to conduct transactions is also dependent on the security and reliability of counterparts' arrangements for SWIFT in the current COVID-19 context.

26.   **A draft report has been issued with specific recommendations to further enhance the robustness of controls.** Specific recommendations have been made to improve controls in the areas relating to: (i) periodic review and update of system configurations; (ii) process and technical documentation; and (iii) information security controls (e.g., firewall rules, encryption, authentication). It would be important to ensure that the improvement efforts to strengthen the control environment are guided by a risk assessment exercise that balances the required level of risk mitigation against the associated costs. The report is being finalized for issuance by early June 2020.

B. Audit of the Fund's Overseas Presence (Report being finalized for issuance)

27.   This audit was designed to assess the adequacy of the existing governance arrangements and controls relating to the administration of the Fund's field offices. It covered the following areas: (i) local employment; (ii) physical security, including business continuity; (iii) IT support including local IT service contracts; (iv) budget and financial administration; and (v) real estate operations. Fieldwork for the audit included a combination of testing and interviews at Fund's HQ; field visits; audio/video conferences for a sample of locations; and a structured survey – which was sent to all field offices.

28.   Since 2005, the Fund has decentralized the implementation of administrative support policies to area departments and to the field offices. The audit noted that this well-intentioned decentralization effort has however not been underpinned by a sufficiently robust "administrative infrastructure" - of institutional policies, procedures, systems, central oversight, clear delineation of roles, and compliance mechanisms – that can help drive consistency of practices across field offices, and act as an enabler and a guardrail for the effective conduct of decentralized field office operations. The absence of a sufficiently robust administrative infrastructure to guide a decentralized field presence model has contributed to several challenges. These challenges collectively pose reputational risks, increase administrative inefficiencies, and impede institutional agility in delivering support services to field offices.

29.   Several institutional initiatives are already underway to strengthen the current administrative mechanisms and address gaps. These include: HRD-led efforts to improve the local employment framework, FIN's efforts to streamline operations through system enhancements and banking arrangement improvements, CSF's efforts to implement the field security recommendations from the 2017 external consultant review, ICD's review of RTAC policies and procedures, and ITD's project for infrastructure refresh at field offices. It is imperative that these ongoing initiatives be sequenced, implemented, and monitored as part of a "top-down package of measures" aimed at ensuring sustainable and effective operation of the Fund's field presence. This will help prioritize, sequence, and coordinate implementation of these measures through a combination of short-term and longer-term measures. The report is being finalized for issuance by early-June 2020.

C. Audit of the Fund's Enterprise Risk Management Framework (Fieldwork largely completed, reporting underway)

30.   The objective of OIA's audit is to assess the effectiveness of the Fund's risk management framework and processes, particularly in the context of fostering greater integration of risk management activities into strategic and day-to-day decision-making. Specifically, the audit will evaluate the processes that underpin the identification, assessment, management, aggregation, and reporting of Fund-wide risks, from an ERM perspective.

31.   The scope of the audit will encompass the ERM components that are central to the effectiveness of the Fund's risk management framework: governance, methodology, risk responses, and reporting. The audit scope specifically includes:

- governance and accountability arrangements for defining and implementing the Fund's enterprise risk management framework;

- mandate, positioning, and staffing of the Office of Risk Management (ORM);

- methodology to support effective Fund-wide risk assessment, remediation, and monitoring, including: the adequacy of the Fund's risk register, the definition and application of the risk areas and risk lenses, the adequacy and level of granularity of Board-endorsed risk acceptance statements, and the processes supporting ORM's assessment of the risk areas (relative to Board acceptance) liaising with first line departments.

- tools developed by ORM for the purpose of identifying, measuring and reporting significant risks (e.g., risk event reporting framework, Fund@risk surveys, risk policies and procedures);

- adequacy and effectiveness of risk mitigation efforts

- relevance of risk reporting in terms of the adequacy and usefulness of risk information to support effective oversight and decision-making by key stakeholders.

The audit findings and recommendations will also be informed by an analysis of the decision-making procedures relating to the Fund's Exceptional Access Policy for lending operations. The audit is also drawing on the participation of qualified external experts and practitioners.

32.   The fieldwork phase of the audit is largely complete. This includes: (i) documentation reviews and process walkthroughs; (ii) stakeholder interviews; and (iii) surveys and benchmarking (including discussions with Chief Risk Officers of some comparator and private sector organziations). The audit is also seeking to leverage best practice guidance from a variety of sources, but duly tailored to the Fund's context. The reporting phase is being approached in two parts: (i) An initial debriefing of key findings and recommendations (targeted for mid-to-late June); and (ii) the development of a draft report by end-June, and finalization by August/September.

ENGAGEMENTS IN FIELDWORK/PLANNING PHASE

A. Administration of the Fund's G-5 Program

33.   The G-5 nonimmigrant visa program by U.S. Department of State (DoS) enables employees of international organizations in the United States to employ foreign workers for in-home domestic work. Full-time Fund staff with valid G-4 visas are eligible to participate in the Fund's G-5 domestic worker program (Program) and can employ G-5 domestic workers (tied directly to their G-4 visa status). The DoS imposes conditions and restrictions for the Program and has

consistently communicated the high priority it places on the fair and equitable treatment of domestic workers. To ensure this fair and equitable treatment, a contract between the G-5 domestic worker and his/her G-4 employer is required and must contain certain prescribed elements, at a minimum. As of August 2, 2019, the Fund had 141 G-4 staff employing 142 G-5 employees; one employer had two G-5 employees.

34.   In recent years, the DoS has tightened its oversight of the Program, increasing the scrutiny on international organizations such as the Fund. On August 2, 2019, the DoS requested that the Fund conducts an internal review of all active G-5 employment relationships. The two-fold purpose of the request was to determine: (i) whether domestic worker employment contracts include all required terms found in the Department of State contract template; and (ii) whether these contracts were amended in a timely manner over the past three years to include the correct minimum wage, and whether the workers were paid accordingly.

35.   OIA assisted HRD with the internal review in response to the DoS request, which was completed in December 2019. The review concluded that: 23 out of 142 contracts were not in compliance with the required terms contained in the DoS template; and 22 out of 142 domestic employees were not always paid the correct prevailing wages over the past three years. In more than half of the contract non-compliant cases, the operating employment contracts had become outdated as they had not been revised to reflect changes introduced in newer contract templates. In about half of the wage non-compliant cases, the G-4 employers delayed in adjusting the applicable wages following increases in minimum wage in their domicile County or State, citing the lack of knowledge of those changes. In other cases, the G-5 domestic employee did not receive the full wages for hours worked due to computational errors. All domestic workers have since been paid the back wages due. HRD has also introduced new measures to prevent the recurrence of these issues, including a March 2019 requirement for all employers of domestic workers to use of an external payroll services vendor that would also provide guidance on compliance with wage requirements. On December 3, 2019, HRD reported the results of the review to the DoS, along with the corrective actions taken to address all the findings.

36.   OIA is currently in the process of completing a broader audit to assess the effectiveness of the Fund's administration of the G-5 Program as a whole, including the governance, compliance, and administrative mechanisms in place to manage risks. The scope of the audit covers G-5 program activities over the past three years, and includes: (i) the governance, accountability, and oversight structure - including delineation of roles and responsibilities among the various stakeholders of the program; (ii) policies, procedures, and processes that support the operations of the program; (iii) control and compliance mechanisms, including the processes for identifying, escalating and resolving issues, and mitigating risks related to the program; and (iv) the availability and use of technology/systems to support the administration of the program. A final report is now expected to be issued in Q1 2021.

B. Review of Data Migration of 1HR

37.   The 1HR program is a transformation of the Fund's Human Resources (HR) processes and systems with the goal to modernize, simplify, and automate HR business processes. The 1HR technology solution implementation involves three main applications/platforms – Workday HCM and ServiceNow applications, and other custom applications on the Microsoft Azure platform. There are also integrations with, and dependencies on, other applications such as the Corporate Data Warehouse (CDW). The program is a multi-year, multi-phase initiative. Phase 1, which started in the Fall of 2017, focused on process redesign and planning. Phase 2, which started in the Spring of 2018, is focusing on the implementation of new, integrated, and modern technology solutions. The "go-live" dates for systems implementation are staggered – Release 0 was launched in March 2020, Release 1 is scheduled for September 2020, and Release 2 is currently planned for December 2020. Data migration from the Fund's legacy systems (PeopleSoft and other applications) involves a fundamental reorganization of HR data and their relationships to the systems and the environments in which they will operate in the future.

38.   The objective of OIA's review is to provide assurance on the reasonableness of the approach, processes, and controls implemented for the migration of HR data from legacy systems through the entire lifecycle of the 1HR implementation. The review covers the effectiveness of the data migration strategy, the governance, conversion (gathering, cleansing, transformation, loading, and validation etc.), and testing of the functional use of the data within the new environment. The review also includes the processes and assumptions being used to ensure that the data conforms to attributes such as relevance, accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, and compliance. OIA is adopting an approach that allows for deliverables at pre-agreed stage gates to ensure that outcomes can be considered timely and prior to the release and use of different modules of the systems. Work related to the Release 1 is well underway, and the review for Release 2 is expected to be completed in December 2020.

C. Review of Security, Risk and Control Considerations of 1HR

39.   OIA's 2014 audit of the administration of salaries and benefits found significant weaknesses in the design and operating effectiveness of controls, highlighting the lack of capacity in HRD to implement robust internal controls and the complexity of the Fund's compensation and benefits system as major contributing causes. To find sustainable solutions to the issues identified in the audit, HRD began several mitigation activities, including the development of an integrated internal control framework, based on a 4-level maturity scale, which was endorsed by Management in February 2020. Achievement of level 2 on the maturity scale is expected in 2021, with the configuration of controls within the redesigned business processes as part of the 1HR program. HRD has hired external experts to work with HR business owners in documenting and quality-reviewing reconfigured end-to-end business processes in the new technology solutions.

40.   OIA's review will provide assurance on the design and implementation of the internal controls for HR processes as part of the 1HR solution implementation. This review will focus on providing assurance on the design of controls in two broad areas:

- *Business Process Risks and Controls* - Assess the design and implementation of process-level controls (as configured within Workday, Microsoft, Azure, ServiceNow, and the related manual processes) to ensure that all significant risks have been identified and properly mitigated; and

- *Security Policies and Access Controls* - Examine the security policies developed for access to Workday, SNOW, and Azure; and confirm the adequacy of controls over security groups configuration and related permissions, including access rights and the ability to initiate/approve business transactions in accordance with the related security policy.

41.   OIA will be adopting an approach that allows for deliverables at pre-agreed stage gates to ensure that outcomes can be considered timely and prior to the release and use of different modules of the systems. Planning activities for this review are currently underway, and the review is expected to be completed with the final release of 1HR in December 2020.

OVERDUE AUDIT ISSUES

42.   OIA issued its six-monthly "snapshot" report on overdue audit issues as of April 30, 2020 (see Appendix I). The report notes that timely mitigation of identified control gaps remains a challenge. Of the thirty-two outstanding audit issues, fifteen are overdue, of which eight are rated "High" impact. The overdue issues flagged in this report pertain to: (i) the development of a holistic HR Control Framework; and (ii) enhancement of several critical controls relating to Identity and Access Management (IAM), Privileged Access Management (PAM), and monitoring of IT Infrastructure Managed Services.

43.   As OIA has noted in prior snapshot reports, the institution will significantly benefit from a sharper focus on timely risk mitigation, particularly recognizing that the risk profile is not static even as mitigation efforts are underway. OIA's analysis of "high-impact" rated issues raised during the last four years indicates that many of these issues have remained overdue for significantly long periods of time. OIA's analysis also indicates that none of the "High" impact rated issues were actioned within the originally envisaged target implementation dates.

OIA INTERNAL ACTIVITIES

A. Program of Work for FY2021

44.   OIA is formulating its Program of Work for FY 2021 against the extraordinary backdrop of the Fund's ongoing crisis response to support membership needs. OIA is adopting deliberate measures to align its work program and approach with the institution's efforts to support membership needs in dealing with the impact of the COVID-19 pandemic. In particular, OIA is

intending to shift its FY 2021 work program planning horizon from 12 months to 6 months – the pivoting of the planning horizon to a 6-month timeframe will allow OIA to embrace short-term prioritization and more frequent review/updates to the work program to mirror the changing pace of risk and assurance needs of the Fund.

45.   Recognizing that several "in-train" corporate initiatives will still need to proceed given their foundational nature, OIA's focus will be on providing advisory support to key internal projects and initiatives (such as the modernization programs). OIA will also defer engagements that would place an undue burden of departments directly engaged in crisis response work. OIA's FY 2021 Program of Work is expected to be circulated for management approval by end-May, following inter-departmental review and consultation.

B. OIA Delivery Model and Staffing

46.   During the past year, there has been a deliberate focus to optimize the use of OIA's existing resource envelope by focusing on productivity improvements, while preserving the quality and impact of OIA's outputs. The productivity gains achieved (outputs for FY 2020 have more than doubled in comparison to FY 2019) are in large part, to a revamped delivery model that the function has embraced – one that provides senior audit staff greater opportunities to demonstrate their technical and leadership competencies. OIA is also looking to complete the staffing of its vacant positions so that the Office can be fully staffed by the end of Q1 of FY 2021. Recruitment is also underway for the replacement of one of OIA's Audit Managers who has recently moved to the Office of Budget and Planning (OBP).

OFFICE OF INTERNAL AUDIT

REPORT ON OVERDUE AUDIT ISSUES

AS OF APRIL 30, 2020

Key Messages

This report presents an overview of outstanding and overdue audit issues. Since the issuance of the last report, OIA has raised four new issues bringing the number of outstanding issues to thirty-two as of end-April, 2020. Of these thirty-two outstanding audit issues, fifteen are overdue, of which eight are rated as "High" impact.

The status of the overdue issues rated as "High" impact is as follows.

➢ The "High" impact issue on *the development of a control framework* (originally due on April 30, 2015) to support the **administration of salaries and benefits** is being addressed, in part, through the solution configuration for the 1HR program, which is ongoing. In February 2020, Management endorsed HRD's integrated internal control framework, which is based on a 4-level maturity scale. Achievement of level 2 on the maturity scale is expected in 2021, with the configuration of controls within the redesigned business processes as part of the 1HR program. Post-1HR activities aimed at sustaining the control framework have also been identified by HRD. OIA plans to audit the effectiveness of this internal control framework, once the desired maturity threshold (Level 2) is achieved through the implementation of the 1HR program.

➢ Projects are underway to address the three key issues noted in the Fund's **Identity And Access Management (IAM)** controls. This includes: (i) *implementing systematic IAM governance processes* to review and address issues with current IAM processes and business rules (originally due on April 30, 2018); (ii) *improving Privileged Access Management (PAM) controls* – including the implementation of a new PAM tool (originally due on April 30, 2019); and (iii) the *implementation of a new IAM solution* to replace the current "home-grown" provisioning tool. The IAM projects and control enhancements are a pre-requisite to the Fund's business and digital modernization programs, and so significant delays in implementation going forward could have risk implications for the modernization projects. The IAM and PAM initiatives are part of the initiatives defined in the Information Security roadmap, which now spans a time horizon of Q3 FY21 to early FY24.

➢ *An Information Systems Management Policy*, which will govern **systems development and maintenance** (including for business-led initiatives), was approved by Management and issued to Departments in February 2020 (originally due on January 31, 2018); OIA will monitor, during FY21, departments' awareness, and adoption of the requirements of this new policy. The second overdue item relates to *The Integrated Project Lifecycle (IPLC) framework*, which presents the minimum expected standards for systems development and maintenance, has also been updated to reflect current practices. An ITD-led working group is now planning on strengthening the IPLC framework (originally due on November 30, 2017) in the context of ITD's new operating model

➢ Two additional "High" impact rated issues have become overdue in this reporting period. These pertain to critical **IT infrastructure managed services** issues covering: (i) *change management efforts;* and (ii) *information security risk management* (both originally due on January 31, 2020). Given the increased use of Managed Service Providers (MSP) within the new IT operating model, these overdue issues become even more critical to remediate in a timely fashion in the context of maintaining robust monitoring controls over an expanded set of service providers who are likely to have access to sensitive Fund systems and information.
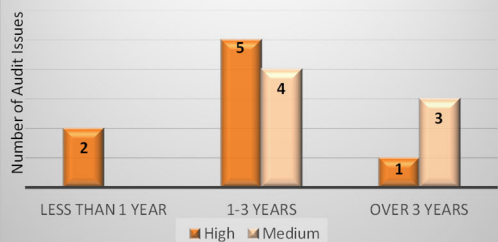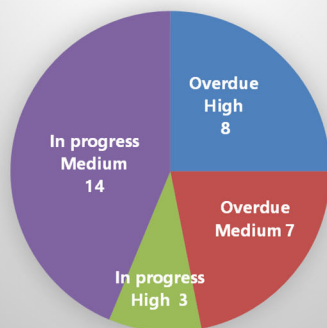
Figure 1. Overdue Audit Issues (past due date)

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.

"...protecting and strengthening the Fund..."