



# Quarter 3 Activity Report

FISCAL YEAR 2018

INTERNAL AUDIT VICE PRESIDENCY

As of April 24, 2018

# Contents

<b>Quarter's Engagements</b>	<b>3</b>
<b>ANNEX: List of Engagements in the FY18 Q3 Activity Report</b>	<b>12</b>

## About IAD

The Internal Audit Vice Presidency (IAD) is an independent, objective assurance and consulting activity that helps to improve WBG operations. It assists the institution in accomplishing its objectives by evaluating the effectiveness of WBG governance, risk management, and control processes. Furthermore, IAD advises management in developing control solutions, and monitors the implementation of management's corrective actions.

IAD's work is carried out in accordance with the Institute of Internal Auditors (IIA) International Professional Practices Framework.

IAD's Quarterly Activity Report summarizes IAD's engagement results for the quarter.

[www.worldbank.org/internalaudit](http://www.worldbank.org/internalaudit)

## Quarter's Engagements

### 1. Audit of WBG's Enterprise Desktop Management and Security

The objective of the audit was to assess whether the governance, risk management, and control activities over the design and deployment of WBG's Enterprise Desktop (ED) provide reasonable assurance that:

- The strategy and objectives have been defined, implemented, and monitored to enable a consistent, secure, and reliable desktop environment;
- The ED10 image\* development, deployment, and ongoing security-monitoring processes have been conducted in a secure manner to ensure the confidentiality and integrity of the ED environment and data; and
- Defined processes are in place to ensure that the ED environment is available and adequately supported to enable the productivity of WBG staff.

The audit concluded that the system of internal controls over the planning, design, testing, deployment, support and maintenance activities for ED10 provides reasonable assurance that the WBG's Enterprise Desktop is managed and secured effectively. The ED security posture has been augmented by more advanced controls in Windows 10 compared to Windows 7 to protect the ED10 environment from evolving system vulnerabilities. Moreover, end-user support, training, and awareness were effective, along with measures to ensure the continued availability of the ED10 environment.

However, IAD identified key issues relating to lack of adherence to established ITS risk management processes during ED10 security implementation, and the need for data protection technical controls at the ED level.

\*The ED10 image includes Windows 10 and the core software and productivity tools used by WBG staff.

### 2. Audit of WBG's Wireless Network Management and Security

The objective of the audit was to evaluate the adequacy and effectiveness of the WBG's wireless network security, particularly to determine whether: (i) policies and standards on the use and deployment of wireless networks were defined and up-to-date to provide adequate guidance for managing and securing the WBG wireless network; (ii) the wireless network architecture and infrastructure were designed and implemented to safeguard the confidentiality, integrity, and availability of critical WBG data assets; and (iii) risk management processes and controls were designed and implemented to enable effective identification, mitigation, and reporting of existing and emerging network threats.

The audit concluded that the system of internal controls over the WBG wireless network, which encompasses governance processes, architectural design, technical configuration, and security management and monitoring capabilities, provides reasonable assurance that the WBG wireless network is appropriately managed and secured. Effective practices were also noted around the support, maintenance, and management of the wireless network environment, based on established standards and procedures.

However, in order to maintain a satisfactory control environment for the wireless network, opportunities for further strengthening were identified in the areas of intrusion detection and prevention, vulnerability management, policy and guidance, and the guest wireless access and acceptable use policy.

### 3. Audit of WBG's Corporate Procurement Processes

The objective of the audit was to assess the governance, risk management, and control framework in place to ensure that WBG procurement activities achieve value-for-money for the institutions. Specifically, the audit assessed whether: (i) WBG corporate procurement and contracting strategies are designed to achieve value for money; (ii) vendor performance is assessed and monitored against business requirements and agreed deliverables; and (iii) post implementation reviews are performed to extract best practices and lessons learned that can be used to inform the development of future procurement and contracting strategies.

The audit concluded that the foundation has been successfully laid for a sound governance, risk management and control framework to ensure that WBG procurement activities achieve value-for-money. Implementation of category management has been initiated and dedicated category teams have been established to support internal business units' needs. For key procurement projects, strategies have been developed to extract optimal outcomes, which are reviewed by relevant procurement committees, and efforts have commenced to rationalize the number of vendors and channel procurement spend to preferred or contracted vendors, thus reducing associated vendor administration costs.

However, opportunities for further improvement exist in several areas to ensure that the nascent measures are embedded into existing business processes and implemented in a sustainable manner. These areas include (i) Category Management and Demand Aggregation – to ensure category management is carried out consistently across all categories and a systematic process is established to routinely extract procurement demands across the WBG institutions; (ii) Vendor Performance Management – to ensure consistency in performance management practices for all vendors, rather than just high-risk high-spend vendors; and (iii) Post-Award Contract Reviews – to ensure post-award reviews are performed for all procurement contracts above US\$1 million.

### 4. Advisory Review of Management of Shared Service Agreements (SSAs) among WBG Institutions

The objective of the advisory review was to identify opportunities for improvement in the management of SSAs among WBG institutions. The aim was to foster a more rational, transparent, simpler and leaner approach that better meets the needs of WBG institutions, ensures reasonable cost attribution across institutions, and maximizes value for money for each institution, while recognizing the need for WBG entities to work in partnership in supporting the WBG's overall strategy. IAD's review focused on organization and governance; cost analysis; continuous improvement; and performance management.

The advisory review noted that implementation of the suggested SSA approach, with the clear objective of supporting more streamlined and simplified SSA processes, will require strategic and managed transitional arrangements. This will entail Executive Sponsorship from the Senior Management of each WBG institution, and buy-in from Service Providers and Recipients.

The key recommendations from this review included: (i) development of a typological approach to classify services; (ii) formulation of a directive to harmonize the essential elements for establishing and monitoring SSAs; (iii) alignment of SSA processes with the Budget process to make business planning more effective; (iv) introduction of the structured management of SSAs by outlining the mechanisms that will be followed for each SSA; (v) provision of guidance on how service recipients or providers can withdraw from services; (vi) development of a better costing approach based on service type; and (vii) improvement of performance monitoring through the development of mutually agreed performance management practices.

## 5. Special Review of the Administrative Expense Transactions Managed by Executives' Front Offices in the WBG Institutions

The objective of the special review was to assess the adequacy of existing controls and institutional oversight arrangements for the use of administrative expenses by World Bank Group (WBG) Executives. Specifically, the review (i) assessed the design and effectiveness of the governance and control framework related to the administrative expense transactions managed by Executives' front offices; (ii) examined the institutional reporting arrangements and assessed the effectiveness of such arrangements in ensuring the proper monitoring and appropriate resolution of identified irregularities; and (iii) identified areas for improvement.

IAD's review concluded that the control framework to manage and oversee administrative expense transactions managed by Executives' front offices provides reasonable assurance that expenses are incurred for business reasons. No instances of misuse of funds or non-compliance with institutional policies were found. Key factors contributing to this assurance are:

- **The existing policies and guidelines** clearly define what constitute valid business expenses and provide criteria for determining an allowable or unallowable expense. They also contain clear delineation of responsibilities for approving managers, budget holders, and their delegates, and define expense substantiation requirements to pay allowable business expenses.
- **The expense approval and review process** enhances the likelihood that travel expenses are incurred for valid business reasons. Not only does business travel have to be pre-approved, but the system is designed to prevent Executives from approving their own trips and expenses. Further, reviews are performed within each unit and by the Accounting and Business Services (WFAAB) team in Chennai (for reimbursements greater than \$5,000).
- **Quality Assurance (QA) reviews** of WBG Executives' expenses are conducted by WFAAB through sample testing of expense transactions. They highlight areas of control weaknesses and prompt management response aimed at addressing such weaknesses, thus strengthening the overall control environment.

Opportunities for further strengthening included instituting measures to: (i) accurately assign and periodically review the set-up of SAP approval profiles to ensure they are appropriate; and (ii) enhance the monitoring and reporting of Executives' administrative expenses.

## 6. Special Review of the WBG Administrative Expense Transactions of Executive Directors' Offices

The objective of this review was to assess the adequacy of existing controls and institutional oversight arrangements related to the utilization of administrative expense transactions incurred by Board Officials. Specifically, the review (i) assessed the design and effectiveness of the governance and control framework adopted by the Corporate Secretariat in the oversight of the administrative expense transactions of Executive Directors' (EDs') Offices; (ii) examined the reporting arrangements for the administrative expense transactions of EDs' Offices, and assessed the effectiveness of such arrangements in ensuring the proper monitoring and resolution of identified irregularities, if any; and (iii) identified areas for improvement.

IAD's review concluded that the control framework to manage and oversee administrative expense transactions for Board Officials provides reasonable assurance that expenses are incurred for business reasons. No instances of misuse of funds or non-compliance with institutional policies were found. Key factors that contribute to this conclusion are:

- **The expense policies and guidelines** serve the dual purpose of providing EDs' offices with clarity on what expenses are generally deemed appropriate and functioning as a reference to help direct expense approvers in the execution of their responsibilities.
- **The expense review and approval processes** ensure compliance with applicable policies and guidelines.
- **Monitoring and reporting practices**, including periodic and ad hoc reports to the EDs' offices for all fixed and variable expenses, enable EDs' offices to review and monitor their expenses.

However, opportunities for further strengthening include closer monitoring of administrative expenses, especially travel related expenses, through enhancements to the existing semi-annual reports on Board administrative expenses.

## 7. Assurance Review of the Bank's Implementation of the Uganda Transport Sector Development Project (Additional Financing): Lessons Learned and Agenda for Action

The objective of the assurance review was to provide independent validation of the implementation of management's action plans committed to in the November 2016 report on the *Uganda Transport Development Sector Project (Additional Financing) (TSDP-AF): Lessons Learned and Agenda for Action*. The results were also intended to inform management of the areas that may require additional attention during implementation of the Environmental and Social Framework (ESF). The scope of the review included all the action plans with target implementation dates of December 31, 2017 or earlier. Two action plans were targeted by management to be completed in January 2018, and thus were excluded from the review.

IAD validated that management has completed the implementation of 30 of 39 actions, 2 are ongoing as they relate to the ESF implementation that is currently being rolled out, 5 were deemed partially completed, and 2 were out of the scope of the review. The actions for the partially completed items are considered ongoing in nature and relate to processes covering staff training and development of guidance.

Key features of management's accomplishments include (i) improved processes for oversight and monitoring of high-risk projects; (ii) development of relevant guidance notes, and extensive communication with staff; (iii) training on risk assessment and other key areas; and (iv) implementation of automated controls.

IAD observed that, during the ESF implementation, management could increase its attention to cross-cutting themes including: (i) monitoring the staff guidance and instruction developed through the action plan; (ii) analyzing whether training courses have fully reached their intended audience; and (iii) improving the accessibility of the procedures, policies, and guidance.

## 8. Audit of the Bank's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Program

The objective of the audit was to evaluate the controls for managing the risks in meeting the objectives of the AML/CFT Program pertaining to money laundering and financing of terrorism risks. Specifically, the audit reviewed (i) governance and oversight arrangements for establishing and updating the AML/CFT program, establishing workflows, and providing implementation support including system tools and training; (ii) the implementation of the Program, including the screening process, business process workflows, and quality assurance arrangements; and (iii) monitoring and reporting to Senior Management on implementation of the Program.

IAD concluded that the governance, risk management and control activities over the establishment, operationalization, and monitoring of the Bank's new AML/CFT Program are satisfactory. The Bank has assessed the applicability of the Financial Action Task Force recommendations, and identified and adopted the relevant recommendations to ensure continued compatibility of the Program with international standards. A Steering Committee provided oversight throughout the design and implementation of the new Program, while a dedicated AML/CFT team has strengthened the Program's governance.

The AML/CFT team performed a comprehensive institution-wide AML/CFT risk assessment during the implementation of the new Program, which identified the risks/gaps inherited from the previous program and informed the design of the new program. As a result, the Bank's screening process has improved significantly. Other improvements in the new Program include enhanced due diligence process workflows to be followed in case of a hit; implementation of a quality assurance program; monitoring of the Program by the AML/CFT team through weekly and monthly reports; provision of semi-annual reports to Senior Management; and establishment of an escalation mechanism.

## 9. Audit of Implementation of SORT in Supporting Operational Decision-Making

The objective of the audit was to assess whether the Systematic Operations Risk-rating Tool (SORT) has been implemented as planned and is being used according to the objectives envisioned in the Bank's Framework for Management of Risk in Operations. Specifically, the audit evaluated whether (i) risks are captured systematically and consistently across the Bank's operations and recorded using SORT; (ii) SORT risk information is used at key decision points in the project life cycle, including by the Regions and GPs; (iii) SORT risk information is used to prioritize management attention and resources at the portfolio level; and (iv) SORT is periodically reviewed as a risk management tool with occasional updates to the Board on its implementation. IAD noted that there are established systems of risk monitoring and management by staff and management outside of SORT, but these were not covered in the audit.

IAD concluded that SORT is well established as a risk recording tool within the broader framework for management of risks in Bank operations. SORT risk ratings are embedded in all mandatory project documents and the recording of risk is fully implemented for all active operations. It is used as an input for framing the risk conversation among stakeholders during project preparation, and the risk ratings help determine the project approval track. SORT risk data is available in an aggregated form in the standard reports and is included in key corporate reports. The Strategy, Risk, and Country Community Unit coordinates and monitors the implementation of SORT, analyzes the emerging data trends, and oversees the system's enhancements.

However, IAD noted gaps in the shared understanding of the strategic purpose and positioning of SORT by the key stakeholders, i.e., staff, management, and the Board. This could adversely affect the reliability of SORT information for decision-making on the risks in operations in the long term. It has also led to opportunities for improvement in SORT implementation in the following areas: (i) use of risk information in SORT during project supervision; (ii) use of risk information in SORT in portfolio monitoring and management; (iii) reporting of risk information in SORT to the Board; and (iv) review and assessment of SORT implementation.

## 10. Audit of Bank's Process for Managing Advisory Services and Analytics Activities

The objective of the audit was to assess the effectiveness of controls introduced by recent reforms to address the earlier identified weaknesses over the delivery of Advisory Services and Analytics (ASA) activities. In particular, the audit sought to provide assurance on whether (i) the initiation of new ASA activities is controlled to be selective and kept within the delivery capacity; (ii) the quality of ASA activities is reviewed at entry and throughout the lifecycle; (iii) problems in activities are systematically identified and addressed for early resolution; and (iv) delivery is monitored and reported to Senior Management and the Board for strategic discussion and decisions. The audit covered the entire lifecycle of ASA activities including initiation, implementation and completion.

IAD noted several significant improvements in the management of ASA activities following the implementation of ASA reforms. Specifically, the ASA Accountability and Decision-Making (ADM) framework has been embedded into the ASA workflow in the Operations Portal, which ensures that ASA activities are approved by the appropriate decision-makers; ASA portfolio indicators, including the portfolio capacity and the delivery indicators, have been developed and are being used to monitor the ASA portfolio size, delivery, and expenditures; and the delivery of ASA activities and ASA expenditures are reported to Senior Management and the Board on a periodic basis.

However, IAD identified several gaps: (i) problems identified in ASA activities are often not resolved in a timely manner; (ii) there is no substantive analysis of the reasons why certain activities are dropped and of the related costs incurred; (iii) a number of ASA activities funded by Bank-executed Trust Funds are not planned through the institutional Work Program Agreement (WPA) process; and (iv) the criteria for the selection of peer reviewers have not been clearly defined.

## 11. Audit of Oversight of Administrative Expenses Managed by Bank's Country Offices

The objective of the audit was to evaluate the design adequacy of the oversight of administrative expenses managed by the various WBG business units, especially those related to Country Offices (COs). Specifically, the audit focused on assessing whether (i) roles and responsibilities are clearly assigned to various units across the WBG institutions to enable sufficient oversight of the use of administrative funds; (ii) the design and implementation of oversight activities related to the use of administrative funds are adequate; and (iii) the arrangements for the reporting of oversight results, management's follow-up on corrective actions, and dissemination of lessons learned for continuous improvement are sufficient. The scope of the audit covered the Bank's COs, but excluded IFC's COs and MIGA's hubs.

IAD concluded that multiple functions perform ex post monitoring and reporting on compliance with policies to mitigate the risk of misuse of funds in COs and improve internal controls. The Quality Assurance (QA) Program of WBG's Finance and Accounting, Accounting Business Services (WFAAB) includes random and targeted testing of administrative expense transactions. WFAAB also conducts annual CO Scorecard reviews and CO bank reconciliation reviews. These processes are supplemented by approximately 15 on-site CO reviews per year. The QA Program results are reported throughout the year via online dashboards, and through annual VPU level summary reports to Senior Management. In addition, the Benefits Governance Team in HRDSO runs a quality assurance program for Global Mobility Support Framework benefits payable to staff including those located in COs, and MoUs between BPS and various Global Practices (GPs) and Regions are in place for monitoring and following up on the exceptions reported by WFAAB. The institution has also established whistle blowing channels, and investigates and takes disciplinary action when misconduct is proven.

However, opportunities for further strengthening of the oversight processes include (i) a process to jointly analyze issues arising from the various oversight reviews and investigations to identify underlying root causes, and implement measures to prevent the recurrence of similar cases; (ii) a comprehensive and integrated institutional risk assessment process to guide the prioritization of oversight resources to high risk areas; (iii) a clear mapping of responsibilities and a common understanding of the roles of each function to ensure that oversight resources are deployed effectively; and (iv) dissemination, to Heads of Mission, of lessons learned to help raise awareness of the types of measures that could prevent any recurrence of the misuse of administrative funds.

## 12. Advisory Review of IFC's Management of Data Access and Protection

The objective of the advisory review was to take stock of the current approach to data access and protection within IFC, and to provide management with advice on the current state of governance, process, and technology practices. The review focused on the control environment for two specific data elements (the Credit Rating and Environmental and Social Risk Rating) across their data lifecycle and provided advice in the following areas: (i) key risks to IFC from sensitive data being accessed by unauthorized or unintended individuals; (ii) policies, procedures, and principles governing data access management and clarity of roles and responsibilities to ensure that sensitive data types are identified and protected from inappropriate access throughout the data lifecycle; (iii) process activities and controls to protect sensitive data from inappropriate access throughout the data lifecycle; and (iv) IT infrastructure and solutions to protect data from inappropriate access.

IAD's review identified opportunities to strengthen IFC's design and implementation of data access and protection controls, and developed recommendations to improve the current state of governance, process, and technology practices, grouped under three main thematic areas:

- *Establish a holistic data access and protection approach to better address the needs of IFC:* Such an approach would enable consistent access management and protection across projects and IT systems.
- *Improve the governance over access management to facilitate the effective operationalization of the Data Access and Protection Framework:* This would strengthen management's control and visibility over users' access to data.
- *Evaluate the adequacy of existing technology solutions to support the framework:* Opportunities exist to implement solutions already owned by WBG as well as to adopt additional solutions to improve control over sensitive data.

## 13. Audit of IFC's Use of Blended Finance in Operations

The objective of the audit was to assess whether IFC has adopted and implemented processes to (i) make decisions to use Blended Finance consistent with the principles communicated to the Board; (ii) measure the results of Blended Finance operations and report them to stakeholders; (iii) generate a sufficient pipeline to meet the targeted use of Blended Finance in line with commitments made to the donors; and (iv) periodically review the functioning and implementation of the Blended Finance framework and apply lessons learned to improve the effectiveness of Blended Finance operations.

The audit concluded that IFC has well established processes and a robust framework for managing Blended Finance in its operations. IFC has established a management committee, called the Blended Finance Committee, that reviews potential investments against Board-endorsed criteria. The Blended Finance Committee consistently reviews and deliberates on proposals for the use of Blended Finance against the principles communicated to the Board, and their decisions are duly documented and communicated to the teams. In addition, Blended Finance staff conduct outreach efforts and spread awareness about Blended Finance through the issuance of Blended Finance-related documents to support IFC investment staff in developing the pipeline for the use of Blended Finance.

However, gaps were noted in the areas of periodic review and reporting of Blended Finance operations to stakeholders, information sharing protocols during supervision of Blended Finance projects, and a mechanism for the allocation of eligible deals to multiple facilities.

## ANNEX: List of Engagements in the FY18 Q3 Activity Report

Report No.	Engagement Name
	<i>WBG</i>
WBG FY18-02	1. Audit of WBG's Enterprise Desktop Management and Security
WBG FY18-03	2. Audit of WBG's Wireless Network Management and Security
WBG FY18-04	3. Audit of WBG's Corporate Procurement Processes
WBG FY18-05	4. Advisory Review of Management of Shared Service Agreements (SSAs) among WBG Institutions
WBG FY18-06	5. Special Review of the Administrative Expense Transactions Managed by Executives' Front Offices in the WBG Institutions
WBG FY18-07	6. Special Review of the WBG Administrative Expense Transactions of Executive Directors' Offices
	<i>Bank</i>
IBRD FY18-03	7. Assurance Review of the Bank's Implementation of the Uganda Transport Sector Development Project (Additional Financing): Lessons Learned and Agenda for Action
IBRD FY18-04	8. Audit of the Bank's Anti-Money Laundering and Countering the Financing of Terrorism Program
IBRD FY18-05	9. Audit of Implementation of SORT in Supporting Operational Decision-Making
IBRD FY18-06	10. Audit of Bank's Process for Managing Advisory Services and Analytics Activities
IBRD-IDA FY18-01	11. Audit of Oversight of Administrative Expenses Managed by Bank's Country Offices
	<i>IFC</i>
IFC FY18-02	12. Advisory Review of IFC's Management of Data Access and Protection
IFC FY18-03	13. Audit of IFC's Use of Blended Finance in Operations