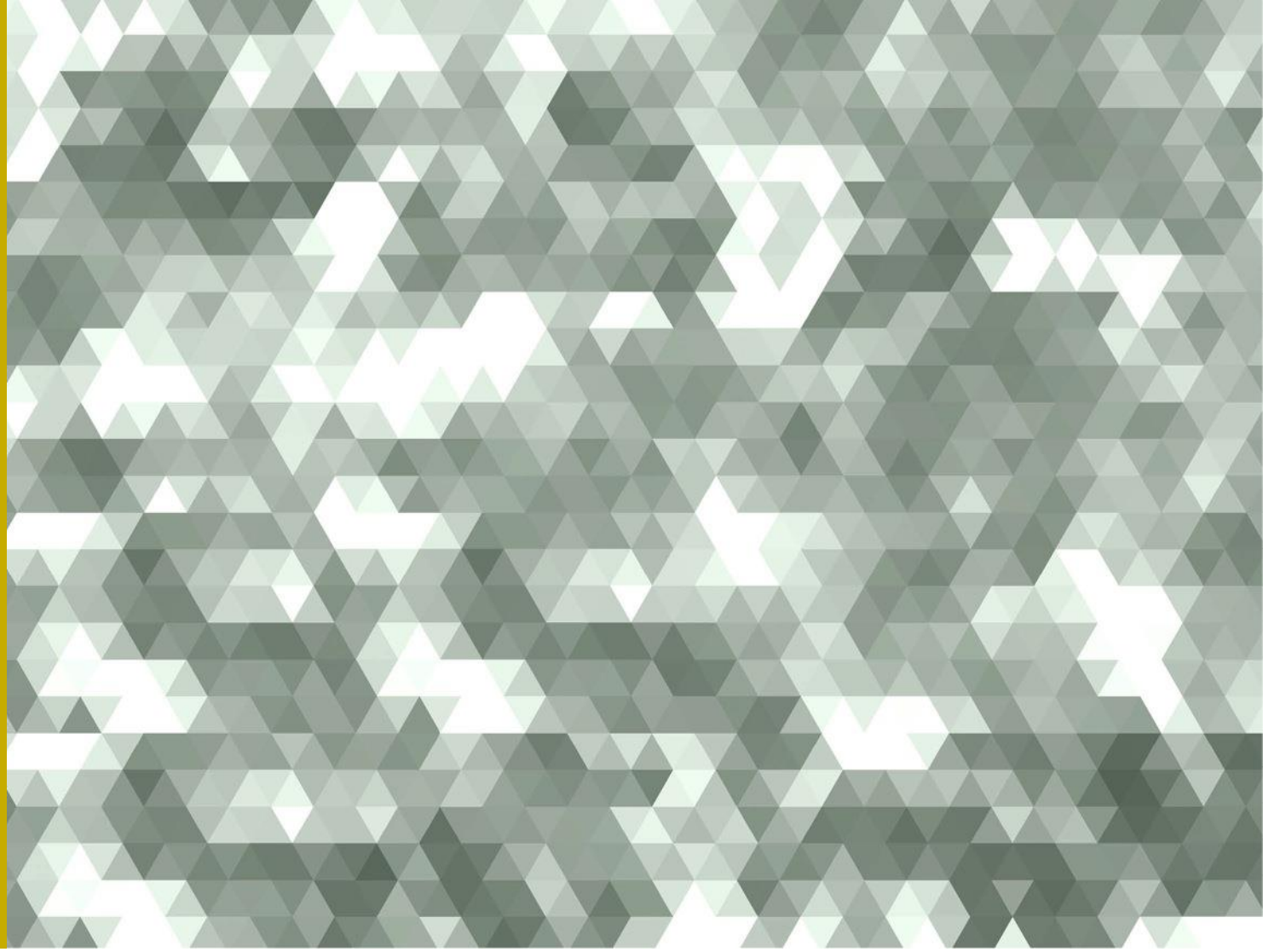

Audit Report

Effectiveness of IT Controls at the Global Fund

Follow-up report

GF-OIG-15-20b
26 November 2015
Geneva, Switzerland

The Global Fund
Office of the Inspector General

Table of Contents

I. Background and scope

Background
In early 2015, the Office of the Inspector General (OIG) audited the controls applicable to the Global Fund's Information Technology (IT) infrastructure, network and applications, including externalized and cloud-hosted services, to assess their effectiveness.

As serious weaknesses and security gaps were found that could have been exploited to inflict harm to the organization, the leadership of both the Audit and Ethics Committee and the Board, at the request of the Inspector General, agreed to postpone the publication of the OIG report to allow the Secretariat to address critical issues. This decision was taken in line with the Policy for the Disclosure of Reports Issued by the Office of the Inspector General.

The leadership of both the Audit and Ethics Committee and the Board requested that the OIG perform a review of the corrective actions taken by The Global Fund Secretariat.

2015 audit
The 2015 audit encompassed the Global Fund's IT infrastructure, network and applications, including the externalized and cloud hosted services. The review aimed to give the Board reasonable assurance on the effectiveness of IT controls both at an entity level and application level. Specifically, this audit tested IT controls over the following areas: access to data, data accuracy, data agility and data availability.

The OIG selected the ISO 27001 standard as the framework for its review which considers new technology evolutions such as mobile devices, remote computing and the integration of clouded services in IT environments.

The audit found that although the Global Fund had undergone an extensive transformation with new IT projects launched to support the New Funding Model and to enhance financial systems, IT security had not been prioritized.

The audit rating of the 2015 report was as follows:

Operational Risk	**Rating**
Data access	**Partial Plan to Become Effective**
Data accuracy	**Full Plan to Become Effective**
Data agility	**Generally Effective**
Data availability	**Full Plan to Become Effective**

Scope
Following the 2015 audit, this follow-up review aimed to assess the progress made by the Global Fund Secretariat in implementing the Agreed Management Actions from the 2015 audit, particularly around data access, accuracy and availability.

II. Executive Summary

The most critical weaknesses identified in the 2015 audit, which related to the improvement of IT security, the management of access, and the monitoring of systems and accounts, have now been substantially remediated. Significant improvements made include:

- recruitment of a Chief Information Security Officer in March 2015;
- extensive review of users' access rights, including access to databases and development of thorough activity report for the high-privilege accounts;
- installation of intrusion prevention and detection systems, designed to monitor traffic and data on the Global Fund's network and reduce the risk of unauthorized or malicious activity;
- a new antivirus solution has been deployed on the majority of the servers and a process to track and approve any exceptions has been put in place;
- strengthening of control procedures, including complexity of password requirements for regular accounts and periodic expiration of passwords for privileged accounts; and
- introduction of a new onboarding/off-boarding policy including contingent workers (consultants and other non-employee accounts), the objective of which is to have a single source of data for both staff and contractors and enable holistic monitoring of all accounts.

The above remediation activities have substantially addressed the vulnerabilities, related to weak access and monitoring, to which the Global Fund was exposed as of the completion of the 2015 audit. Notwithstanding this significant improvement, other weaknesses continue to exist in IT management that require attention.

The most significant vulnerability that has not yet been addressed relates to availability of systems and data. The Global Fund still does not have a formalized and fully tested IT disaster recovery plan. This is largely because the IT Department has outsourced the management and provision of all servers and related application services to an external provider. Discussions with the relevant third parties have started, but the contractual arrangements to enable a disaster recovery plan have not been formalized. Until such a plan is in place and has been tested, a risk remains that IT systems or data could become unavailable for a prolonged time as a result of a disaster or other interruptions, with potentially adverse impact on the continuity of business operations during that period. A full back-up service is expected to be provided by an external provider till Q2 2016

In addition, the following gaps also need to be addressed before the improvements made can be fully effective:

- the Management Executive Committee has not yet reviewed and approved several critical policies related to access, data classification, encryption or the overall approach to Global Fund IT security;
- exceptions identified during the review of access rights have not yet been fully resolved, nor are the activity reports for high privilege accounts being regularly monitored;
- the effectiveness of the antivirus solution is still limited, as four servers are not yet covered;
- an authentication software for systems requiring higher level of security is still to be installed; and
- not all consultants are yet integrated in the Human Resources Module of the Global Fund System, thereby limiting the effectiveness of the new on-boarding/off-boarding approach.

Overall, based on the evidence from our follow-up review, the OIG's opinion is that the Global Fund has addressed the most critical weaknesses identified in our earlier audit. However, additional effort is required to fully implement the Agreed Management Actions in the 2015 audit report, Further detail on individual actions can be found in Section III of the report.

III. Status of the Agreed Management Actions

01 Access to data

Agreed Management Action 1.1: Periodic reviews of users' access rights and application roles

The Global Fund Secretariat will improve the processes in place around data access, notably by: ▪ Performing a comprehensive users' access review for all Global Fund databases to assess whether mismatches and gaps still exist through consistency checks between the data storage locations. This should include a systematic review of current users' roles and permissions to ensure that they were granted on a *Need to know* basis. Users who changed job assignment within the Secretariat should be reviewed specifically in case they have unrevoked rights from their previous function. ▪ Performing a review of all service accounts within the Active Directory to ensure that they are still used and that their application owner and servers they work on are clearly identified. This should include restricting those accounts through group policy objects so that no interactive login is allowed and login file access permission are limited to only to required systems. ▪ Establishing a comprehensive list of all the production systems_subject to monitoring (including vendor-managed appliances and servers, but not test and development systems) and ensure that they are included in the DELL Secure Works monitoring solution, or an equivalent and appropriate solution. The Secretariat will ensure that pre-defined reports allow the generation of a thorough and tamper-proof activity report of any high-privileged account	
Owner: Chief Information Officer	**Target date:** 31 December 2015
Status: **Partially completed**	

The Global Fund Secretariat has implemented a number of improvements around data access, in particular:

- The review of user access for all Global Fund databases has been properly conducted. Application owners have been interviewed or surveyed. Based on information provided, all accesses to databases have been amended accordingly. Accesses to databases are only granted through group policy that defines user security and networking policies at machine level. Access, even in read-only, has been reduced as much as possible. Access to the different Share Point webpages are monitored through the Active Directory, but these permissions can be overridden and adjusted individually to match user need by the line manager/team site administrators.

- Service accounts have been linked to group policy objects. No user can log into the service account as the service accounts work only to connect software to database. Nevertheless, an exception list still exists. It contains service accounts for which owners and/or function have not been clearly identified and database accounts with direct access to the database. According to the IT Department, this list should be reduced before the end of the year; however, this exception list of direct access will continue to exist for specific purposes and will be controlled using an exception report.

- The IT Department established a list of all servers to select those with sensitive data that should be included in the Dell Secureworks Monitoring tool. Out of a total of 158 production servers, 53 have been included in the monitoring tool. Selected servers are those with more sensitive data based on recommendations from Dell. Pre-defined reports allowing the generation of a thorough and tamper-proof activity report of any high-privileged account adapted to The Global Fund

specificities are available but they are not regularly monitored. A dedicated employee has been appointed to perform this task from October 2015.

Agreed Management Action 1.2: Segregation of duties matrix for ERP platform and controls for user's access

The Financial Systems and Processes Department will formalize the segregation of duties responsibility matrix and perform a formal review of the users who are currently granted access rights in more than one module to assess potential conflicts. A formalized process for approval and tracking of exceptions will be developed as well. The IT Department will put in place the required preventive and detective controls for a continuous assessment of application set up against responsibility matrix and request Finance approval for any exception identified.	
Owner: Chief Information Officer and Manager, Financial Systems and Processes	**Target date:** 30 June 2015
Status: **Completed**	

The segregation of duties matrix has been formalized by the Finance Department in June 2015. It has been developed with the support of each manager of the Finance Department but the document has not yet been formally approved by the Chief Financial Officer. The IT department has updated user profiles based on this analysis and has developed a tool to track exceptions on the profile of users based on the roles and responsibilities assigned. The tool has been available since the end of June 2015. The Finance Department is expected to issue a report on a monthly basis in order to comment any exception or to update user right profiles.

Agreed Management Action 1.3: IT security function, policies and users awareness

The Global Fund Secretariat will improve the processes in place around IT security, notably by: ▪ The process of recruiting a Chief Information Security Officer (CISO) will be completed. This process started during the audit as the position was advertised. A candidate has already been selected and will start in March. To improve the security function within the organization, security related documents will be regularly updated. ▪ The IT Department will design a series of training sessions in collaboration with HR to raise awareness on information security matters and propose these to the Management Executive Committee for approval and implementation.	
Owner: Chief Information Officer	**Target date:** 30 June 2015
Status: **Partially Completed**	

Following the appointment of a Chief Information Security Officer in March, a series of IT policies have been updated by the IT Department. The Global Fund user's access policy is considered in force by the IT Department, however it has not been published on the intranet, or endorsed by the Management Executive Committee.

The Chief Information Security Officer has designed a plan and a road map to increase user's awareness on IT security but no formal approval from the Management Executive Committee has been requested and the program has not yet been rolled out. No information regarding the IT security has been published on the intranet and no training session has been organized with standard users of the organization to strengthen their IT security awareness.

Agreed Management Action 1.4: Data classification, data protection and confidentiality

Regarding the data classification project, IT will provide input for the Policy Guidelines which are being finalized by Legal Department. The SharePoint 2013 Document Management project will also implement a matrix to allow documents to be classified. The project is currently migrating legacy documents into the platform. A classification in the form of metadata addition to sites (currently Public, Internal, Confidential and Restricted in draft) will be enabled. As part of the project, IT Department plan to brand SharePoint sites and documents with an icon that represents their classification. The Chief Information Officer will propose a data encryption risk assessment analysis for Global Fund data stored on laptop computers or external media to the Management Executive Committee for decision.	
Owner: Chief Information Officer	**Target date:** 30 September 2015
Status: **Not Completed**	

The IT department has updated the Data Classification Policy which defines classification categories (public, intern, confidential and highly confidential) and provides a classification matrix matching confidentiality classification with certain types of documents and information. The legal department has circulated this matrix to each department for feedback, and plans to submit this policy to the Management Executive Committee in late 2015. No implementation of Data Classification will be performed on Share Point before the approval of the Data Classification Policy by the Management Executive Committee.

The Chief Information Officer did an assessment regarding the encryption of data and devices for the Secretariat but this analysis was not validated with data owners. The decision regarding the data encryption has not been yet submitted to the Management Executive Committee for approval.

Agreed Management Action 1.5: Password policies in place are not robust enough

The Global Fund Secretariat will improve the processes in place around access to systems, notably by: ▪ Taking immediate action to ensure that all named users' accounts, regardless of their role and position within the organization, have an expiring password and that all local administrative passwords are strengthened. ▪ Performing a review of the IT Security policy and the password requirements configuration and practices, assessing the desired level of identity and security for all IT systems and roles, proposing to the Management Executive Committee for approval a new IT Security policy taking these elements into consideration.	
Owner: Chief Information Officer	**Target date:** 31 December 2015
Status: **Partially Completed**	

All high privilege accounts now have an expiring date and the password complexity for those accounts has been strengthened. Passwords of normal accounts have also been reset with more complexity added.

The IT Security Policy has been updated with two new sub-policies: the user access policy and the password protection policy which describes password complexity. The policies have not been submitted to the Management Executive Committee for approval but this is scheduled for the fourth quarter of 2015.

Agreed Management Action 1.6: Access to Global Fund Technology network

As part of their roles and responsibilities, the new CISO will review the risks and controls over infrastructure security, and propose appropriate mitigations. Solutions for a multifactor authentication for Virtual Private Network and improved control access to Global Fund wired network will be proposed by the CISO to the CIO. The Telnet protocol will be phased out in Q2-2015 once a new solution will be available.	
Owner: Chief Information Officer	**Target date:** 30 September 2015
Status: **Partially Completed**	

A risk assessment was conducted by the CISO and the two factors authentication requirements have only been identified for treasury application and will be deployed in the next months. No general requirement for two factors authentication (2FA) has been identified at this point but IT Department continue to work with different providers to ensure that the infrastructure meets the standards in case of further deployment. Regarding wired connection security, the telnet protocol was replaced by a solution allowing for an encrypted authentication and communication channel in August 2015.

02 Data accuracy

Agreed Management Action 2.1: Onboarding process for full time employees and contractors

A process will be implemented to comprehensively review all Global Fund employees (internal and external) to make sure that the authoritative record for users (in GFS) is comprehensive and adequate. A project to create GFS as the single source of user data will be initiated with the Corporate Services (HR) team in IT.	
Owner: Chief Information Officer	**Target date:** 31 December 2015
Status: Partially Completed	

A new on-boarding/off-boarding policy including contingent workers was formalized in August 2015. Based on this policy, all employee and contingent worker data will be kept in the GFS module, which is part of the ERP platform. When a new employee or new contingent worker starts work at the Global Fund, HR and other relevant departments complete a form within GFS that automatically grant the user changes their job, their old access rights are automatically disabled once the new job is activated. All employee data are kept within a GFS folder and all historical changes are also retained.

However, the external personnel (consultants) are not yet integrated in the GFS module, and employees who have left the Global Fund but remain in the Active Directory are also not included in GFS for monitoring.

Agreed Management Action 2.2: Monitoring of servers, antivirus solutions and vulnerability assessment

Immediate roll-out action of missing anti-virus agents will be considered and performed, prioritizing servers in a production role and/or with access to the Internet. Exceptions based on Microsoft recommendations for database and virtual host's servers will be documented. An intrusion detection system and prevention system will be put in place. As part of his/her roles and responsibilities, the new CISO will assess and propose to the CIO costed solutions to monitor and protect the organization's network infrastructure and datacenters.	
Owner: Chief Information Officer	**Target date:** 30 June 2015
Status: Partially Completed	

The Microsoft End Point Security solution was installed on all servers in September 2015 to replace the Trend Micro solution. However, four servers need additional work before the anti-virus is fully effective.

The Chief Information Security Officer has submitted costed solutions to protect and monitor the network system to the Chief Information Officer. Based on the three Intrusion Detections/Protection systems (IDS/IPS) proposed, one was selected and after being tested since July it was implemented in production in September.

03 Data agility

Agreed Management Action 3.1: Change management and system development controls

As a compensative control, the change management request reference numbers of the 3rd party vendors should be integrated into the existing ad hoc field in the Service Now tool	
Owner: Chief Information Officer	**Target date:** 30 June 2015
Status: **Completed**	

A facility to manually insert the references from 3rd party vendors in the Service Now tool is now in place.

04 Data availability

Agreed Management Action 4.1: Business continuity planning

The business impact analysis (BIA) documentation as well as business continuity plan (BCP) will be finalized and signed off by the Chief Information Officer. All Global Fund data will benefit from a reliable back up and the full disaster recovery test will be completed as scheduled, business continuity in case of the unexpected unavailability of the Secretariat premises will be considered.	
Owner: Chief Information Officer	**Target date:** 30 September 2015
Status: **Not Completed**	

A business impact analysis has been formalized and signed off by the Chief Information Officer. The business impact analysis does not include a section dedicated to the minimum scope of (replacement) resources (buildings, staff, IT/data, external service providers and staff) that must be available in the event of a crisis in order to achieve the desired level of recovery.

The OIG found that the IT disaster recovery plan has not been formalized or fully tested; this is largely because the IT Department has outsourced the management and provision of all servers and related application services to an external provider. Discussions with the relevant third parties have started but the contractual arrangements to enable a disaster recovery plan have not been formalized. A full back-up service is expected to be provided by an external provider till Q2 2016

We also note that the IT strategy, including the current data availability strategy, has never been discussed at the Management Executive Committee.

Annex A General Audit Rating Classification

Highly Effective	**No significant issues noted**. Internal controls, governance and risk management processes were adequate, appropriate, and effective to provide assurance that objectives should be met.
Generally Effective	**Some significant issues noted but not material to the overall achievement of the strategic objective within the audited environment.** Generally, internal controls, governance and risk management processes were adequate, appropriate, and effective. However, there is room to improve.
Full Plan to Become Effective	**Multiple significant and/or (a) material issue(s) noted. However, a full SMART (*Specific, Measurable, Achievable, Realistic* and *Time-bound)* plan to address the issues was in place** at the time audit Terms of Reference were shared with the auditee. If implemented, this plan should ensure adequate, appropriate, and effective internal controls, governance and risk management processes.
Partial Plan to Become Effective	**Multiple significant and/or (a) material issue(s) noted. However, a partial SMART plan to address the issues was in place** at the time audit Terms of Reference were shared with the auditee. If implemented, this plan should improve internal controls, governance and risk management processes.
Ineffective	**Multiple significant and/or (a) material issue(s) noted.** Internal controls, governance and risk management processes were not adequate, appropriate, or effective. They do not provide assurance that objectives will be met**. No plan to address the issues was in place** at the time audit Terms of Reference were shared with the auditee.

Annex B: Methodology

The Office of the Inspector General (OIG) performs its audits in accordance with the global Institute of Internal Auditors' (IIA) definition of internal auditing, international standards for the professional practice of internal auditing (Standards) and code of ethics. These Standards help ensure the quality and professionalism of the OIG's work.

The principles and details of the OIG's audit approach are described in its Charter, Audit Manual, Code of Conduct and specific terms of reference for each engagement. These help our auditors to provide high quality professional work, and to operate efficiently and effectively. They also help safeguard the independence of the OIG's auditors and the integrity of their work. The OIG's Audit Manual contains detailed instructions for carrying out its audits, in line with the appropriate standards and expected quality.

The scope of OIG audits may be specific or broad, depending on the context, and covers risk management, governance and internal controls. Audits test and evaluate supervisory and control systems to determine whether risk is managed appropriately. Detailed testing takes place across the Global Fund as well as of grant recipients, and is used to provide specific assessments of the different areas of the organization's' activities. Other sources of evidence, such as the work of other auditors/assurance providers, are also used to support the conclusions.

OIG audits typically involve an examination of programs, operations, management systems and procedures of bodies and institutions that manage Global Fund funds, to assess whether they are achieving economy, efficiency and effectiveness in the use of those resources. They may include a review of inputs (financial, human, material, organizational or regulatory means needed for the implementation of the program), outputs (deliverables of the program), results (immediate effects of the program on beneficiaries) and impacts (long-term changes in society that are attributable to Global Fund support).

Audits cover a wide range of topics with a particular focus on issues related to the impact of Global Fund investments, procurement and supply chain management, change management, and key financial and fiduciary controls.