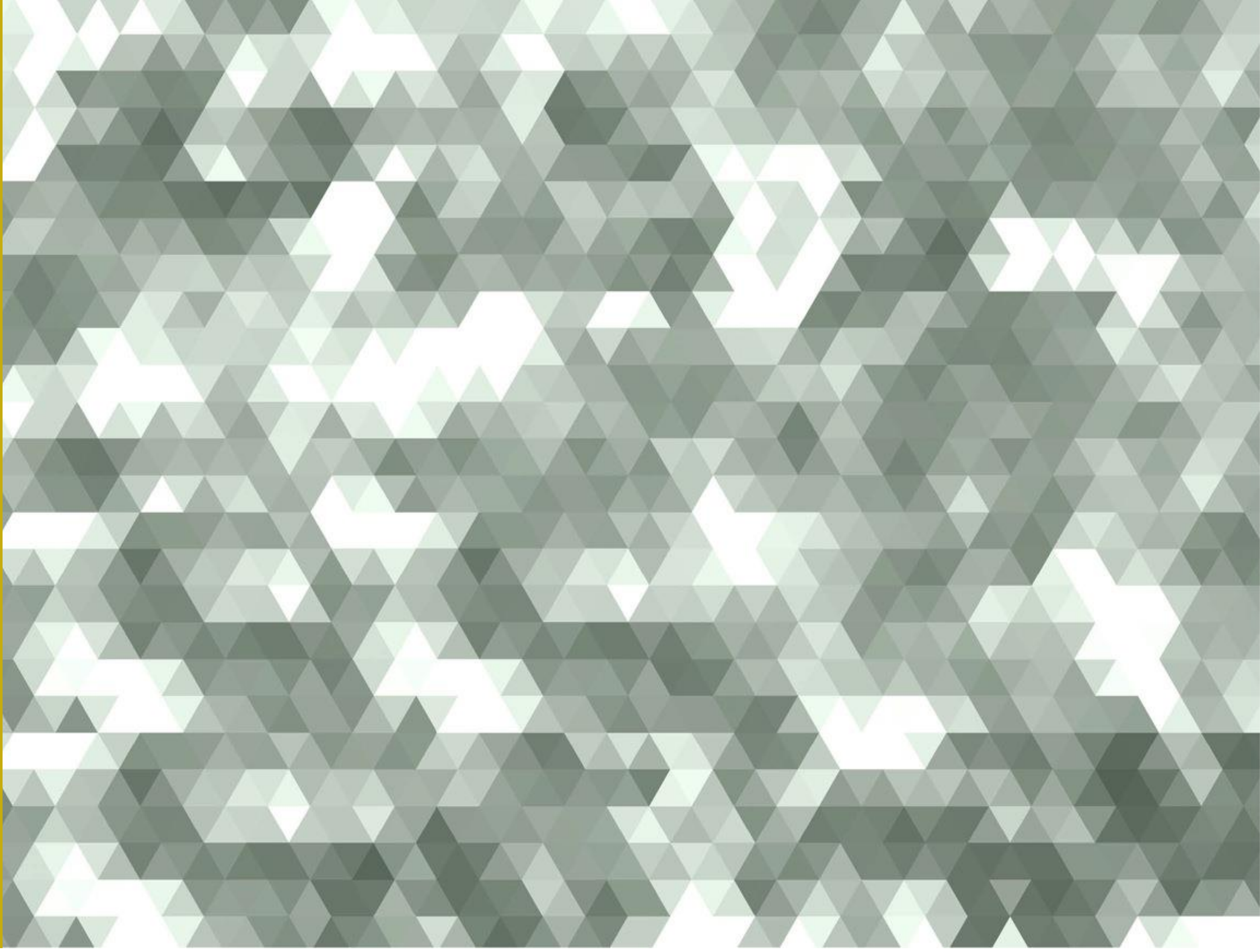

Audit Report

Effectiveness of IT controls at the Global Fund

GF-OIG-15-020
11 March 2015
Geneva, Switzerland

The Global Fund
Office of the Inspector General

Table of contents

I. Background

In early 2015, the Office of the Inspector General (OIG) audited the controls applicable to the Global Fund's 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 on 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 until October 2015 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 IT controls audit was led by the Office of the Inspector General in order to provide the Global Fund with reasonable, independent and objective assurance over the design and effectiveness of the IT controls in place to manage the key risks impacting programs and operations.

Technical environment

The Global Fund operates a Microsoft Active Directory for the authentication of its internal and external users. The Active Directory notably acts as the authoritative record for identification and access to all Global Fund applications and cloud services, except ERP suite and Local Fund Agent CRM applications, which are maintained separately and follow their own processes and requirements. ERP stand-alone authentication and communication occurs over dedicated link between Global Fund network and the ERP provider center located in the USA. Other hosted applications, are accessed through the Internet.

The Global Fund offers various types of remote access to end-users. Global Fund laptops can connect through the Internet to its internal network using a VPN,[1] E-mail can be accessed through web access and user-provided computers or mobile devices. The authentication for VPN and e-mail web access is over a secure channel through a single-factor (username and password).

The change management workflow is managed through a web-based solution called Service-Now. A change management coordinator exists for each of the two defined streams: infrastructure and operations. There is a comprehensive catalogue of infrastructure components and applications subject to change management requests. It lists the application or infrastructure components' business owners and responsible parties in technology and infrastructure maintenance.

The business continuity and disaster recovery plans have been formalized by the IT department, as recommended by the previous OIG audit, and its final implementation is scheduled for Q2 2015. The criticality of the applications with respect to business continuity has been assessed; an outage impact analysis has then been performed to align recovery time with application criticality.

The core infrastructure components support and deliver the most critical services for the Global Fund since they represent the network entry point and authentication realm for all the organization's users. Some of the infrastructure core components are by nature redundant because they are distributed over all the existing organization's sites. There is the primary data center (PDC) located in the organization's premises in Vernier, Switzerland and there is a process of migrating high priority systems like Exchange Email in both centers.

[1] Virtual Private Network: a network configuration which allows a user to securely reach a private network over the Internet

II. Scope and Rating

Scope

The scope of work encompassed the Global Fund's IT infrastructure, network and applications, including the externalized and cloud hosted services.

The audit review of IT controls seeks 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 the IT systems**: logical and system administrator access to IT applications and servers, data security, data classification, privacy and protection, physical access to IT infrastructure
- **Accuracy of IT systems**: data accuracy
- **Agility of IT systems**: change management and system development controls
- **Availability of IT systems**: business continuity and disaster recovery components

OIG selected the ISO 27001 standard in its 2013 version as a framework to perform both this IT controls audit and the high-level review in 2014. This updated standard takes new technology evolutions such as mobile devices, remote computing and the integration of clouded services in IT environments into consideration.

Following the initial planning assessment, certain controls over the human resources (terms and conditions of employment, recruitment screening), intellectual property (licensing) contracts compliance and governance (contact with authorities and special interest groups, regulation of cryptographic controls) were not included in the current audit objectives and not tested.

Not in Scope

The OIG dedicated network and infrastructure, physically split from the rest of the organization, was not in the scope of the current audit.

Rating[2]

Operational Risk	**Rating**	**Reference to findings**
Data access	**Partial Plan to Become Effective**	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Data accuracy	**Full Plan to Become Effective**	2.1, 2.2,
Data agility	**Generally Effective**	3.1
Data availability	**Full Plan to Become Effective**	4.1

[2] See Annex A for the definition of OIG ratings.

III. Executive Summary

In 2012 an external review recommended that the Global Fund's IT infrastructure be gradually outsourced. Since then, proactive measures have been taken to comply with this recommendation. In 2013-2014 the focus of IT was to move its application base and its infrastructure to outsourcing partners with a focus on the cloud.[3] During this transition, more attention was given to managing the move to the cloud while still ensuring current services meet the expected operational needs of the Global Fund.

Over the last years, the Global Fund Information Technology landscape has undergone an extensive transformation. In the last two years, new IT projects to support the implementation of the New Funding Model and enhanced financial systems were launched. Key initiatives include the Finance Step-Up[4] project and CRM tool for Grant Management and other functions.[5]

Historically, the Global Fund organizational IT security has not been prioritized, given the openness and transparency elements of the business model. To address current needs of integrity and resilience, with a view to better record management, and to ensure risks are mitigated, the Global Fund is evolving into a more stringent model. This model will impose restricted accesses based on data sensitivity, confidentiality and classification ultimately determined by its owners.

Internal controls over IT were deemed to be **generally effective for data agility** (change management and system developments). The controls over **data availability** (business continuity and disaster recovery components) **and data accuracy** showed some weaknesses but the Secretariat has **a full plan to become effective.**

The controls regarding **data access** (logical and access, data security, privacy and protection) are not adequate and only **a partial plan to become effective is in place.** Among the most critical findings were:

1. Data access:

Most of the IT internal controls are only partially or inadequately supervised; a task which is usually assigned to a dedicated **Information System Security function**. Furthermore, the OIG found obsolete and outdated IT security policies, a general lack of awareness for best practices in IT security by employees and ultimately deficiencies in security and monitoring systems.

The absence of a formal **segregation of duties matrix within the ERP business applications** creates a risk of incompatible roles being allocated to a limited number of users. This further hinders implementing preventive and detective controls over roles and accountability within ERP business applications.

Although work has started, **no regular reviews of users' access** are conducted, which results in rights or permissions being inadequately granted (for example, employees who left the organization but are still defined in business applications or users terminated by the Human Resources Department but still present as enabled users in the Active Directory). The

[3] Cloud computing is the use of the internet to run applications or store data.

[4] Finance Step Up is a transformation project launched in 2014 and designed to overhaul Global Fund financial systems and processes, provide a new financial data model and equip all staff with a common financial language

[5] CRM – Customer Relationship Management is a project designed to provide a single platform for grant management under the new funding model focusing on the automation of the existing processes

risk posed by internal moves from one department to another without the revocation of previous access rights should also be considered. More importantly, the way in which server software rights (“service accounts’) are configured **does not appropriately limit access based on the tasks required**; this creates risks that a problem which could be limited to one system affects others. Access and use of such access rights are also not monitored in a comprehensive and auditable manner, making incident detection and response difficult.

The **data classification** framework developed by the Legal Department will be ready for implementation by IT once it has been submitted, reviewed and approved by the Management Executive Committee (MEC). This framework introduces a new approach in terms of risk assessment and data protection which has been overlooked up to now. It is also a first step towards introducing the business to data classification, access and retention processes. This will be one of the tasks of the new Chief Information Security Officer currently under recruitment.

Password policies are not robust enough and do not correspond to best practice. The analysis of **domain password policies reveals inconsistent settings in terms of complexity, expiration, length and history**. Furthermore, non-expiring passwords were found by the auditors for named administrative accounts and standard users.

Remote services, including Virtual Private Network remote access, rely on a **username and password pair for access**. Best practice is to use multifactor authentication, reducing the risk of credential theft by malicious users. Multifactor authentication relies on something you own (phone, token) in addition to something you know (username, password) to gain access to resources.

2. Data accuracy:

Servers within the organization were not monitored by an anti-virus solution which represents a high risk of malware infestation.

After performing a vulnerability assessment using the Microsoft recommended tool, the OIG identified 31 out of the 50 Windows infrastructure servers tested which had not been upgraded with the latest security patch. This poses a **“severe risk” according to Microsoft tool classification.**

The on-boarding procedure of internal users follows two distinct workflows. Full-time staff members are identified through an Employee ID and follow the standard HR policy through Global Fund Systems. Contractors, or contingent workers in the ERP provider universe, follow a parallel on-boarding process which is not managed by HR but directly by the procurement and IT departments. This results in unaligned data for the two different types of employees.

3. Data availability:

Following an OIG recommendation in 2013, a Business Continuity Plan (BCP) was developed, with an initial deadline of 31 October 2014. The IT department revised this and to date a full disaster exercise has not taken place. A disaster recovery exercise focusing on the priority of applications is planned for Q3 2015, however, the disaster recovery plan has been partially tested with ERP platform. The exercise proved successful for the ERP business suite which was recovered within a day, in accordance with the terms of the managed cloud services agreement. The BCP for other IT systems and resources relies on the Data Protection Manager Infrastructure

At the time of the audit, all the data that were intended to be protected had been migrated to the Data Protection Manager Infrastructure.[6] Notably, SharePoint 2007 database was not included in the Data Protection Manager as it was causing repeated failure of the entire backup due to size.[7] A separate back up for this database was put in place, however this back up proved to be ineffective and failed during the audit period.

[6] DPM, Data Protection Manager, is the centralized Microsoft backup solution

[7] A SharePoint 2007 database used as an office data repository in the Global Fund old Intranet environment. The product lifecycle has come to an end and is no longer supported

IV. Findings and agreed actions

01 Access to data

1.1	Periodic reviews of users' access rights and applications roles.

Users' access rights are not properly managed. No regular user reviews based on consistency checks are carried out for the Global Fund data storage locations.

A Federated Identity Management model is used by the Global Fund to automate creation, deletion and management of users and rights on Global Fund systems. Such a model is adequate for introducing new users and access rights emanating from membership in a group. Permissions can be revoked as part of the termination process when a user is deleted from the Active Directory. [8,9]

- This model has limited effectiveness if an end-user simply moves to another department or cost center rather than leaving the organization. In these cases, his or her employee ID and login credentials don't change and membership of the former department group is not necessarily revoked by the group owner.

- In addition, compounding this issue, no formal reviews of users' access rights have taken place since the Chief Information Security Officer's function was removed in 2012.

For ERP platform[10], the OIG noted that deleted users in the Active Directory, essentially consultants or contractors who have left the organization, still exist with full access and rights in the ERP provider universe. The undue access risk of these users is largely mitigated by the fact that access to the E-Business suite is only possible when logged into a Global Fund computer, which is usually inaccessible to consultants and contractors who have left the organization.

- Access to service accounts is not restricted to the systems in which they are intended to operate; for example, a service account for a given application or group of servers should have a login restriction for those systems.[11] For highly-privileged service accounts, such as those with domain administration rights, a thorough description of their usage, as well as the possibility to identify their application owner, should be available within the Active Directory as attributes (the manager attribute is a possible option).

Numerous systems, including domain controllers, had no DELL Secure Works agents installed for users monitoring.[12,13]

- The audit trail for usage of administrative and high privileged accounts has material gapsand no control exists to compensate for the lack of monitoring.

[8] Federated Identity Management: allows users previously authenticated in the GF environment to access clouded services

[9] The Microsoft directory service which allows the identification and authentication of users and computers

[10] An integrated solution for applications and business software comprised of various modules

[11] Functional accounts running a task, a service or a scheduled job anonymously on a server or workstation. Service accounts are typically not linked to named users but to applications

[12] A Windows authentication server

[13] An agent is a computer program that acts on behalf of a user or a program and generally retrieves information to push it to, or have it pulled from, a centralized management system console

Agreed Management Actions

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 have been granted on a *Need to know* basis. Users who have 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

1.2	Segregation of duties matrix for the ERP platform and controls for users' access.

The segregation of the duties matrix for the ERP application is not formalized and controls to assess incompatible roles and responsibilities in the ERP provider environment are not in place.

The segregation of duties for the ERP applications suite is not sufficiently formalized within the different functions of the Finance Department. Users with privileges higher than a read-only permission have access to multiple modules. The OIG's analysis showed that in practice permissions were granted on a *Need to know* basis by business owners depending on the user's function with the Global Fund, but no clear segregation of duty matrix exists within the FISA Division.

In the absence of a clear responsibility matrix, the risk related to potentially conflicting responsibilities between the accessible modules of the ERP solution by the finance department employees remains.

Agreed Management Actions

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

1.3	IT Security function, policies and users awareness.

The Information System Security function does not exist within the organization, IT security policy is not regularly updated and there is no IT security awareness training for employees.

- A security function represented by a Chief Information Security Officer (CISO) does not exist as this function was abolished after 2012. IT security matters were delegated to the Technical Infrastructure and Maintenance Services Team. An Information Security Officer role has been recently re-created within the organization.

- The OIG observed that the current IT policy is adequately communicated and available online to the organization's users. However, its content is obsolete and contains information which does not necessarily reflect the organization's current situation, in particular around data protection, reasonable personal use of resources, a "clean desk policy", regular security awareness training, password policy or security classification.

- Currently the Global Fund does not provide IT security awareness documentation or trainings for its employees even though security awareness is one of the main objectives of IT management for the current year.

Agreed Management Actions

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 MEC for approval and implementation.

Owner: Chief Information Officer
Target date: 31 December 2015

1.4 Data classification, data protection and confidentiality.

There is no data classification policy in place to assess and formalize the level of confidentiality and protection needed for every type of data.

Following the high-level audit performed by the OIG in April 2014, a joint IT-Legal led project for data classification was initiated and responsibilities for designing the framework and policy were clearly defined. The deadline for finalizing this project was set for 1 October 2014.

Currently draft versions of the proposed Global Fund Information Classification Policy, Information Handling Guidelines and Data Protection Policy are being reviewed. The draft version of the data classification framework established by the Legal Department defines four classification categories: *Public*, *Internal*, *Confidential* and *Restricted*; however, the classification of Global Fund data according to the above mentioned categories has not been implemented and the IT systems are not enforcing or taking such classifications into account.

The Global Fund does not implement hardware encryption to protect the organization's data stored locally on laptop computers or external media against loss or theft. It also limits the guarantees the Global Fund can offer in terms of managing confidential information. This entails data pertaining to employees, commercial and technical partners, as well as implementers and beneficiaries. Data may be accessed by anyone with physical access to servers, workstations or laptops. The Chief Information Officer considers that the relative lack of sophistication of Global Fund users and processes means that encryption will be complex and will likely result in data loss.

Agreed Management Actions

Regarding 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 the IT Department plans 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

1.5	Password policies in place are not robust enough.

Analysis of the password policies in place revealed weaknesses and inconsistencies. Password expiration policy could be manually overridden for certain users' accounts.

The password policies implemented in the authentication realms do not follow the requirements fixed by the current Global Fund security policy. Inconsistent settings were observed regarding history, password age, complexity requirements and expiration policy.

Agreed Management Actions

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 MEC for approval a new IT Security policy taking these elements into consideration.

Owner: Chief Information Officer
Target date: 31 December 2015

1.6	Access to Global Fund Information Technology network.

Access to remote services, including remote access to the Global Fund network via a Virtual Private Network, relies on single factor authentication.

A username and password pair is commonly used to control access to restricted systems. However, even when strong passwords are used, this carries some significant inherent weaknesses. Best practice is to move away from such so-called "single factor" authentication to multifactor authentication. Multifactor authentication relies on something you own (phone, token) in addition to something you know (username, password) to gain access to resources. One notable advantage of multifactor authentication is that it resists common attacks which obtain the password either from an infected computer or when the password is transmitted from the computer to the recipient application.

Currently, VPN access into the organization network and access to other remote services, such as webmail, relies on a single factor authentication system.

Beyond the remote access to systems, the Global Fund does not currently implement sufficient access control over its wired network. Although wireless access to the organization's network is sufficiently controlled through the use of encryption certificates, it is still be possible to connect an external computer to the corporate wired network and obtain an IP address on a client's computer range.[14]

The equipment used as the backbone of the Global Fund network is called network switches, which are present on each floor as well as in the data centers. These are complex systems that can be configured and managed like server computers. The configuration interface can be accessed using the insecure legacy Telecommunication Network (Telnet) protocol.[15,16] Telnet sends all data, including passwords, in clear text over the network. It is easy for someone with access to the physical network between an administrator and the switch to retrieve passwords and tamper with the configuration.

Agreed Management Actions

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 VPN 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

[14] IP address: a unique identification number allocated either statically or dynamically and defining an equipment in a network based on the Internet protocol (IP)

[15] Telnet is a legacy protocol used to emulate a command-line interface on remote systems. Though generally outdated, it is still in use to manage network devices such as switches or routers

[16] A switch is a device which connects computers and other equipment together on a network. Opposed to a hub which broadcasts information packets to all connected hosts, a switch can filter communication according to ports

02 Data accuracy

2.1	User on-boarding policy and accuracy of users' data.

The on-boarding process for full-time employees and contractors is done through different IT processes and is managed by different departments.

The onboarding of Global Fund full-time employees is managed by the Human Resources department and consultants by the Procurement Unit. Both processes use different IT processes and systems to provision resources and access.

GFS is currently used to maintain permanent staff records whilst contractors are created through a separate process (Service-Now[17] application form) into the Active Directory.

As a result, data anomalies can occur. For example, some consultants didn't have a record for a responsible line manager in the Active Directory at the time of the audit. Mismatches in terms of users' login naming conventions were identified in the following repositories: Active Directory, ERP-based GFS and the KABA database (controlling physical access to the building).

Inconsistencies in user management can result in unmanaged contractors or permanent staff still being identified as 'contingent workers' although they have become full-time employees, or retaining physical access after they have left the organization. Consolidating the authoritative record into GFS and unifying the process for contractors with an expiration date at the term of their contract, could enhance the user's management process.

Agreed Management Actions

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

[17] One of the Global Fund clouded services provider

2.2	Monitoring of servers, antivirus solutions and vulnerability assessment.

No intrusion detection system (IDS) or intrusion prevention systems (IPS) solutions are in place at the boundaries of the organization's network perimeter. Some servers are not monitored with an antivirus solution.[18,19]

After assessing the anti-malware solutions and interviewing the network engineer, the OIG noted that no IDS / IPS solutions were in place at the boundaries of the organization's network perimeter. Such systems are designed to monitor network for malicious activity, detect, log and report on such activity and ultimately assist in blocking or preventing it. Malicious activity notably comprises of network traffic created by viruses or similar nefarious software.

According to the activity log of the corporate anti-virus solution, numerous servers are currently not monitored. Consistency checks performed with Active Directory outputs showed that some servers were not monitored against virus infestation since they had no antivirus agents installed. According to the IT Department this was a deliberate choice based on recommendations by the software vendor to turn off anti-virus scanning in certain situations, but these exceptions are not tracked or documented and therefore there is no audit evidence in this respect.

Vulnerability assessments performed on a limited range of 50 randomly selected Windows servers resulted in a *"Severe Risk"* rating (according to Microsoft classification) for 31 servers, mostly because of unapplied security patches.[20]

Agreed Management Actions

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 hosts 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 data centers.

Owner: Chief Information Officer
Target date: 30 June 2015

[18] An IPS, or Intrusion Prevention System, is a network security appliance. Opposed to an IDS, it will attempt to automatically block /stop the malicious activity

[19] An IDS, or Intrusion Detection System, is a device or software application which monitors a network or a host system activities for malicious activities or policy violations. It generates logs, alerts and reports of those activities

[20] A security patch or corrective hotfix is a code update which fixes vulnerabilities in an operating system or in an application

03 Data agility

3.1	Change management and system development controls

Change management and system development controls were found to be effective but improvements are needed regarding the tracking of change management requests.

Dependencies between infrastructure and operations are not detectable through the change management request system; for example, if a pre-requisite exists at the infrastructure level, it is not necessarily reflected as part of the operational change request.

A separate workflow is required for the cloud service providers who manage their own change request process, in particular for the ERP platform or for the virtual data center (VDC) provider. [21], [22] Changes exclusively initiated through these platforms are not necessarily traceable through the Service Now tool; it is possible to manually add all changes requests in Service-Now, although this is not currently done on a routine basis.

This means that changes in one system can have an unforeseen negative impact on other systems, which are only detected when a change is put into production; as these changes are not recorded in a central database, it may make it more difficult trace the root cause of an issue.

Agreed Management Actions

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

[21] Externalized service providers whose systems located in the cloud trust GF authenticated users and grant them access to their service platforms

[22] A managed hosting service provider of the Global Fund

04 Availability of data

4.1	Business impact analysis and business continuity planning

Not all the Global Fund data benefit from a reliable back up as the project to manage disaster recovery has not yet been finalized.

Following an OIG audit in April 2014, the IT department accepted that IT disaster recovery should be a prioritized for the Global Fund. A project to implement a full disaster recovery plan was presented to the Audit and Ethics Committee in October 2014 with the deadline of Q2 2015 for a full disaster recovery test. However, at the time of the audit, the OIG noted:

- The business impact analysis (BIA), as the foundation of the business continuity plan (BCP), had not been signed-off by the Chief Information Officer. [23], [24]
- At the time of the audit, all the data that were intended to be protected had been migrated to the Data Protection Manager Infrastructure.[25] Notably, SharePoint 2007 database was not included in the Data Protection Manager as it was causing repeated failure of the entire backup due to size. [26] A separate back up for this database was put in place, however this back up proved to be ineffective and failed during the audit period.
- The number of available VPN connections in case of a full disaster recovery does not accommodate concurrent access of all employees working at the Secretariat. In the case of a full disaster recovery, the maximal number of available VPN connections is currently limited to 242. Furthermore, the BCP assumes that all users will have their professional laptop available to continue working, without regard to the business roles of these users. Nevertheless, this entails that without prioritized access control access to key users may not be available in a timely manner.

Agreed Management Actions

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

[23] BIA, acronym for Business Impact Analysis, an evaluation and classification of infrastructure components and applications which will ultimately establish a criticality level

[24] BCP, acronym for Business Continuity Plan

[25] DPM, Data Protection Manager, is the centralized Microsoft backup solution

[26] A SharePoint 2007 database used as an office data repository in the Global Fund old Intranet environment. The product lifecycle has come to an end and is no longer supported

V. Table of Agreed Actions

No.	Category	Agreed Management Action	Owner/ Date
1.1	Periodic reviews of users' access rights and applications roles.	The Global Fund Secretariat will improve the processes in place around data access, notably by: • Performing a comprehensive users' access review for all GF 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
1.2	Segregation of duties matrix for the ERP platform and controls for users' 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	**Owner:** Chief Information Officer Manager, Financial Systems and Processes **Target date:** 30 June 2015

		responsibility matrix and request Finance approval for any exception identified.	
1.3	IT Security function, policies and users awareness.	The Global Fund Secretariat will improve the processes in place around IT security, notably by: Completing the process of recruiting a Chief Information Security Officer (CISO) which started during the audit when the position was advertised. A candidate was already selected and will start in March. As to improve the security function within the organization the security related documents will be regularly updated. Having the IT Department design a series of training sessions in collaboration with HR to raise awareness on information security matters and propose these to MEC for approval and implementation.	**Owner:** Chief Information Officer **Target Date:** 31 December 2015
1.4	Data classification, data protection and confidentiality	Regarding 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 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
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 MEC for	**Owner:** Chief Information Officer **Target Date:** 31 December 2015

		approval a new IT Security policy taking these elements into consideration.	
1.6	Access to Global Fund Information 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 multi factor authentication for VPN 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
2.1	User on-boarding policy and accuracy of users' data.	A process will be implemented to comprehensively review all GF 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.	**Owners:** Chief Information Officer **Target date:** 31 December 2015
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 hosts 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 data centers.	**Owner** Chief Information Officer **Target date:** 30 June 2015
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
4.1	Business impact analysis and 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

VI. 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.

VII. 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.