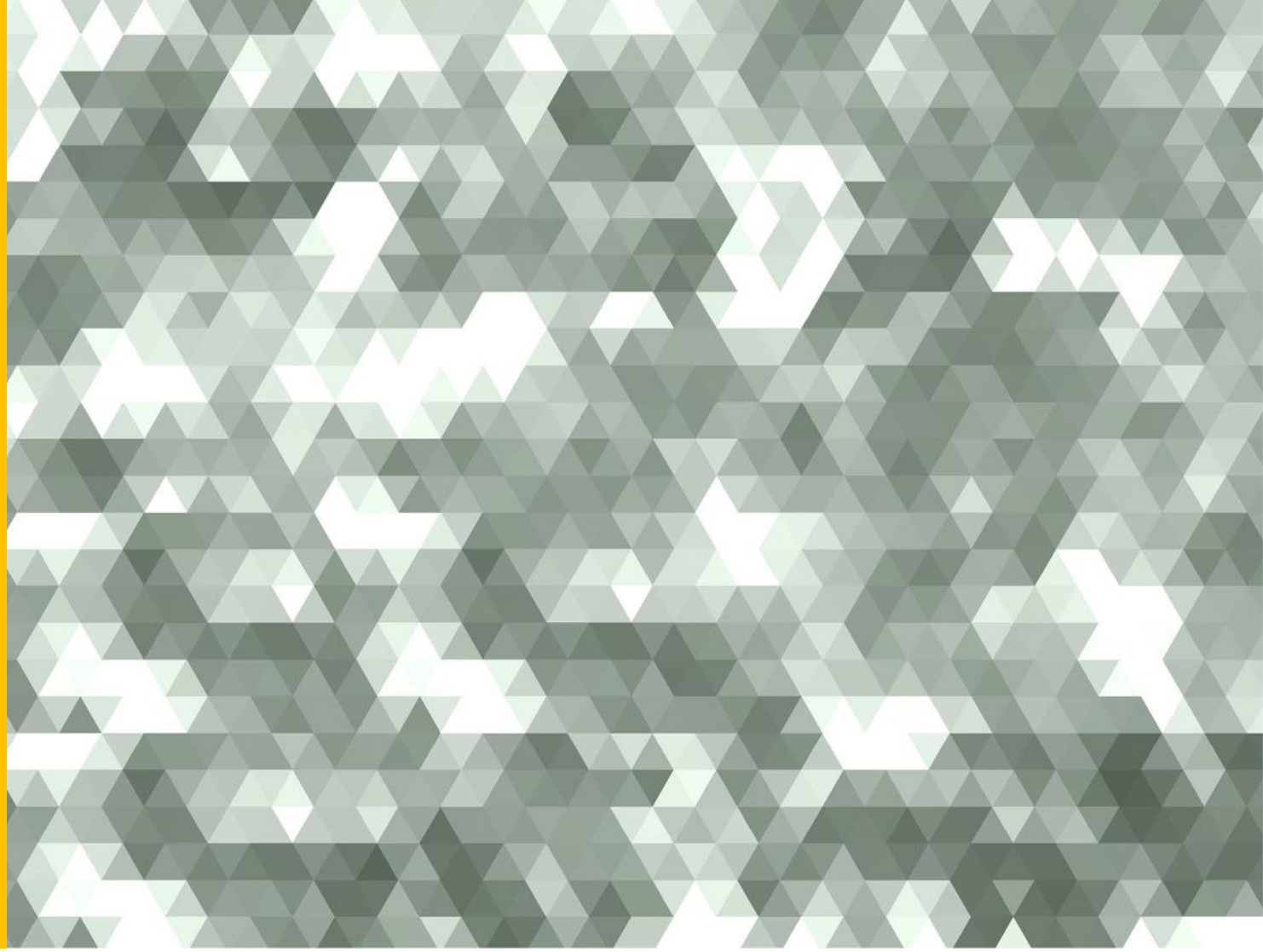


Audit Report

Cloud Computing at the Global Fund
Effectiveness of IT Controls

GF-OIG-17-013
28 June 2017
Geneva, Switzerland

The Global Fund
Office of the Inspector General

What is the Office of the Inspector General?

The Office of the Inspector General (OIG) safeguards the assets, investments, reputation and sustainability of the Global Fund by ensuring that it takes the right action to end the epidemics of AIDS, tuberculosis and malaria. Through audits, investigations and advisory work, it promotes good practice, reduces risk and reports fully and transparently on abuse.

Established in 2005, the OIG is an independent yet integral part of the Global Fund. It is accountable to the Board through its Audit and Finance Committee and serves the interests of all Global Fund stakeholders. Its work conforms to the International Standards for the Professional Practice of Internal Auditing and the Uniform Guidelines for Investigations of the Conference of International Investigators.

Contact us

The Global Fund believes that every dollar counts and has zero tolerance for fraud, corruption and waste that prevent resources from reaching the people who need them. If you suspect irregularities or wrongdoing in the programs financed by the Global Fund, you should report to the OIG using the contact details below. The following are some examples of wrongdoing that you should report: stealing money or medicine, using Global Fund money or other assets for personal use, fake invoicing, staging of fake training events, counterfeiting drugs, irregularities in tender processes, bribery and kickbacks, conflicts of interest, human rights violations...

Online Form >
Available in English, French, Russian and Spanish.

Letter:
Office of the Inspector General
Global Fund
Chemin de Blandonnet 8, CH-1214
Geneva, Switzerland

Email
ispeakoutnow@theglobalfund.org

Free Telephone Reporting Service:
+1 704 541 6918
Service available in English, French, Spanish, Russian, Chinese and Arabic

Telephone Message - 24-hour dedicated voicemail:
+41 22 341 5258

Fax - Dedicated fax line:
+41 22 341 5257

More information: www.theglobalfund.org/oig

Audit Report

OIG audits look at systems and processes, both at the Global Fund and in country, to identify the risks that could compromise the organization's mission to end the three epidemics. The OIG generally audits three main areas: risk management, governance and oversight. Overall, the objective of the audit is to improve the effectiveness of the Global Fund to ensure that it has the greatest impact using the funds with which it is entrusted.

Advisory Report

OIG advisory reports aim to further the Global Fund's mission and objectives through value-added engagements, using the professional skills of the OIG's auditors and investigators. The Global Fund Board, committees or Secretariat may request a specific OIG advisory engagement at any time. The report can be published at the discretion of the Inspector General in consultation with the stakeholder who made the request.

Investigations Report

OIG investigations examine either allegations received of actual wrongdoing or follow up on intelligence of fraud or abuse that could compromise the Global Fund's mission to end the three epidemics. The OIG conducts administrative, not criminal, investigations. Its findings are based on facts and related analysis, which may include drawing reasonable inferences based upon established facts.

Table of Contents

1. Executive Summary

1.1. Opinion

Cloud computing 'is the delivery of on-demand computing resources from applications to data centers, over the internet, on a pay-for-use basis.'[1] The Global Fund started using cloud computing as an approach to IT service delivery in 2014. Approximately 60% of IT infrastructure and applications are currently managed by external providers through cloud computing techniques, as well as related types of outsourced and hosted services. This has improved the flexibility of IT operations through better availability of services. However, the absence of an overarching strategy and limited management of associated risks have affected the effective roll out of cloud computing. Therefore **significant improvement** is needed to design a cloud computing strategy aligned to the Global Fund's business needs and to manage the related risks.

Generally, the Secretariat has improved its IT controls since the last OIG IT audit in 2015 (see Section 3.3). However, there are still areas for improvement in cloud computing-related data access and accuracy. Nevertheless, no significant instances of data loss or service interruption have occurred since 2015. The basic IT controls are therefore considered as **partially effective.**

1.2. Key Achievements and Good Practices

Adoption of cloud computing: The Global Fund has engaged market leading partners to provide its cloud computing services. The outsourcing of the operational management of key IT services has resulted in a number of benefits including regular updates of server-based application and software by the service providers, reduced data management sites at the Global Fund and staff are able to access data remotely through the internet.

Improvement in IT controls: The Global Fund's IT Department has grown significantly since 2015, in line with the business needs of the organization. Basic IT controls have improved since the last OIG audit in 2015. At the time, the OIG had identified serious weaknesses and security gaps, which could have been exploited to inflict harm on the organization. Those fundamental weaknesses have since been materially addressed.

Several initiatives have strengthened IT controls around access, accuracy and disaster recovery management. Password policy has been strengthened and an IT disaster recovery plan developed for existing IT applications. Penetration and vulnerability testing of key IT applications to ensure appropriate safeguards have been instituted. In addition, an IT Security Regulations Policy is under development to provide guidance on data transmission and other IT risks.

1.3. Key Issues and Risks

Absence of a comprehensive strategy for cloud computing: The adoption of cloud computing as a general approach to service delivery is not guided by a clear strategy and implementation plan. This approach to limit the amount of services delivered directly through Global Fund-owned or controlled infrastructure has compounded an already fragmented IT infrastructure. The Secretariat has also not duly considered the long-term impact of cloud computing on the organization. Cloud computing at the Global Fund has evolved naturally with neither a defined approach nor roll out plan. The absence of a clearly formulated rationale and defined targets for cloud computing make it difficult to evaluate actual progress after three years of implementation.

Limited risk management: Cloud computing generally results in the transfer of several IT risks to a cloud services provider. However, the IT risk profile of the organization changes such that there is increased exposure to other types of risk such as data management, supplier performance and legal risks. For instance, cloud computing enables the Global Fund to store data in various locations,

[1] https://www.ibm.com/cloud-computing/learn-more/what-is-cloud-computing

which reduces the risk of total loss in case of a significant data incident. At the same time, this decrease in operational risk may also be accompanied by an increase in legal risk as confidentiality of the Global Fund data may be weaker if stored in countries that do not provide privileges and immunities to the organization and could subpoena its records. Furthermore, there may be a risk that the Global Fund becomes too dependent on certain providers who could exploit this dependency to make unfavorable changes in contractual terms. These and similar risk trade-offs have not yet been formally assessed nor has the potential business impact been evaluated and, where necessary, led to clear mitigating actions.

Gaps in management of service providers: The IT Department has assigned dedicated staff to manage various cloud service providers. However, the absence of a clear framework and formalized processes to manage them have resulted in inconsistencies across the organization with key aspects of provider performance not effectively monitored.

1.4. Rating

Objective 1. A strategy and implementation plan does not currently exist to guide the Global Fund's adoption of cloud computing. The rationale and the business objectives for the adoption of cloud computing are yet to be defined. Therefore **significant improvement is needed** to design a cloud computing strategy aligned to business and operational needs.

Objective 2. Risks related to the adoption of cloud computing are yet to be assessed and measures defined to mitigate the relevant risks. Thus, risk management in relation to cloud computing **needs significant improvement**.

Objective 3. There have been significant improvements in IT controls at the Global Fund since 2015. Data recovery and security awareness have been enhanced. Improvements are required in controls related to data access and accuracy. The IT controls are therefore rated as **partially effective.**

1.5. Summary of Agreed Management Actions

The Global Fund Secretariat has plans to address the risks identified by the OIG through the following summarized Agreed Management Actions:

- The development of an IT strategy with clear objectives for approval by the Management Executive Committee.
- The enhancement of IT governance mechanisms through an overhaul of the existing Enterprise Architecture Board (an internal board set up in 2016 to oversee IT decisions).
- The improvement in the management of IT risks through the identification of potential cloud computing risks, an impact assessment and the institution of measures to mitigate the risks. The identified risks and related mitigation measures will be incorporated into the Global Fund Organisational Risk Register which is reviewed by the Management Executive Committee on quarterly basis.
- The enhancement of security specifications for data transfers by leveraging existing Global Fund Information Classification and Handling Regulations.
- The development of a segregation of duties matrix for the outstanding applications and further enhancements and testing of disaster recovery plans.

2. Background and Context

2.1. Overall Context

Cloud computing involves the transfer of the management and delivery of an organization's IT needs (infrastructure, processing, storage needs, and/or applications) to a third party referred to as cloud service provider. If well managed, cloud computing can result in important benefits for the organization, including: cost savings arising from limited capital expenditure on IT infrastructure; flexible availability of computing power to manage a growing or shrinking volume of data; significantly improved flexibility of IT operations through increased availability of computer resources; delegated responsibility for software and security updates; increased agility to respond to changing operational requirements; and the opportunity to integrate the management of data and information across the organization.

These potential benefits also come with different risks profile that need to be fully considered. These include the potential breach of confidential information managed outside of the organizational boundaries; legal vulnerabilities as sensitive data may be stored in jurisdictions where the organization may not enjoy privileges and immunities; increased vulnerability to vendor performance issues due to a higher level of reliance on external service providers; and potential cost inefficiencies if the adoption of cloud computing is not well managed to reduce the risk of redundancies or duplication across the cloud ecosystem.

This multiplicity of both real business opportunities and significant risks highlight the need for a structured and well thought-out cloud strategy that sets a clear vision for the target state of the IT infrastructure, a structured roadmap to achieve that state, an effective process to analyze the risk/reward trade-offs, and sound IT governance to challenge and validate the high level strategic choices being made.

The Global Fund procured its first cloud computing solution in 2014. In 2013-14, the organization outsourced material IT applications and infrastructure to external service providers. The Global Fund adopted a hybrid model[2] for cloud computing due to legacy IT systems[3], security requirements and customization capability of the systems. The Global Fund uses both public and private clouds, as well as more traditional remote hosting arrangements. A public cloud is where business data sits with other company data accessible to all users. The service provider institutes measures to safeguard access and to isolate data for its various clients. The Global Fund also uses private clouds arrangements that are designed to serve its exclusive needs. The organization also uses virtual data centers where specific equipment and systems are provisioned and maintained in part by a third-party for the use of the Global Fund.

The Global Fund adopted three delivery methods to support its cloud computing:

- *Software as a Service* (SaaS), which is a method for delivering software applications over the internet on demand, typically on a subscription basis through relationships with key external service providers. For instance, SaaS is used for the Global Fund's treasury function.
- Under the *infrastructure as a service* model, the Secretariat has outsourced the storage and management of its IT infrastructure, such as servers, to an independent service provider.
- An *on-demand environment* for developing, testing, delivering and managing software applications referred to as 'platform as a service' (PaaS). This is used by the Secretariat for cloud-based financial and grant management applications.

2.2. IT Technical Environment

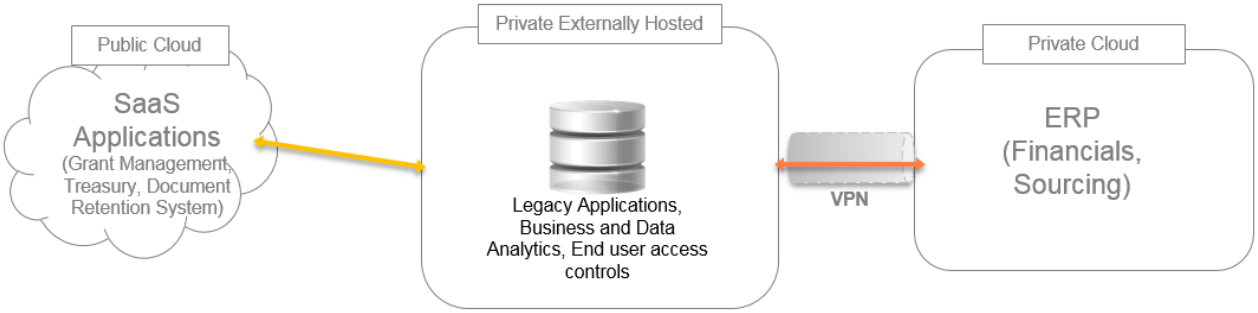
The Global Fund operates a 'Microsoft Active Directory' to validate the authenticity of its internal and external users. Whilst the majority of cloud based applications and services require this for user

[2] Hybrid Cloud: A mix of cloud vendor services, internal cloud computing architectures and classic IT infrastructure, forming a hybrid model that uses specific technologies to meet specific needs.
[3] Legacy system refers to an application or product that has been in the IT landscape for over 24 months in stable use, with plans to either upgrade the system to a new version, migrate to a new or different platform or decommission the system altogether.

access to systems, the Enterprise Resource Planning (ERP) suite and other cloud-based applications use additional and stand-alone authentication requirements.

Cloud computing takes services from within an organization onto shared systems. These applications are usually accessed through the internet. As a result, the cloud infrastructure is managed and maintained by the cloud service provider, rather than the Global Fund, with additional authentication requirements.

The diagram below provides an overview of cloud computing arrangements at the Global Fund:



Change management is undertaken through a web-enabled solution which is utilized for both infrastructure and application updates and changes. A Change Control Board has been in place since 2014 and uses a web-enabled solution as the backbone to manage all incidents, maintenance and change requests. The Board meets every week to approve system developments/ changes into production, to evaluate readiness to deploy, to ensure release discipline and to approve or reject changes.

2.3. IT Organization at the Global Fund

There are two main teams within the Global Fund's IT Department: a customer facing delivery team and a service provider delivery team. The customer facing delivery team provides IT support to Global Fund business units while the service provider oriented teams are responsible for technical and maintenance services and data integration. Each team is led by a Business Partner Manager with overall responsibility for the performance management of the cloud and non-cloud supplier services supporting their respective portfolios.

The responsibility for software licensing rests with the Technical Infrastructure Maintenance Services team. The IT Department is headed by a Chief Information Officer with responsibility for IT strategy and governance, who reports to the Chief Financial Officer. In addition, cross-cutting areas including Information Security, Strategy and Architecture, business and project management teams report directly to the Chief Information Officer. The total IT operating and infrastructure budget for 2017 is US$31.3m.

3. The Audit at a Glance

3.1. Objectives

The overall objective of this audit is to provide reasonable assurance on the adequacy and effectiveness of IT controls at the Secretariat, with a particular focus on cloud computing.

The audit specifically assessed whether the:

- IT framework and strategy for cloud services are designed adequately in line with business and operational needs;
- risks associated with cloud computing are effectively managed; and
- IT controls at the Global Fund and the cloud providers are adequate and effective for optimal performance and security.

3.2. Scope

This audit included:

- a review of strategy documents and the Secretariat's management of risks associated with cloud services;
- a review of IT policies and processes at the Global Fund;
- an assessment of the Secretariat's assurance mechanisms for cloud service providers;
- interviews with selected business owners of applications on the cloud;
- validation of IT architecture and controls of six key cloud applications; and
- a review of 82 control areas across the six sampled cloud applications covering application security, data security and integrity, system user access, incident and maintenance management, system development, knowledge management and disaster recovery planning.

The audit team did not visit the cloud service providers, however, it reviewed independent third party certifications on the controls implemented by the service providers.

3.3. Progress on Previously Identified Issues

The OIG conducted an audit of the 'Effectiveness of IT Controls in 2015 (GF-OIG-15-020) which focused on data access, accuracy, agility and availability. A follow-up audit took place in November 2015 (GF-OIG-15-020B). The risks identified from those audits relating to the IT applications that existed at the time have been addressed. However, there are potential emerging risks since the IT environment has changed.

Previous relevant OIG audit work

Audit of the Effectiveness of IT Controls at the Global Fund GF-OIG-15-020

Audit of the Effectiveness of IT controls at the Global Fund (Follow-up Report) GF-OIG-15-020B

4. Findings

4.1. No strategy and implementation plan to support the adoption of cloud computing

The Global Fund first adopted a cloud computing solution in 2014 and had moved approximately 60% of its IT applications and services to cloud computing by the end of 2016. However, this decision was not informed by a comprehensive strategy and implementation plan.

Cloud computing has increased the availability of IT services and reduced the need to manage an on-site data center at the Global Fund. Most of the cloud-based applications use the security, back-up and disaster recovery capabilities of the service providers. The applications and software are regularly updated by the service providers.

The Management Executive Committee endorsed an IT Strategy for 2014-2016 in September 2014. However, the strategy did not cover the use of cloud computing by the Global Fund. There was no needs assessment, cost benefit analysis or risk analysis of cloud computing before or after its implementation. An implementation plan has not yet been developed to identify the nature of the services required and the timelines for the roll out of various cloud computing services. This has compounded already fragmented IT infrastructure and services and poor application integration. The IT Department currently does not have one single view of IT architecture covering all applications and services operated through the cloud. An architecture framework is required to ensure that IT strategy, design and planning decisions are accurately taken. The absence of an architecture framework can impact the sustainability and support for systems as well as increasing costs through inappropriate investments or more maintenance costs.

Long term implications of cloud computing: The long-term effects of cloud services are yet to be assessed and considered by the organization. The adoption of cloud computing inevitably has an impact on IT resources (number and skills set of staff, and infrastructure) required by the organization. These implications still need to be assessed. With respect to long-term service availability, not all IT decisions have been aligned to cloud computing. For instance, even after the adoption cloud computing, the Global Fund has continued to procure some software applications that are not aligned to its new cloud orientation. This creates continuity, latency and availability risks if the client server for the non-cloud application is not operating or available.

Monitoring whether cloud computing is meeting its objectives: The Global Fund has not assessed whether the benefits of cloud computing have been achieved since its adoption in 2014. This is mostly because the rationale for the adoption of cloud computing was never defined. Changes in Chief Information Officers and IT staff require that the basis of major IT decisions are documented to enable successors to effectively implement and evaluate decisions on key areas such as returns on investment. Assessing results against defined objectives enables the organization to identify areas for self-correction within a reasonable time.

The root causes of the gaps in the cloud strategy and implementation plan are due to the limited IT governance mechanisms at the Global Fund. There are no established governance structures to review and approve major IT decisions at the Global Fund. An Enterprise Architecture Board was founded in May 2016 by the Chief Information Officer to improve IT governance. The Enterprise Architecture Board consists of the Chief Information Officer, IT Project Management Office and IT Business Partner Managers with the objective of approving all enterprise technology decisions. However, the board has been unable to execute its role effectively for several reasons. The body was not recognized and accepted by the Secretariat's internal project steering committees as an information technology decision-making body within the Global Fund. Business process owners were not engaged on the roles and responsibilities of the board. In addition, required processes and assessment criteria of the board have not been fully developed. The lack of a formalized governance process means that the Board has not been involved in most IT decisions. The Management Executive Committee has not yet reviewed the adoption of cloud computing, defined the target objectives or progress against those targets, the risk trade-offs and mitigation of keys risks.

Agreed Management Action 1: As planned in the context of the Chief Information Officer's transition, the Secretariat will develop an IT Strategy that includes cloud computing. The Global Fund IT Strategy will define how the IT Department is organized and how it operates. The IT Strategy will set practical objectives for IT service quality, usability and acceptance. The Global Fund IT Strategy will be presented to the Management Executive Committee for approval.

Owner: Head of Finance, Information Technology, Sourcing and Administration Division

Due date: 31 December 2017

Agreed Management Action 2: The Secretariat will enhance IT governance mechanisms by overhauling the existing Enterprise Architecture Board. The Enterprise Architecture Board's organization, scope, terms of reference including membership, processes and decision criteria will be better defined as part of IT Strategy.

Owner: Head of Finance, Information Technology, Sourcing and Administration Division

Due date: 31 December 2017

4.2. Limited risk management for cloud computing

Cloud computing enables organizations to outsource the management of certain IT related risks to third parties. However, it also exposes the organization to other risk types such as data, supplier and legal risks which require proactive measures to mitigate them. The Global Fund needs to assess the potential risks arising from cloud computing and institute measures to mitigate them.

The Secretariat has transferred the responsibility for the day to day management of some operational IT risks to the cloud computing service providers. Operational responsibilities vary across the key suppliers depending on the contracts and nature of service but typically include back up and disaster recovery arrangements, on-going service management, software upgrades and deployment of applications. The Global Fund remains ultimately accountable for these risks and is expected to mitigate them through supplier management, performance management and controls assurance activities. Cloud computing also changes the risk profile of the organization and could result in data, supplier and legal risks which are yet to be assessed by the Global Fund.

Data management risks: Cloud computing results in data protection risks to the organization since it reduces control over how the service providers process data. Data protection is further complicated by multiple data transfers between systems and locations. This requires the Global Fund to define the nature and type of data (based on data classification requirements) that is maintained on the cloud and the minimum security requirements for its transfer. The Global Fund has not yet determined the type of data to be maintained on the cloud and related controls. This could result in sensitive information being held on the cloud without appropriate controls.

Whilst key system and application interfaces have been documented, the security specifications for these interfaces have not been identified and documented in the case of one key application. There are currently no defined minimum protection requirements for transfer of data onto the cloud. This has resulted in inconsistent security requirements adopted by the various system owners, which increases the organization's exposure to data quality and consistency risks. Where data is transferred between different locations and systems, there is a risk that it could be intercepted. This risk increases in shared cloud environments and could result in sensitive or confidential information being inappropriately accessed.

Supplier risk: The Global Fund is yet to perform risk assessment of the cloud service providers to determine the level of service risk and, consequently, what resources are required to manage the respective suppliers. This, and the absence of corporate measures to mitigate risks associated with cloud computing, has resulted in inconsistent practices by the Global Fund's IT Business Partner Managers responsible for managing key supplier relationships. For instance, there are inconsistent levels of assurance obtained over supplier controls by the system owners at the Global Fund. The Global Fund has not assessed or obtained independent third party certification over supplier IT controls for three out of the six key cloud applications since 2014. The standard industry practice requires that these certifications be performed at least every two years. These applications maintain authoritative grant data and are used as the main knowledge management systems of the Secretariat.

Where third party certifications have been obtained, the findings in the reports are not adequately followed up. For instance, an independent party's review of one of the key applications (used by nearly all Global Fund staff and over 400 grant implementers as of May 2017) identified major deficiencies in controls maintained by the supplier. However, there is no evidence that the Global Fund has followed up on the deficiencies to determine their impact on services received from the supplier and the potential mitigation measures required.

Legal risk: Cloud computing service providers store data in various locations to mitigate the risk of total loss in the case of data incidents or breaches. This exposes the Global Fund to a potential subpoena to disclose information in countries where the organisation does not have privileges and immunity. The likelihood and impact of this risk are yet to be assessed by the Global Fund. The IT Department has mitigated some of this risk by contractually requesting certain service providers to only store Global Fund data in Switzerland and the United States. However, the organization is still exposed due to the data storage and hosting arrangements for two of its major applications. The

existing contract for these applications allows the service provider to transfer data to countries where the Global Fund does not have privileges and immunity without the Secretariat's permission.

The IT Department completes a monthly risk report which is incorporated in a corporate risk register managed by the Risk Department. As indicated in an OIG audit report on Risk Management,[4] skills gaps in the Risk Department have affected their ability to ensure that technical IT risks have been identified and appropriate mitigation measures considered prior to the adoption of cloud computing solutions.

The Global Fund has initiated a process to develop an IT Security Regulations Policy to provide guidance on data transmission and other IT risks. A draft policy was prepared in January 2017 and is currently being reviewed by the IT Department. Once finalized, the policy will define and prescribe a set of measures to mitigate IT risks including those outsourced through cloud computing.

Agreed Management Action 3: The Secretariat will improve the management of IT risks by identifying the potential cloud computing risks, assess their impact and institute measures to mitigate them.

The identified risks will be mitigated through:

- The Sourcing Department's enforcement of existing procedure to ensure that the Legal and IT Departments are engaged in reviewing all future cloud related IT contracts.
- A review of the feasibility of amending the two contracts to address the identified gaps and to institute alternative measures to address the gaps if the contract negotiation outcome is not favorable.
- The use of measures such as the Enterprise Architecture Board to ensure that a disaster recovery plan is developed for the two IT applications identified in the review. The plans will be tested by the Global Fund's IT Department in coordination with the cloud service providers. The disaster recovery tests, which are executed twice a year, will ensure that the Secretariat data are not lost and remain accessible within the agreed service levels.
- A review, at a minimum every two years, of third party certifications for the three identified applications and follow up on any findings that may pose a risk to the Global Fund.
- Improvements in the process to monitor user activities through the identification of up to three activity exceptions to be monitored. The implementation of an alert mechanism to flag those exceptions on critical functions. This mechanism will be rolled out in a staggered manner across the identified cloud applications.

Owner: Head of Finance, Information Technology, Sourcing and Administration Division

Due date: 30 September 2018

Agreed Management Action 4: The IT Department currently completes a monthly risk report based on one risk indicator which is incorporated in the Global Fund Organizational Risk Register (ORR) maintained by the Risk Department. The IT Department will update the monthly risk report to incorporate the potential cloud computing risks and work with the Risk Department to have them appropriately incorporated in the ORR. The ORR is reviewed and approved by the Management Executive Committee on a quarterly basis.

Owner: Head of Finance, Information Technology, Sourcing and Administration Division

Due date: 30 September 2017

[4] Global Fund Risk Management Processes GF-OIG-17-010

4.3. Sub-optimal management of cloud service providers

The Global Fund's IT Department has assigned dedicated staff to manage various cloud services from market leading providers. Supplier management is focused on service availability and incident resolution. However, service level agreement for the grant management platform is not designed adequately to enable effective monitoring. Performance management of some critical aspects of one supplier contract covering virus detection and removal have been sub optimal.

Contracts are in place for all six applications reviewed. The Secretariat holds regular meetings with the service providers which focus on service and incident management to ensure service availability and delivery.

Performance Management of Cloud Suppliers: The Global Fund does not have a defined framework on which suppliers should be managed. This has resulted in varied practices by the respective IT Business Partner Managers. For instance, frequency of performance reviews, contract review meetings and escalation channels for issues identified are not defined. These have led to adhoc resolutions of identified issues by the IT Business Partner Managers. This impacts effective oversight and knowledge management within the IT Department.

Supplier performance is not reviewed against service level agreements for three out of the six applications. In the case of one supplier, the service level agreement covers key security requirements such as virus detection and removal, and spam effectiveness but compliance with these requirements is not periodically assessed.

There are opportunities for improvement in the maturity of the Global Fund's management of IT service providers. The IT Department has not conducted a risk assessment of the cloud service providers to determine their strengths, weakness and required performance management controls. The IT Department's discussions with suppliers are focused on price and delivery and have not developed on to shared objectives, risk management or support in delivery of the service.

Contract management: There are areas to improve in the terms of the contracts signed with service providers to support the secure and continuous availability of data across all applications. For instance, service availability and required security levels are not well defined in the contract and service level agreement for the grant management platform. In particular, one service level agreement does not have a specified lead time within which the supplier is required to restore services in the event of disruption. The service level agreement only indicates that the supplier should provide reasonable assistance to restore services.

The contract signed for two of the six applications does not have clauses for the supplier to disclose material risks that could impact service delivery or service security in line with industry practice. The inclusion of a risk disclosure, which is standard industry practice, mandates the service provider to proactively report any known or probable risks affecting its ability to provide the agreed services.

There are inconsistencies in the monitoring and follow up of key contractual obligations for the cloud service providers. While the key contractual obligations under the Treasury Management System and ERP are adequately managed, this is not the case for the service provider of two other key applications. In particular, data storage compliance, disaster recovery and back-ups for those applications are not followed up. The OIG acknowledges that the Global Fund has engaged well established and market leading suppliers for its cloud computing services. Consequently, it may have limited leverage in negotiating the terms of the contracts. However, the Secretariat is yet to explore the option to use existing and more favorable contract terms negotiated between United Nations-related entities and the major service provider used for two of the six applications reviewed.

Agreed Management Action: Refer to AMA 3

4.4. IT Access – Gaps in data access and security controls for cloud applications

The Global Fund has enhanced its password management practices and performed independent security checks for its ERP system and Treasury Management application. However, the management of user access rights and monitoring of cloud computing activities need improving.

IT security awareness and training courses have increased across the organization, with new policies due to be rolled out on information security and passwords. Training on an 'Information Security Awareness Program' for password and email security has been assigned to all Global Fund staff through an e-learning platform.

Management of user access rights: A segregation of duties matrix to define the access rights[5] of users has not been developed for two out of six key cloud applications. This limits the ability of the IT Department to routinely review the relevance of roles and responsibilities assigned to users of the applications. In the absence of a clear responsibility matrix, there is a risk of conflicting responsibilities between the accessible modules of the applications. As the use of cloud-based platforms continues to grow, inappropriate user access to specific functions in the applications could lead to the loss of data or sensitive information leaking through privilege user abuse.

Where a segregation of duties matrix has been prepared, there is no evidence that it is regularly reviewed by the IT Department and business process owners. Responsibility for user access rights on the documentation retention platform is assigned to site owners. The matrix is managed through an annual attestation by the site owners. However, the attestation does not include review of the appropriateness of roles and responsibilities assigned to the users.

Monitoring of computers activities: The cloud service providers regularly update the anti-virus and firewalls on the applications. However, there is limited monitoring by the IT Department, of computer user activity across all the cloud-based applications to detect unauthorized or malicious activities in a timely manner. The Global Fund's systems have audit trail functionality (such as computers logs and activity traceability) to support monitoring of computer activities. The IT Department only utilizes the audit trail functionality upon departmental request and does not proactively monitor areas such as high or unusual levels of user logins to specific applications. A detailed and comprehensive computer activity log would provide alerts for incident response purposes. It could be used to control the manner in which confidential data is used and shared as well as to detect any inappropriate use of data. The absence of such controls could affect the ability of the Global Fund to identify data leakage and detect unauthorized or malicious computer activities in a timely manner.

Agreed Management Action 5: Based on the segregation of duties matrix for the identified applications, the Secretariat will perform a formal review of the end-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 also be developed.

Owner: Head of Finance, Information Technology, Sourcing and Administration Division

Due date: 30 June 2018

[5] The management of user accounts, particularly those with special access privileges are essential to protect against misuse and unauthorized access. Accounts should be assigned only to authorized individuals and provide the minimum level of access to applications, computers and networks. (https://www.itgovernance.co.uk/access-control-and-administrative-privilege)

4.5. IT Data Accuracy – Weaknesses in the management of IT interfaces and encryption controls affecting data accuracy

The adoption of cloud computing and the fragmented nature of the IT architecture have created multiple interfaces which need to be identified and their security levels evaluated.

Cloud computing results in the transfer of data across multiple applications and systems. This requires that all the interfaces between the systems and applications be identified to ensure appropriate security controls are instituted. The Chief Information Security Officer started penetration testing across key departments and applications in the third quarter of 2016. Penetration testing is initiated by an organization to self-identify potential vulnerabilities in its IT infrastructure and systems that could be exploited by external parties and proactively institute measures to address the gaps. A risk-based penetration testing roadmap has been drafted for 2016-17 covering three main applications and functional areas. These include the grant management application, documentation retention system and Human Resource interfaces. Penetration tests are completed by an independent third party provider engaged to analyse systems and/or networks. Where cloud suppliers do not allow customer penetration testing, assurance is sought through relevant customer trust portals.

IT interfaces and reconciliation controls: There are multiple interfaces between the various applications used in the Global Fund. Some of these interfaces have not been clearly documented by the IT Department and reconciliation controls instituted to ensure consistency of data across the applications. There are opportunities for the IT Department to automate certain interfaces. For instance, the lack of an automated interface between the online and offline trading platforms of the treasury management system was identified in an OIG audit of Global Fund Treasury Management.[6] The absence of a complete and defined listing of interface and reconciliation controls can result in inconsistent data across the various applications. This could lead to use of incorrect data for decision-making.

Data encryption controls: The IT Department has not ensured consistent encryption controls across data transfers for all IT interfaces. The data encryption mechanism used to transfer data across cloud applications is at the discretion of each IT Business Partner Manager. As a result, there is a risk that insufficient levels of encryption levels may be used for the same information across the various systems. As data flows through systems, encryption is only as effective as the weakest link in the process.

Data encryption controls operated by cloud service providers are required to be certified by independent third parties through ISO 27001 reviews[7]. However, the Global Fund has not obtained these certifications from the service provider of its three main applications since 2014. This certification is required at least every two years in line with the industry's practice. With respect to the grant management platform where the certification[8] has been obtained, no action has been taken by the Secretariat despite the significant control gaps identified in the report. The Secretariat is developing an IT Security Regulations Policy to provide guidance on data transmission and related controls.

Agreed Management Action 6: In addition to agreed management action 3, the Secretariat will:

1. Leverage the existing Global Fund Information Classification and Handling Regulation to work with the data owners to ensure security specifications for the data transfers or interfaces are

[6] GF-OIG-17-001 Global Fund Treasury Management

[7] ISO 27001 is an information security standard published by the International Organization for Standardization focused on Information security management systems. Service Organization Control (SOC 2) reviews look at a service organization's controls over governance, risk, compliance, due diligence and oversight relevant to the security, availability or processing integrity of systems or the privacy or confidentiality of the information systems processes. SOC 3 reports are a trust services report for service organizations focused on security, availability, processing integrity, confidentiality and privacy of a service organizations systems.

[8] Supplier certification is an independent review of IT security controls and may take the form of an SSAE16 or a SOC 2 report.

documented for cloud applications identified in the review and reconciliation controls instituted. Proper level of information security will be implemented to meet the documented requirements.

2. Perform feasibility and cost-effectiveness analysis of automating critical manual interfaces for the identified applications.

Owner: Head of Finance, Information Technology, Sourcing and Administration Division

Due date: 30 September 2018

4.6. Improvement required in disaster recovery planning and testing for some cloud applications.

The Secretariat has made significant progress in its disaster recovery plans with some areas of improvement still needed. Following the OIG's audit of IT controls at the Secretariat in 2015, a disaster recovery plan was developed for the key applications that existed at that time. However, similar plans are yet to be developed for applications procured after the 2015 audit.

There are opportunities to improve the disaster recovery plans developed by the Secretariat. In conjunction with the cloud service providers, the Secretariat has developed and tested disaster recovery plans for the treasury management, grant management and ERP applications. The plans do not prioritise the information to be recovered in line with data classification. There is no evidence that business stakeholder engagements were incorporated in the recovery plan for the grant management application.

Disaster recovery plans are yet to be prepared for two of the six applications. In line with the contract signed with the service provider, the Secretariat remains responsible for the recovery of its data in the event of a disaster. The contract indicates that the supplier is not a disaster recovery specialist and the Secretariat should institute its own measures to recover data in the event of any system failure. However, the Global Fund currently has no mechanism to back up the data in those two applications stored on the cloud and there are no alternative plans to recover the data in the event of system failure. The applications hold the majority of Global Fund business documents and are used as the main knowledge management tools. Some of the documents in these applications include grant agreements, grant performance reports, contracts with service providers and electronic communication with various stakeholders. This risk materialised in December 2014 with a major documentation retention system storage incident. This resulted in the loss of access to documents and emails in some cases for over a week. Disaster recovery arrangements have materially improved since this incident with disaster recovery tests being performed regularly for applications held within the private externally hosted cloud.

Agreed Management Action: Refer to AMA 3

5. Table of Agreed Actions

Agreed Management Action	Target date	Owner
1. As planned in the context of the Chief Information Officer's transition, the Secretariat will develop an IT Strategy that includes cloud computing. The Global Fund IT Strategy will define how the IT Department is organized and how it operates. The IT Strategy will set practical objectives for IT service quality, usability and acceptance. The Global Fund IT Strategy will be presented to the Management Executive Committee for approval.	31 December 2017	Head of Finance, Information Technology, Sourcing and Administration Division
2. The Secretariat will enhance IT governance mechanisms by overhauling the existing Enterprise Architecture Board. The Enterprise Architecture Board's organization, scope, terms of reference including membership, processes and decision criteria will be better defined as part of the IT Strategy.	31 December 2017	Head of Finance, Information Technology, Sourcing and Administration Division
3. The Secretariat will improve the management of IT risks by identifying the potential cloud computing risks, assess their impact and institute measures to mitigate them. The identified risks will be mitigated through: o The Sourcing Department's enforcement of existing procedure to ensure that the Legal and IT Departments are engaged in reviewing all cloud related IT contracts. o A review of the feasibility of amending the two contracts to address the identified gaps and to institute alternative measures to address the gaps if the contract negotiation outcome is not favorable. o The use of measures such as the Enterprise Architecture Board to ensure that a disaster recovery plan is developed for the two IT applications identified in the review. The plans will be tested by the Global Fund's IT Department in coordination with the cloud service providers. The disaster recovery tests, which are executed twice a year, will ensure that the Secretariat data are not lost and remain accessible within the agreed service levels. o A review, at a minimum every two years, of third party certifications for the three identified applications and follow up on any findings that may pose a risk to the Global Fund. o Improvements in the process to monitor user activities through the identification of up to three activity exceptions to be monitored. The implementation of an alert mechanism to flag those exceptions on critical functions. This mechanism will be rolled out in a staggered	30 September 2018	Head of Finance, Information Technology, Sourcing and Administration Division

Agreed Management Action	Target date	Owner
manner across the identified cloud applications.		
4. The IT Department currently completes a monthly risk report based on one risk indicator which is incorporated in the Global Fund Organizational Risk Register (ORR) maintained by the Risk Department. The IT Department will update the monthly risk report to incorporate the potential cloud computing risks and work with the Risk Department to have them appropriately incorporated in the ORR. The ORR is reviewed and approved by the Management Executive Committee on a quarterly basis.	30 September 2017	Head of Finance, Information Technology, Sourcing and Administration Division
5. Based on the segregation of duties matrix for the identified applications, the Secretariat will perform a formal review of the end-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 also be developed.	30 June 2018	Head of Finance, Information Technology, Sourcing and Administration Division
6. **In addition to agreed management action 3,** the Secretariat will: 1. Leverage the existing Global Fund Information Classification and Handling Regulation to work with the data owners to ensure security specifications for the data transfers or interfaces are documented for cloud applications identified in the review and reconciliation controls instituted. Proper level of information security will be implemented to meet the documented requirements. 2. Perform feasibility and cost-effectiveness analysis of automating critical manual interfaces for the identified applications.	30 September 2018	Head of Finance Information Technology Sourcing and Administration Division

Annex A: General Audit Rating Classification

Effective	**No issues or few minor issues noted**. Internal controls, governance and risk management processes are adequately designed, consistently well implemented, and effective to provide reasonable assurance that the objectives will be met.
Partially Effective	**Moderate issues noted**. Internal controls, governance and risk management practices are adequately designed, generally well implemented, but one or a limited number of issues were identified that may present a moderate risk to the achievement of the objectives.
Needs significant improvement	**One or few significant issues noted**. Internal controls, governance and risk management practices have some weaknesses in design or operating effectiveness such that, until they are addressed, there is not yet reasonable assurance that the objectives are likely to be met.
Ineffective	**Multiple significant and/or (a) material issue(s) noted.** Internal controls, governance and risk management processes are not adequately designed and/or are not generally effective. The nature of these issues is such that the achievement of objectives is seriously compromised**.**

Annex B: Methodology

The OIG 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 documents 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 at the Global Fund as well as in country, 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.