Aidspan
Independent observer of the Global Fund

# SIGNIFICANT IMPROVEMENTS REQUIRED IN MANAGING CLOUD COMPUTING AT THE GLOBAL FUND, OIG SAYS

While the Secretariat has improved its IT controls since the last IT audit conducted by the Office of the Inspector General (OIG) in 2015, significant improvements are required in two areas: (a) designing a cloud computing strategy; and (b) managing the risks associated with cloud computing.

The OIG recently concluded an audit on cloud computing at the Global Fund. A report on the audit was released on 28 June 2017 (see GF-OIG-17-013).

The audit report defines “cloud computing” as the delivery of on-demand computing resources, ranging from applications to data centers, over the internet on a pay-for-use basis. 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.

Overall rating

The growth of cloud computing has improved the flexibility of IT operations through better availability of services, the OIG said. “However, the absence of an overarching strategy and limited management of associated risks have affected the effective roll out of cloud computing.” The OIG concluded, therefore, that significant improvement is needed to (a) design a cloud computing strategy aligned to the Global Fund’s business needs and (b) to manage the related risks.

The OIG said that the Secretariat has improved its IT controls since the last OIG IT audit, though there remain areas for improvement in cloud computing-related data access and accuracy. Nevertheless, the

OIG said, no significant instances of data loss or service interruption have occurred since 2015. The OIG concluded, therefore, that the basic IT controls are partially effective.

The four tiers in the OIG's rating scheme are "effective"; "partially effective"; "needs significant improvement"; and "ineffective."

Editor's note: There are two reports on the 2015 audit: (1) "Effectiveness of IT Controls at the Global Fund," 11 March 2015; and (2) "Effectiveness of IT Controls at the Global Fund (Follow-Up Report)," 26 November 2015. In the OIG's database of audit and investigations reports, both reports, though listed separately, bear the same date (26 November 2015) and the same number (GF-OIG-15-020).

Findings

The OIG noted that the Global Fund's IT Department has grown significantly since 2015, in line with the business needs of the organization. The OIG said that basic IT controls have improved since the last OIG audit. 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."

The OIG said that 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 OIG observed. In addition, it said, the Secretariat has 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."

Cloud computing has increased the availability of IT services and reduced the need to manage an on-site data center at the Global Fund, the OIG said. 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.

Risk management

Cloud computing generally results in the transfer of several IT risks to a cloud services provider, the OIG said. 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, the OIG said, cloud computing enables the Global Fund to store data in various locations, which reduces the risk of total loss in case of a significant data incident. At the same time, however, there may be 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 that could subpoena its records. Furthermore, the OIG said, 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," the OIG said.

Governance

The gaps in the cloud strategy and implementation plan are due to the limited IT governance mechanisms at the Global Fund, the OIG said; there are no established governance structures to review and approve major IT decisions. The OIG noted that an Enterprise Architecture Board was founded in May 2016 by the Chief Information Officer to improve IT governance. The board consists of the Chief Information Officer,

the IT Project Management Office and IT business partner managers. However, the OIG said, the board has been unable to execute its role effectively for several reasons, including the fact that the body was not recognized and accepted by the Secretariat's internal project steering committees as an IT decision-making body within the Global Fund.

"The lack of a formalized governance process means that the [Global Fund] Board has not been involved in most IT decisions," the OIG said. "The Management Executive Committee has not yet reviewed the adoption of cloud computing, [or] defined the target objectives or progress against those targets, the risk trade-offs and mitigation of keys risks."

Disaster recovery

Following the OIG's audit of IT controls in 2015, disaster recovery plans were developed for the key applications that existed at that time, including the treasury management, grant management and enterprise resource planning applications. The OIG said that these plans should be improved. The plans do not prioritize the information to be recovered in line with data classification, the OIG said. As well, there is no evidence that business stakeholder engagements were incorporated in the recovery plan for the grant management application. (A spokesperson for the OIG explained to Aidspan that the OIG believes there should be a consultative approach to designing and negotiating a disaster recovery solution based on business-critical priorities.)

Disaster recovery plans have yet to be prepared for two applications procured after the 2015 audit, the OIG said. For these applications, in line with the contract signed with the service provider, the Secretariat remains ultimately responsible for the recovery of its data in the event of a disaster. However, the Global Fund currently has no mechanism to back up the data in those two applications and there are no alternative plans to recover the data in the event of system failure.

According to the OIG, these two 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. The risk of data loss materialized in December 2014 when there was 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 actions

In response to the OIG's findings, the Secretariat has agreed to implement several actions, including the following:

- Develop an IT strategy with clear objectives for approval by the Management Executive Committee.
- Enhance IT governance mechanisms through an overhaul of the existing Enterprise Architecture Board.
- Improve 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 Organizational Risk Register which is reviewed by the Management Executive Committee on quarterly basis.
- Develop a segregation of duties matrix for outstanding applications and further enhancements and testing of disaster recovery plans.

Read More