



Audit Report

Audit of the Global Fund's Grant Operating System

GF-OIG-20-014
3 June 2020
Geneva, Switzerland

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; and human rights violations...

Online Form >

Available in English, French, Russian and Spanish

Email:

hotline@theglobalfund.org

Letter:

The Office of the Inspector General
The Global Fund
Global Health Campus
Chemin du Pommier 40
1218 Grand-Saconnex
Geneva, Switzerland

Free Telephone Reporting Service:

+1 704 541 6918

Telephone voicemail:

+41 22 341 5258

More information about the OIG

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	4
1.1.	Opinion.....	4
1.2.	Key Achievements and Good Practices	4
1.3.	Key Issues and Risks	5
1.4.	Rating	5
1.5.	Summary of Agreed Management Actions	6
2.	Background and Context	7
2.1.	Overall Context.....	7
3.	The Audit at a Glance.....	8
3.1.	Objectives	8
3.2.	Scope	8
4.	Findings	9
4.1.	Inconsistencies in system development and testing have impacted the efficient and effective use of GOS	9
4.2.	Weaknesses in incident management impacting the efficient and effective use of GOS....	12
4.3.	Insufficient organizational readiness to continue enhancements to GOS, post-Project AIM	15
4.4.	Gaps in IT controls and processes to safeguard GOS as a core system	18
5.	Table of Agreed Actions	20
	Annex A: General Audit Rating Classification	21
	Annex B: Methodology.....	22

1. Executive Summary

1.1. Opinion

Since 2015, the Global Fund has invested significant resources into developing a customized grant operating system (GOS), an enterprise resource planning tool which allows the Global Fund Secretariat to manage and monitor grants on a cloud-based platform. The system also allows external parties such as Local Fund Agents to access particular modules to support improved collaboration and faster information sharing in a structured manner. In the absence of in-house technical skills, the project has been mainly developed by external vendors, with the Global Fund's IT department playing a larger role from 2018 onwards.

The development and roll out of GOS represents a positive evolution in the Secretariat's operating model. The investment has provided the Global Fund a more integrated and effective system to support the Grant Management lifecycle. It has also catalyzed further improvements more broadly across the organization's grant management processes. There have been substantial organizational efforts to complement the new system with related improvements to policies, processes and data flows. This has enhanced the ability to monitor grant processes and has led to better defined roles and responsibilities across the organization in relation to key grant management activities.

Project AIM (Accelerated Integration Management), the name of the project to deliver GOS between 2016-19, allowed the organization to tackle issues including a heavy reliance on manual processes, a highly fragmented IT landscape to support grant management, and a lack of a holistic view across portfolios. GOS now supports each stage of the grant lifecycle through a single platform, standardizing delivery and integrating grant management and financial systems. GOS has simplified the IT system landscape and enhanced reporting capabilities for decision making. GOS processes have been customized to enable them to keep pace with organizational developments such as differentiated portfolio management, risk management assessments and new funding request modalities. While there have been some delays in the roll-out of some GOS capabilities, delivery has been designed in order to meet critical grant lifecycle milestones.

Several of the issues in this report have been self-identified by the Secretariat, including issues with user experience, system development and testing, and effective resourcing. The IT department has launched a new IT strategy aiming to create a vendor management office and strengthen project management. In addition, subsequent to this audit, the IT department has launched an RFP process to relook at vendors to undertake components of GOS incident management, which will potentially improve the quality of service to users over time.

While the system itself is functional, issues remain in systems development and lifecycle controls, and incident management is still weak. This has limited country teams' ability to optimally use GOS and has impacted the effectiveness and efficiency of GOS, which are rated as **partially effective**.

The dismantling of Project AIM's governance, oversight and support without appropriate mitigations has created risk and delivery pressure on current operations and future GOS module launches. The launch of the first module since the AIM project was closed has seen delays of 3 months, impacting the planned roll out and post-launch safeguards. There is limited accountability across Secretariat functions to ensure deadlines are met, due to unclear roles and responsibilities and capacity limitations. The governance structures and capacity to continue GOS's delivery and support are rated as **partially effective**.

1.2. Key Achievements and Good Practices

GOS has been rolled out as the Global Fund's enterprise resource tool for Grant Management, replacing several legacy systems and enabling more efficient and effective management of grants.

GOS represents a fundamental shift in the execution of grant management activities, moving away from manual processes to managing the grant lifecycle through a single solution. GOS had led to a more standardized and consistent approach to grant management, promoting better alignment and adherence to Global Fund Policies and processes. It has also supported the embedding of key grant management concepts across the grant life cycle, e.g. ensuring risk management principles are considered at key points. It has catalyzed significant changes in data management, governance and data analytics, and has led the way for more sophisticated reporting systems to be launched.

Significant development work was undertaken to deliver GOS under AIM Phase 1 and 2. Since 2016, numerous modules have been launched that have built system capabilities across Grant Management, Risk, Access to Funding, and Finance. The design of Project AIM governance and oversight structures to deliver GOS was strong, with regular project engagement with senior management. Project AIM has also seen increasing levels of maturity through stronger vendor contracts, positive trends in incident management resolution times, and the prioritization and execution of change management and training.

1.3. Key Issues and Risks

Prior to the audit, the Secretariat completed a self-assessment to communicate key issues related to the project and GOS delivery. Whilst management has been proactive in identifying issues and evaluating key risks, several of those issues have not been sufficiently mitigated.

User experience is a challenge, with inconsistent user interfaces and a lack of integrated visualization across modules. This has required end-users to input the same data multiple times, reduced user adoption, and increased error rates, often taking time to resolve. Gaps in system development quality controls and internal guidance across the audit period have negatively affected users. Some GOS modules launched with serious bugs which were left unresolved, contributing to user issues during live production. Similarly, inconsistencies in **GOS systems testing** have contributed to a negative user experience of the system.

Despite recent GOS launches being significantly larger than original assumptions, these will not all have the supporting governance and oversight of Project AIM. Instead, respective module owners are leading the development of these releases through their routine arrangements and with the available staff. Thus, the **organizational readiness** to simultaneously resolve historic issues, maintain the system, and expand GOS is in question. The audit highlighted challenges in timely project delivery, post-Project AIM. Launch timing and sequencing will be crucial for country teams to use the system in line with grant lifecycle requirements. In addition, risks were self-identified around the strategic approach, the long-term vision for GOS, and the level of module integration.

Regarding other GOS-related IT controls, management has highlighted the absence of a policy and limited effectiveness of controls over user access, although with no mitigating action plan.

1.4. Rating

	<p>Objective 1. Governance structures and capacity in place to continue delivery and support of GOS.</p> <p>OIG rating: partially effective.</p>
	<p>Objective 2. Efficiency and effectiveness of the delivery of GOS to support the Global Fund Secretariat in achieving its corporate objectives and the assessment of relevant IT controls.</p> <p>OIG rating: partially effective.</p>

1.5. Summary of Agreed Management Actions

The Global Fund Secretariat will work stakeholders on agreed management actions that will focus on the following areas:

- A clear Systems Development Life Cycle operational methodology
- Comprehensive guidance and targets on incident management and resolution
- Key policies on user access management and disaster recovery and backup
- Governance requirements to be adhered to for future launches

2. Background and Context

2.1. Overall Context

The Grant Operating System (GOS) is the Global Fund's core platform to manage grants throughout their lifecycle (e.g. funding request to grant closure) including the entry and recording of electronic approvals on key grant life cycle controls. It houses modules relating to grant risk management, interfaces with other Global Fund systems that are used for disbursements, and contains key master data sets for the organization. GOS was delivered through a project management approach, the outcome of a project called Accelerated Integration Management (AIM). Project AIM sought to integrate and align Global Fund processes and data, replacing several legacy systems to support efficient portfolio management. The project benefitted from a well-designed governance structure with senior management involvement, oversight and endorsement. Project AIM was launched in September 2015 after an earlier project, the Grant Management Platform (GMP), failed.

GMP, launched in 2014, aimed to develop a portal for implementing the New Funding Model on a Salesforce platform. It was halted in September 2015 after a detailed assessment highlighted a lack of project structure and governance, causing the project to fail on several dimensions. The review led to the launch of Project AIM, which retained a few residual elements of GMP; the Salesforce platform was retained to develop GOS and an original version of Salesforce used for GMP was partially used to host the Local Fund Agents portal until 2018.

Project AIM used an agile methodology¹ for systems development. Phase 1 was initially planned to take 12-18 months. By the end of 2017, Phase 1 was completed after delivering seven incremental releases which covered most grant lifecycle processes and prepared the launch of an Integrated Risk Module (IRM). AIM Phase 1 was managed by a joint-project team, with a single supplier contracted for all releases and mainly Grant Management Division staff. The Grant Management Division in close collaboration with the selected suppliers led both AIM Phase 1 and 2, as opposed to the IT department. However, there was a continued and progressing involvement from IT in all technical aspects of the project from Phase 1 to Phase 2. AIM Phase 2, designed to consolidate previous releases and new functionalities, was launched at the beginning of 2018. It involved a consolidation phase, delivered two releases, and enhanced the Finance module. Phase 2 was governed similarly to Phase 1 and managed by an extended project team – under Phase 1 and Phase 2 the main supplier was Deloitte (with IBM supporting the IRM module), with extensive involvement from both Grant Management and IT, alongside other business functions including Risk and Finance.

At the end of 2018 a decision was taken to transition GOS from Project AIM to business as usual. An exit strategy from Project AIM was prepared² and the transition took place in June 2019. The exit strategy plan, prepared and agreed within the Secretariat, proposed eight operational launches for the grant lifecycle 2020-2022. The first launches were initially planned to be delivered in July 2019 (Allocation and Funding Request) and in January 2020 (Grant Making³). Following project stakeholder consultations, the releases were rescheduled for September 2019 and February 2020. Since 2016, the Global Fund has invested US\$16.3m⁴ to develop this customized system to manage grant lifecycles.⁵ It has also incurred additional costs of US\$6.6m (US\$1.6m yearly) for licenses and incident management & support. In October 2019 there were over 2,300 Salesforce platform users⁶: two-thirds are external users (Partners, LFA Portal users), and the remaining third are internal GOS users, split between Country Teams and other Global Fund staff.

¹ Agile methodology delivers requirements in a prioritized order using short, fixed-duration 'sprints' to provide regular delivery of working software.

² AIM Steerco 21 – 06 December 2019.

³ Including Integrated File Handling

⁴ Staff time and level of effort dedicated to/ after Project AIM has not been quantified in monetary terms, nor was included in the investment costs above.

⁵ The full investment made in previous solutions (e.g. Grant Management Platform) is not available, due to limited project costing and institutional memory in 2015.

⁶ GOS is branded as GOS to internal Global Fund Secretariat users only and a Salesforce portal to external users

3. The Audit at a Glance

3.1. Objectives

The overall objective of the audit is to provide reasonable assurance to the Board on the strategic and operational delivery of the Grant Operating System (GOS). Specifically, the audit aims to assess the:

- governance structures and capacity in place to continue delivery and support of GOS;
- efficiency and effectiveness of the delivery of GOS to support the Global Fund Secretariat in achieving its corporate objectives, and the assessment of relevant IT controls.

The audit focused on the current and future framework for the delivery and ongoing roll-out of GOS launches. In order to leverage insights, the audit reviewed key aspects of the delivery of GOS from 2016 to 2019, including lessons learnt from relevant pre-GOS projects.

3.2. Scope

The audit methodology includes:

- review of relevant documents, including Project AIM and vendor documentation;
- analysis of progress, delivery, governance, resourcing, financial and operational challenges;
- interviews with Secretariat, external auditors and other key stakeholders;
- user survey⁷ and a workshop with core GOS users;
- testing of General IT controls (GITC) including user access, incident management and maintenance, systems development and testing, knowledge management and disaster recovery.

The audit scoped out:

- GOS Recoveries module - covered in the OIG's 2019 Recoveries audit;
- Data Governance, Data Management and Data Quality – covered in the OIG's 2018 "Data Management audit";
- Business controls around key Secretariat processes - covered through OIG's 2017 "Grant Monitoring audit" and other upcoming Secretariat process audits.

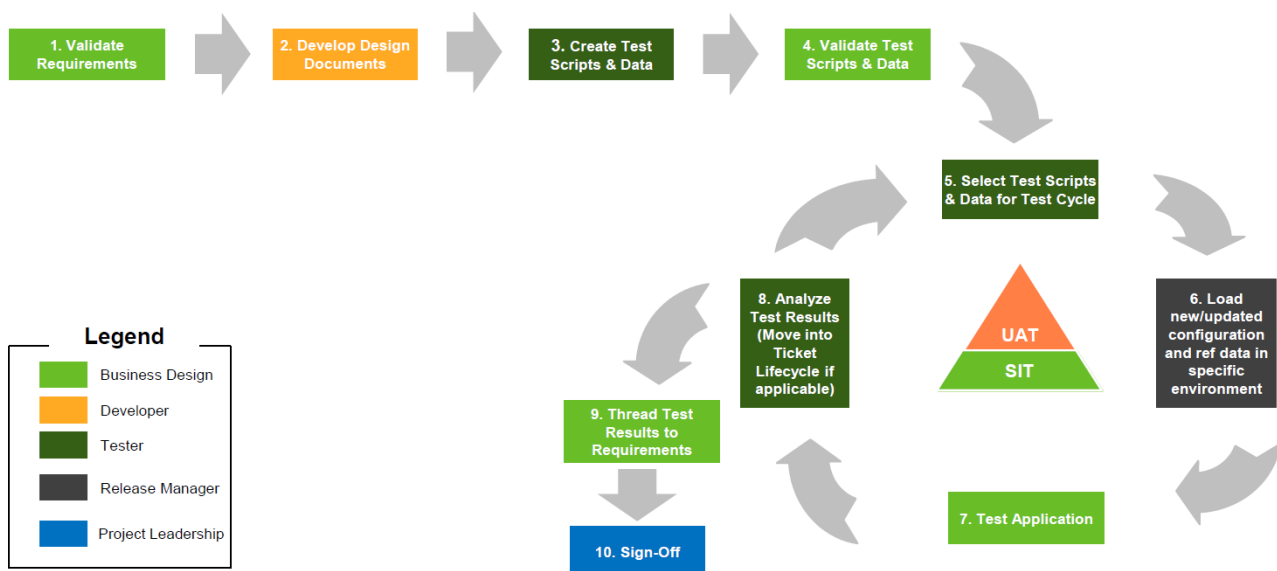
⁷ The survey was open to the most frequent users of GOS (Global Fund Secretariat staff members)

4. Findings

4.1. Inconsistencies in system development and testing have impacted the efficient and effective use of GOS

The launch and roll-out of the Grant Operating System (GOS) is by far the most material system launch the Global Fund has undertaken. As GOS is based on a highly customized Salesforce platform, Systems Development Life Cycle (SDLC) activities are crucial to the effective delivery, roll-out and maintenance of the system. SDLC activities are a sequence of phases that must be followed in order to convert business requirements into an IT system or application. The SDLC process typically includes requirements, design, implementation, testing, and checkout phases – see *Figure 1*. Several models can be used for SDLC. Project AIM selected and used the Agile methodology for systems development. This approach delivers requirements in a prioritized but flexible manner, using short ‘sprints’, to provide regular delivery of working software. After launch (or Go-Live) the system goes through a Hypercare period⁸, a critical component to ensuring a functioning system. Project AIM introduced the Global Fund to SDLC principles and framework, which were not adhered to on previous organizational systems. While SDLC principles and framework have become more embedded, the operational application of the SDLC for the GOS system has not, due to the lack of operational guidelines.

Fig. 1: Systems Development Life Cycle used for GOS – Steerco materials



Despite change management and user training being prioritized, limited oversight and insufficient rigor over system development and testing during AIM phase 1 and 2 have impacted the efficient and effective use of GOS, and the overall user experience. 66% of surveyed users rated the design and roll-out of multiple training materials⁹ as “good” or “very good”¹⁰, however, user experience has been partially affected by weaknesses in System Development and Testing for some GOS modules.

Deficiencies in system testing have affected the overall benefits of GOS impacting the user experience

User experience refers to the quality of a user's interaction with, and perceptions of, a system. Overall, 77% of surveyed users described GOS as currently “very useful” or “useful”, and 65% of surveyed users said GOS was “very good” or “good” at providing more structure and discipline around rules and policies than existed previously. However, issues with GOS user experience were

⁸ Hypercare represents the stabilization period after a system launch. It focuses on customer support, data integrity and system stability.

⁹ GOS training sessions, hand-outs, videos and clinics were prepared in 2017. Over 65% of staff attended GOS training sessions in 2017 and 2018.

¹⁰ OIG launched a user satisfaction survey on GOS, receiving feedback from 176 GOS users in the Secretariat.

identified through GOS ticket analysis and the OIG survey, through user interviews, and in the Secretariat's own self-assessment. These issues include the inability to import key documents to the system, data duplication, the need to input the same data across different modules, and the unavailability of templates. These issues result in the need for regular assistance, guidance, training and repetitive tickets. The Integrated Risk Management (IRM) and Grant Implementation modules were highlighted as the most challenging: 69% of users rated IRM module usability for data entry and review as "needing improvement" or "poor", while 74% of users said the latter module required manual workarounds or offline approvals.

Operational guidance around SDLC testing standards and criteria has not been defined by the Secretariat. Thus, GOS testing methodology is driven by the individual teams supporting launches and the vendor contracted for each module, resulting in inconsistent levels of quality and testing. Inconsistencies were noted across the IRM¹¹ and Grant Revisions¹² modules in the number of passes required in the User Acceptance Testing (UAT) stage to proceed to Go Live. On a sample of user stories selected across modules launched under AIM Phase 1 and 2¹³, OIG identified differences in the pass levels required between different test scripts, and low levels of users completing testing during UAT. In some instances, test passes were recorded even though 50% of the test steps could not be performed. There were cases where the final round of UAT failed, but with no documented tickets raised or additional testing re-performed.

These deficiencies in system development and testing have contributed to sub-optimal system performance at launch. This has led to a number of post-launch defect tickets for users of the Master Data, Grant Revisions, Grant Closure and IRM module functionalities. Issues noted included the consistency of GOS options available using different internet browsers, documents that could be deleted from the system following validation, budget revisions not being reflected, and issues in utilizing and updating the risk management module for some High Impact and Core Countries¹⁴.

Inadequate governance and oversight over system development activities

A production tracker is an agile project management and development life-cycle application for tracking all system development activities. A production tracker was used throughout GOS development phases, however historic data was not available to OIG due to an incomplete migration of data from early module releases.¹⁵ As a result, OIG is unable to provide comprehensive assurance that agreed SDLC testing principles were followed for all releases under AIM Phase 1. Based on the data available for releases under AIM Phase 2, OIG identified omissions of key data fields in the production tracker. These included the absence of audit trails detailing how some testing failures were addressed, the lack of a hierarchy for all releases and associated user stories¹⁶, and incorrect timestamps for key activities. These issues occurred despite the initial tracker contract highlighting the need to retain copies of all information, as the tracker is not a document repository.

There was a lack of oversight and quality-assurance controls around the closure of key SDLC activities prior to launch. Controls were missing that would have ensured the adequate classification and remediation of issues before modules were launched and checks to ensure that the Steerco documents accurately reflected the system's status, in line with the production tracker. This resulted in issues with the launch of the IRM Module, for which there was a clear disconnect between the status of the system per production tracker and what was reflected to the Steerco at the time of go-live. A control gap was also identified, with no conditional approval to ensure that issues were resolved following Steerco approval decisions. This resulted in unresolved tickets following the release of new modules. For example, when the IRM module was presented to the Project AIM

¹¹ The IRM module was launched in February 2018, under AIM Phase 1 with IBM as the supporting vendor

¹² The Grant revisions module was launched in May 2017, under AIM Phase 1 with Deloitte as the supporting vendor

¹³ These include the Grant Closure module (launched under AIM Phase 2, July 2018), IRM module (launched under AIM Phase 1, Feb 2018), Master Data Management (launched under AIM Phase 1, Feb 2017), IMM module (launched under AIM Phase 2, 2019) and consolidation launch (launched under AIM Phase 2, April 2018)

¹⁴ Issues in the ability to use the IRM module and update the Key Risk Matrix were noted by the OIG for the Nigeria, Angola and Liberia Portfolios.

¹⁵ Production tracker data for the majority of modules launched under AIM Phase 1 was only partially migrated.

¹⁶ During the consolidation phase - at the beginning of AIM Phase 2.

steerco in Q1 2018, 29 Critical, Very High or High open tickets had been logged in the production tracker¹⁷. These tickets were still open as of November 2019, even though the IRM module had been launched for more than 18 months. The IRM module was the only module which OIG could clearly identify as having material issues with managing tickets and bugs at the point of go-live. However, as noted in the previous paragraph, the status of tickets and bugs at go-live in the production tracker for the other AIM launches is not complete, and thus OIG cannot provide assurance that IRM was the only instance.

Agreed Management Action 1

The Secretariat will:

- ensure that a SDLC testing methodology is adopted, in line with ISO standards in order that testing for future releases meets required standards and criteria;
- ensure a stronger quality sign-off process is put in place to confirm that bugs in the Project Tracker are updated and all critical and high bugs are resolved prior to go-live for future releases.

Owner: Chief Information Officer

Due date: 30 June 2021

¹⁷ In addition to three acknowledged defects from User Acceptance Testing (UAT), this population also includes 13 tickets raised during System Integration Testing (SIT) but not closed off in Production Tracker and 13 tickets that were presented to the OIG as high-critical enhancements rather than bugs but with insufficient evidence provided to determine the correct classification

4.2. Weaknesses in incident management impacting the efficient and effective use of GOS

Incident Management is the practice of restoring normal service operation as quickly as possible, while minimizing impact to business operations and maintaining quality. Along with system development, testing and change management, it is one of the critical pillars required to support a system launch. The Global Fund uses the ServiceNow (SNOW) platform for incident management. Users raise tickets on incidents, which are then allocated to different ticket queues. GOS tickets follow a three-tiered technical support model.¹⁸ Tickets go through a triage process to ensure they are routed to the responsible parties and prioritized correctly¹⁹. Depending on the request type, GOS-related tickets are assigned to different support groups:

- Tickets for “Policy Question” and “Incorrect Data” go to different Global Fund teams²⁰;
- Tickets for “System Bug” and “System Navigation” are managed by IT, but resolution is currently outsourced to a vendor.

Tickets in ServiceNOW can also relate to required enhancements that are identified after modules have been launched, due to issues flagged by users.

Over 12,000 Salesforce and GOS-related tickets have been raised since 2016. Almost two thirds of them were raised in 2018 and 2019, linked to the expanding functionality of GOS with more modules being launched and the increased use of the ticketing platform. Critical and high priority tickets represent less than 7% of tickets in this period. Tickets raised in 2018 and 2019 took on average 22 days (for critical tickets) and 36 days (for high priority tickets) to be closed²¹. Despite an overall improvement of resolution time, the volume of total tickets remains high: 415 tickets for “System Bugs” and 820 tickets for “Incorrect Data” were raised between June and October 2019.

Fragmented and limited incident management targets, service level and associated resource planning

The Global Fund has not defined a corporate-wide, acceptable level of service for incident resolution, or the resourcing requirements needed to reach an acceptable level of support. Service Level Agreements have been created for parts of the support structure (e.g. IT support outsourced to IBM) but not for the GOS internal support structures managed by different Global Fund teams. As a result, there are no targets and no consensus on what time period to resolve a GOS ticket constitutes an acceptable level of service. In Q1 2019, the Operational Efficiency team completed a workload analysis that explored incident management staffing support, resulting in adjustments to capacity, but aside from this, no corporate wide-assessment has been completed to determine the levels of capacity and capability required for incident management support. The duration required to close critical and high tickets has affected end-users who suffered challenges with:

- Grant revisions module reflected in Annual Funding Decisions, impacting multiple grants
- Grant disbursement module and incorrect approvals in GOS, impacting countries and Multi-Country Grants
- Grant closures monitoring, impacting multiple grants
- Grant closure and the uploading of closure reports

The Secretariat has sought to mitigate the impact of these issues and ensure process timelines were met. Additional support was provided in the form of support sessions and walk-in clinics. However, the expected efficiencies from the embedding of processes into the GOS system were lost in these instances due to additional efforts being required either by the end-users or support teams.

¹⁸ Technical support levels: Level 1 is the initial support level responsible for basic customer issues; Level 2 is a more in-depth technical support; Level 3 is the highest level of support, responsible for handling the most difficult or advanced problems.

¹⁹ Four priorities are currently used for GOS tickets: Critical, High, Medium and Low.

²⁰ Mainly to Grant Management’s Operational Efficiency team (Level 1 and Level 2) and other departments (Level 2) depending on the owner of the GOS module

²¹ Since October 2019 an automatic closure process has been put in place ensuring closure 5 days after resolution date

Weak vendor management controls and oversight across incident management activities

The Global Fund is reliant on a materially outsourced model for both the delivery and support of GOS. However, there is no comprehensive vendor management approach or mechanisms to monitor and manage vendor services. Regarding incident management:

- Whilst vendor service level agreements detail key performance indicators and targets to be adhered to, the Global Fund does not have the reporting capabilities to hold vendors to account on their deliverables. Thus, there is no effective performance management.
- The incident management logging and tracking system has reporting limitations that do not allow for aggregated analysis of key fields, including the number of re-assignments of tickets or the timeframe to escalate tickets.
- Historic vendor contracts mainly for AIM Phase I, including the IRM Module and start of AIM Phase II, contained weaker exit criteria compared to vendor contracts of the most recent launches; initial vendor contracts required only critical and very high bugs to be resolved prior to a module launch. Whilst this is a risk-based approach, the required analysis - including cost and time impact for the remaining issues to be resolved through standard incident management protocols - had not been undertaken.

The above weaknesses limit the organization's ability to monitor both a vendor's effectiveness and the quality of service for end-users.

However, OIG did note improving trends in terms of the robustness of vendor contracts, with the latest vendor contracts signed in 2019 holding stronger exit criteria, ensuring that even medium bugs need to be resolved prior to a module launch. In addition, the revised IT strategy²² has given rise to the development of a Vendor Management Office within the IT department to strengthen vendor oversight. Subsequent to the audit, the IT department initiated an RFP process to re-select providers of incident management services to the organization.

Gaps in policy and guidance for incident management

Challenges around incident management resolution are compounded due to fragmented roles and responsibilities, which impact transparency and accountability. A responsibility matrix between grant management and IT is not adhered to and is not reflective of actual business practice. Tickets are assigned back and forth between the different support teams, with a lack of transparency to end-users awaiting resolution. As such, multiple stakeholders are involved with no accountability over resolution delays.

The lack of guidance on engagement with the ticket creator has resulted in communication gaps, with GOS users needing to follow up (by email or in person) on average 3.2 times to resolve their tickets, with some cases where users had to chase 10 times. The lack of policy guidance on the escalation of tickets results in ad-hoc approaches to ticket treatment. For example, there is no guidance for ticket escalation – when a ticket escalation should occur, who can and should elevate the ticket priority - impacting resolution times. A sample of OIG tickets²³ highlighted that tickets are reassigned on average 6.5 times²⁴ during the total time the ticket is open, causing delays in ticket resolution. Our analysis noted that:

- One mechanism used to shorten resolution times is to raise the priority of the ticket. This was undertaken for 62% of tickets (despite lag time), however there was no consistency on when the priority was increased.
- On average it took 25²⁴ days to increase ticket priority.

²² The 2017-2022 IT strategy was refreshed in 2019 to include new priorities including enhanced vendor management and project management

²³ 13 tickets were sampled to perform detailed analytical reviews. Manual testing was undertaken due to restrictions in the reporting capabilities of the Secretariat systems to reliably measure key elements across the entire ticket population. These tickets covered system bugs, support requests from users in relation to data issues as well as enhancements needed to resolve user issues.

²⁴ The analysis supporting this number excludes tickets that were related to enhancements that would by their very nature require a number of reassignments and do not follow the same needs around ticket prioritization

Agreed Management Action 2

The Secretariat will:

- implement policy and guidance on internal incident management protocols, including targets for resolution;
- ensure that incident monitoring capabilities are implemented to track incident management key performance indicators and the quality of issue resolution.

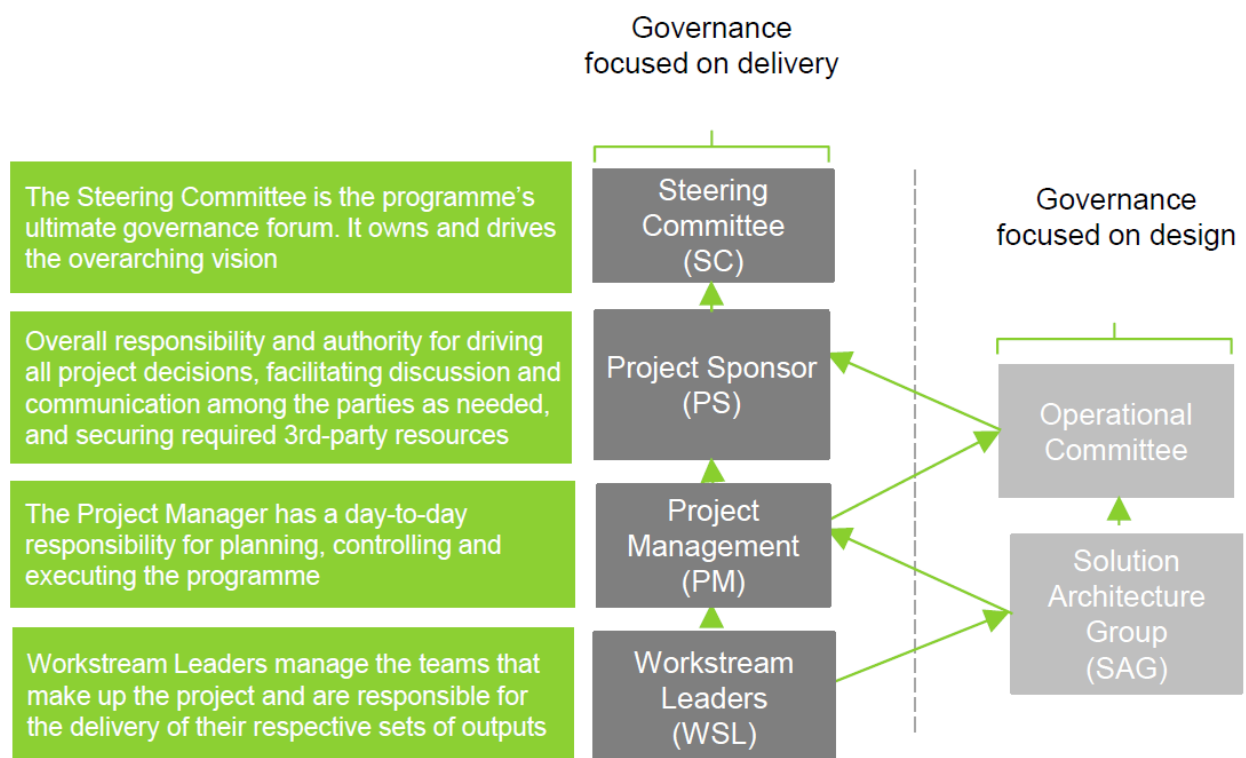
Owner: Chief Information Officer

Due date: 31 December 2020

4.3. Insufficient organizational readiness to continue enhancements to GOS, post-Project AIM

The Grant Operating System was delivered through a project management approach for most of its development under Project AIM. Its project management structure was housed mainly in the Grant Management Division, with a comprehensive governance structure with senior management involvement, oversight and endorsement, as detailed in Figure 2 below. The design of the governance and oversight structures for Project AIM was strong, and benefited from frequent engagement with Global Fund senior management. Project AIM was formally dissolved in June 2019, following a decision taken at the end of 2018. At that point, Project AIM had been running for over 27 months, had supported over 12 GOS releases²⁵ and overseen US\$17m spent on building and supporting the GOS platform²⁶.

Fig. 2: Project AIM governance structure – Steerco materials



Due to concerns over abruptly ending the project structure, Project AIM was extended by a further 6 months - until the end of June 2019 - extending the handover period whereby responsibility to manage GOS moved to other parts of the organization. This led to additional staffing support being granted in response to concerns raised at the Project AIM steerco level on the resources available to support the system going forward. This extension was a corporate decision to mitigate delays in operationalizing the first launch of GOS planned after Project AIM, as well as to allow time for new contracts to be signed with vendors for the maintenance of GOS.

At the start of July 2019, Project AIM's project management and project governance structures were dismantled, in line with the Global Fund's objective for GOS to become a business as usual (BAU) activity, as opposed to a project run by the Secretariat. The primary responsibilities for GOS platform development, maintenance and management were transferred to the IT department, at a time when the IT department was undergoing significant changes, including a restructure with headcount implications. This transformation covers all aspects of the IT department and will have implications

²⁵ AIM Steerco 21 – 06 December 2019.

²⁶ Financial information from Global Fund Finance Department – US\$ 12.4m investment, US\$ 4.6m in support and license costs and excluding internal staff costs which were not quantified in monetary terms.

on the management and support provided to the GOS system. The resourcing implications for GOS development and maintenance are not yet known at the time of the audit, as implementation of the changes is still ongoing. As part of the move to BAU, a determined effort has been undertaken to widen the competitive pool of vendors to support future GOS development, and to move away from overdependence on a small number of suppliers.

The disbanding of AIM's project management and governance structures might impact GOS's future delivery

The dismantling of key project management and governance structures was concluded without a clear understanding of GOS's current and future requirements in terms of governance, vendor management and in-house capacity and capabilities. Rather than being in a mature and stable state (in line with a Business-As-Usual approach) the GOS platform continues to require significant support and oversight to manage material launches and the resolution of historic outstanding issues.

Eight launches are planned over the next three years (2019-2022). The cost for the first two launches²⁷ is estimated at US\$1.5m, comparable to the average cost of each release under Project AIM. The US\$1.5m sum is 50% larger than anticipated when the decision to end Project AIM was taken. In addition, there have been several requirements to stabilize the GOS platform, whose completion was significantly delayed by several months after moving to BAU, impacting the level of support required to maintain the system. This is linked to stabilization requirements being deprioritized over other needs to support enhancements and new functionalities.

The revised Global Fund IT strategy is looking at options to strengthen project management and overall governance, which will benefit GOS management going forward, however the strategy was still not fully implemented at the time of the audit.

Human resources capacity and capability gaps to manage GOS, post-Project AIM

In line with the proposed changeover from Project AIM to a BAU model, the number of in-house staff and consultants directly involved in the management and support of GOS delivery was significantly reduced, from 26 FTEs²⁸ at the end of Project AIM to an estimated 14²⁹, with drops in both the Operational Efficiency team and the IT department³⁰. The absence of key in-house skills in critical areas such as system testing, Salesforce software architecture, and user experience, continues to impact the development of the GOS platform, as noted in finding 4.1. The gaps in capacity and capabilities are linked to the lack of a clear human resources needs assessment, skills gap analysis, and definition of additional capacity requirements to support the GOS platform. At the time of the OIG audit, the reassessment of HR needs of the IT department was ongoing, as part of the IT Strategy refresh finalized in October 2019.

Gaps in effective governance, knowledge management and oversight of GOS, post-Project AIM

Under Project AIM, there was a strongly designed governance and oversight structure, materialized through numerous Steering Committee meetings, under which cross-departmental activities were coordinated, monitored and approved to advance development of the GOS platform. In contrast, the first GOS release after Project AIM (Launch 1) had no steering committee to ensure effective coordination and collaboration between different Secretariat departments. Only operational meetings between the process owner, IT and the contracted supplier were held on a routine basis. The retention and transfer of knowledge between new vendors working on different launches is a risk that has not yet been mitigated in the absence of rigorous vendor management. This illustrates limited leverage of lessons learnt from previous projects. GOS's precursor, GMP, also faced critical gaps in governance and oversight that ultimately resulted in project failure.

²⁷ Cost of vendor contracts for Launch 1 and Launch 2, post Project AIM.

²⁸ Full Time Equivalent (FTE) is the number of hours worked by one employee on a full-time basis. At June 2019 there were 17 OE/AIM related staff and 9 IT/AIM related staff per the Project AIM final Update June 2019

²⁹ At December 2019 there were projected to be 10 OE/AIM related staff and 4 IT/AIM related staff as per the Project AIM Final Update June 2019.

³⁰ In March 2019 the IT department went through a transformation decreasing headcount from 34 to 28 staff

As a consequence of the issues highlighted, the effective delivery of the first major GOS launch, post-Project AIM, is at risk.

The lack of a clear governance and oversight mechanism, as well as human resource limitations for the GOS platform, have resulted in significant issues related to the delivery of Launch 1. This launch is expected to provide key functionalities related to grant documents such as the performance framework and the grant budget, which are critical to the grant life cycle and need to be adequately built into GOS, especially with a new grant cycle about to begin. These remain incomplete and in the absence of a broader governance function to align different stakeholders, there is inconsistent awareness in the Secretariat of the criticality of these functionalities and limited knowledge on how they can be effectively delivered. These issues increase the risk to Global Fund operations, as this launch relates to funding requests and allocations and has a significant impact on the entire grant management lifecycle.

Launch 1 was initially envisioned to be completed by July 2019, but under the vendor contract this launch was moved to September 2019. Despite this extension, at the time of the OIG audit, the launch was not ready and had been delayed by over three months. This had a significant impact on the roll out strategy of the Launch 1 module. The initial plan was for there to be a soft launch rather than vendor-supported Hypercare. Hypercare normally occurs straight after the module has been developed and then gone live for general use. However, this was not planned to occur as there was an intentional gap between the launch being completed and the module being used by the organization.

Subsequent to the audit, Launch 1 was completed with key changes to the launch plan, including a much shorter soft launch than expected, although the Secretariat stated that Hypercare did take place. This raises the likelihood of risks around future user experience issues and incident management challenges. This was a concern at the time of the audit, given the large number of issues raised in Launch 1 system integration testing (SIT),³¹ of system errors at deployment, if not effectively resolved between the phases of SIT-UAT and UAT-Go Live. Launch 1 system development and testing and Go Live had not been completed at the time of the audit fieldwork, thus OIG could not provide assurance on the Systems Development Life Cycle for this enhancement of GOS.

As GOS Launch 1 is part of a wider roadmap of eight cascading launches, any impact on one launch diverts resources from the following planned launches and increases the risk of knock-on delays. This is particularly critical in a grant-making year, as the absence of key grant documentation within the system can have downstream impacts on the effectiveness of other modules.

Agreed Management Action 3

The Secretariat will revisit and adjust the governance requirements, based on the scope and resource requirements of each future launch-related release.

Owner: Head of Grant Management Division

Due date: 31 December 2020

³¹ SIT report for Launch 1 – 27 September 2019.

4.4. Gaps in IT controls and processes to safeguard GOS as a core system

User access and disaster recovery are two key elements to safeguard GOS as a core system, used by the Global Fund for the management of grants throughout their lifecycle. In a positive move, the Global Fund is in the process of obtaining ISO 27001 certification, the information security standard for IT covering all legal, physical and technical controls involved in an organization's information risk management processes. Once obtained, recertification is needed every three years.

OIG's IT audit in 2015 identified serious weaknesses and security gaps. However, basic IT controls have since improved, as acknowledged in the 2017 Cloud computing audit and in addition, there have been several initiatives to strengthen IT controls around access and disaster recovery management. Nevertheless, as noted below some key issues remain outstanding.

Incomplete reviews over GOS user access

User access control is the process through which users are granted access and certain privileges to systems, resources or information. GOS user access is controlled by the allocation of each user to predefined user groups. One group is role-based (e.g. Fund Portfolio Manager) and manages user rights, while another group is level-based (e.g. Country, Region) and controls user access to different parts of the system. Issues identified by the external auditor relating to GOS super-users' access have been addressed by the Secretariat, and additional testing by the external auditor has not identified other significant issues.

As of October 2019, there were over 2,300 Salesforce users³², only 36% of whom had logged in during the previous three months.

At the time of the audit, the policy for GOS User Management was in draft, despite the system having been in production for more than two years. The roles and responsibilities for GOS user review are allocated informally to Secretariat departments. In the absence of a GOS User Management policy, the frequency of user review is not established. In 2019, a single and incomplete user review was performed, which included only Country Team staff, one subset of internal users. The user review process is largely manual, relying on staff-driven checks and on confirmations requested and sent via e-mail. Due to system limitations, the audit trail for access granted to users is available only for the last three months.

These gaps highlight insufficient prioritization of user access management. Despite user access issues being raised by the External Auditor in 2017 and 2018 appendices to the Management Letters, the Secretariat has not finalized the user access policy, operationalized its implementation or tracked its progress. This can lead to delayed termination of GOS users, risking unauthorized access to critical programmatic and financial data by current or former staff. It may also affect the ability of the External Auditor to provide assurance on GOS user access for the audit period. Periodically analyzing GOS usage and user review may also generate savings on license costs.

System backup and disaster recovery policies need to be formalized

Disaster recovery represents a set of policies, tools and procedures which protect an organization, allowing it to recover, or to continue using its systems, following a natural or human-induced disaster. Backup is the process of making copies of data, to use in the event the original data or data files are lost or destroyed. Penetration testing is a method of testing, measuring and enhancing established security measures on information systems and support areas.

For the Global Fund, principal reliance for backup is put on Salesforce itself, with additional processes undertaken by the Global Fund IT function. A new tool for back-up came into use in August 2019, and GOS backups happen daily, however there are no updated user manuals for this process.

³² Two thirds are external users (Partners, Local Fund Agent portal users), the remaining third are internal users split between Country Team staff (managing grants) and other Global Fund staff (accessing and using the information available).

At the time of the audit, disaster recovery and backup policies for GOS were not finalized, with limited clarity around actions to be taken in case of a disaster recovery scenario.

In addition, there is no formal agreement across the Secretariat on the recovery point objective/time objective,³³ key elements of any disaster recovery plan. Responsibilities to monitor and follow up on agreements related to recovery point/time objective have not been allocated, and the frequency for recovery testing, data seeding with the new tool and penetration testing, not defined. Penetration testing on the Salesforce platform (GOS) has only been performed twice since 2016.

These issues jeopardize the organization's ability to manage a disaster, due to its limited scenario planning. They also raise the risk of significant impact on organizational grant management processes if the recovery point objective/time objective is not established.

Agreed Management Action 4

The Secretariat will complete a user access policy and procedures and ensure that user access recertification controls are implemented on a yearly basis.

Owner: Chief Information Officer

Due date: 31 December 2020

Agreed Management Action 5

The Secretariat will complete policy and guidelines for GOS disaster recovery and backup activities.

Owner: Chief Information Officer

Due date: 31 March 2021

³³ The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs. (<https://whatis.techtarget.com/definition/recovery-time-objective-RTO>).

5. Table of Agreed Actions

Draft Agreed Management Action	Target date	Owner
1. The Secretariat will: <ul style="list-style-type: none"> • Ensure that a SDLC testing methodology is adopted, in line with ISO standards in order that testing for future releases meets required standards and criteria. • Ensure a stronger quality sign-off process is put in place to confirm that bugs in the Project Tracker are updated and all critical and high bugs are resolved prior to go-live for future releases. 	30 June 2021	Chief Information Officer
2. The Secretariat will: <ul style="list-style-type: none"> • Implement policy and guidance on internal incident management protocols, including targets for resolution; • Ensure that incident monitoring capabilities are implemented to; track incident management key performance indicators and the quality of issue resolution. 	31 December 2020	Chief Information Officer
3. The Secretariat will revisit and adjust the governance requirements, based on the scope and resource requirements of each future launch-related release.	31 December 2020	Head of Grant Management Division
4. The Secretariat will complete a user access policy and procedures and ensure that user access recertification controls are implemented on a yearly basis.	31 December 2020	Chief Information Officer
5. The Secretariat will complete policy and guidelines for GOS disaster recovery and backup activities.	31 March 2021	Chief Information Officer

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 focus on issues related to the impact of Global Fund investments, procurement and supply chain management, change management, and key financial and fiduciary controls.