Audit Report

Audit of the Global Fund's Secretariat Information Technology General Controls

GF-OIG-25-016
22 December 2025
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, enhances risk management, and reports fully and transparently on abuse.

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.

Email:
hotline@theglobalfund.org



Table of Contents

1. Executive Summary 3
1.1 Opinion 3
1.2 Key Achievements and Good Practices 4
1.3 Key Issues and Risks 5
1.4 Objectives, Ratings and Scope 6

2. Background and Context 7
2.1 Overview of IT General Controls at the Global Fund 7
2.2 Overview of key Global Fund IT systems covered by the General Controls 7
2.3 Assurance review over IT General Controls 8

3. Findings 9
3.1 IT general controls are robust and well implemented across key domains such as network security, IT operations, and change management 9
3.2 While data security controls are well designed, inconsistent implementation of data classification increases risk of data privacy and confidentiality breach 11
3.3 Access management controls are well managed throughout the user account lifecycle, except during consultant offboarding 13

Annex A. Audit Rating Classification and Methodology 16

1. Executive Summary

1.1 Opinion

Information Technology General Controls (ITGCs) are foundational policies, procedures, and activities that ensure the integrity, confidentiality, and availability of IT systems and data. Since the launch of phase 2 of the IT transformation in 2019, IT solutions and systems have continuously been enhanced to better align with core business priorities and requirements. Robust ITGCs are essential to mitigate key IT-related risks including IT service disruption, data loss or corruption, cybersecurity threats, and unauthorized access to confidential information. This OIG audit complements existing external assurance reviews sponsored by the Chief Information Officer. These include the work performed by the Global Fund's external auditor and regular ISO certification reviews.[1]

The Global Fund Secretariat has established comprehensive procedures, processes, and tools that address key areas of ITGCs throughout the IT service lifecycle. These areas include access management, change management, data security, network security, and IT operations. Dedicated teams within the IT Department are responsible for overseeing, coordinating and managing these controls. In response to the rapidly evolving IT landscape and emerging threats, the IT team continually enhances the design of ITGCs. This work is informed by insight from regular internal and external assurance reviews, as well as ongoing risk assessments. The design of ITGCs is assessed as **effective** to mitigate key information technology risks.

ITGCs are effectively implemented and monitored across most areas. IT operations include regular data backups to support rapid recovery. A robust IT vendor management is in place mitigating risks associated with outsourcing key IT systems and core IT activities to third parties. The timely resolution of IT incidents contributes to the continuous availability of IT services. In addition, key controls are in place to manage risks related to system changes, helping to maintain the availability and resilience of IT systems. The IT Department also enforces multiple controls and safeguards to ensure secure and reliable network traffic, while protecting against cybersecurity threats.

Robust data security controls and procedures are in place for various IT systems. For user access management, the system correctly removes access upon the contract end date recorded in Workday. Therefore, ITGCs' design and operational effectiveness to preserve confidentiality, integrity and availability of data and systems is **effective**.

However, their effectiveness in achieving the overall control objective is compromised by dependencies on manual business processes. Delayed notification of consultants' departure by hiring departments to Human Resources causes consultant[2] accounts to remain active after the consultants have left the organization, increasing the risk of unauthorized access to data and systems. The issue was raised by external assurance providers in previous years. Similarly, document access restrictions rely on users applying the correct security labels. Our review identified several confidential documents widely accessible on the intranet because users failed to apply the

[1] ISO standards are globally recognized standards in specific domains. The Global Fund has successfully renewed its ISO certification in three IT domains in 2025: ISO 27001 (Information Security Management System), ISO 22301 (Business Continuity Management System), and ISO 20000 (IT Service Management System)

[2] Consultants are individual consultants from temporary agency service providers, payroll service providers and/or independent consultants who work with the Global Fund. They can also be members of service providers contracted by the Global Fund to deliver specific work. Depending on the nature of their work, the Hiring Department can decide to allocate them an internal user account to facilitate their access to Global Fund resources. At end of contracting period or in case of replacement, their assigned user accounts must be deactivated.

required labels. Consequently, the Supporting Business Processes are only **Partially Effective** to preserve confidentiality, integrity and availability of data and systems.

1.2 Key Achievements and Good Practices

Access management controls generally function well across the user account lifecycle

The Global Secretariat has implemented access management controls to safeguard data and systems from unauthorized access through user accounts. Controls to create new user accounts and assign access rights are well designed and effective. Multi-factor authentication (MFA)[3] is consistently enforced for all internal user accounts, to reduce risk exposure to unauthorized access. User access rights, including those for privileged accounts,[4] are subject to periodic reviews by system owners to ensure proper segregation of duties and alignment with users' roles and responsibilities. Accounts of former Global Fund employees are promptly deactivated upon their departure.

Data security controls are robust across key IT systems used at the Secretariat

The Global Fund IT Department has implemented several controls to safeguard data integrity and confidentiality, including strong authentication methods to prevent unauthorized access to user accounts. Recognizing the varying sensitivity of data, the IT team has established procedures to classify information into four risk-based categories. Automated labelling is applied to Microsoft Office documents and Outlook emails to regulate data sharing.

Business applications enforce data access restrictions based on user access roles and permissions. In addition, the IT team implements an encryption method aligned with industry best practices to ensure that data transmitted over networks and stored in databases remains unreadable to unauthorized individuals or systems, safeguarding data confidentiality and integrity.

Robust controls and measures to strengthen network security against cybersecurity threats

The Global Fund has implemented robust controls to safeguard its assets from external threats, particularly cybersecurity attacks. These controls are consistently applied across key entry points, including network devices, servers, endpoint devices, and user interfaces. Key measures include properly configured routers and firewalls, effective network segmentation, regular user training to raise cybersecurity awareness, installing/updating antivirus software and patches on endpoint devices (e.g. laptops and mobile phones) and continuous monitoring and management of system and network vulnerabilities.

Adequate controls are consistently applied to ensure secure changes in IT systems

Ineffective change management can introduce vulnerabilities and operational issues. Adequate controls are consistently applied to ensure that changes to IT systems are secure, and do not compromise data integrity or system availability.

IT operations are well managed to ensure the availability of IT services

The IT team has developed and enforced adequate procedures to ensure IT operations controls are effective to ensure the continuous availability of IT systems and data. These include regular data

[3] Multi-Factor Authentication (MFA) requires users to set strong passwords (e.g. complexity, expiration) and use an additional authentication factor such as a verification code sent via text message or voice call, or the Microsoft Authenticator application
[4] A privileged account is a user or system account that has elevated access rights and permissions beyond those of a standard user account, allowing it to perform sensitive administrative functions (e.g. managing other users access rights)

backups, centralization and timely resolution of IT incidents, as well as structured processes for contracting, monitoring, and offboarding IT vendors.

The Global Fund IT system benefits from several independent assessments which contribute to its continuous strengthening

The Global Fund undergoes three ISO certifications review every three years: ISO 27001 (Information Security Management System - ISMS), ISO 20000 (IT Service Management System - ITMS) and ISO 22301 (Business Continuity Management). These reviews are conducted by an independent certification body and provide assurance over the design and operating effectiveness of the ITGC components outlined above. The Global Fund external auditor conducts a review of ITGC on an annual basis, focusing on change management, IT operations, and access management controls. All these reviews foster a learning environment by identifying issues early, to fix them and enhance existing controls.

Key Global Fund IT cloud service providers' (SOC)[5] Type 2 reports (including those supporting network security and maintenance, Grant Operating System, payment application, and direct procurement system*)* are reviewed on an annual basis. This additional assurance suggests that Global Fund contracts with service providers which maintain robust controls to ensure service availability and safeguard the integrity and confidentiality of client data including those of the Global Fund.

1.3 Key Issues and Risks

Inconsistent data classification on SharePoint[6] allows unauthorized access to personal and confidential data

A significant volume of information stored in SharePoint folders is not adequately protected. Currently, any employee or consultant with an internal Global Fund account can access documents that should be restricted, including personally identifiable information, contact details of external stakeholders, staff health data, and confidential communications.

Non-compliance by users to adhere to data classification protocols and available technical controls, limited automated access controls (especially for PDF files), inconsistent data restriction practices across departments, and the absence of compliance monitoring drives the issue. In response, the IT Department conducted training on data classification to strengthen data protection. In coordination with other Departments / Divisions, IT Department is taking action to regulate SharePoint access.

Failure by departments to notify HR of consultant departures resulted in prolonged system access beyond contract end dates

IT security standards such as ISO 27001 require the immediate deactivation of user accounts upon the departure of an employee or consultant, to prevent unauthorized access and reduce the risk of dormant account exploitation. The OIG found that 23% of consultant accounts that ended between January and June 2025 were deactivated with delays between 14 and 68 days. Eight consultants accessed their accounts after their official departure dates.

This recurring issue, previously highlighted by the Global Fund's external auditor, stems from insufficient coordination between hiring managers and the Human Resources Department. While no

[5] A Systems and Organization Controls (SOC) Type 2 report is an independent audit that examines how a service organization's internal controls function over a defined period according to the Trust Services Criteria (security, availability, processing integrity, confidentiality, and privacy)
[6] Microsoft SharePoint is a web-based platform that enables Global Fund staff to create, store, organize, share and manage information and documents

security breaches have been reported to date, timely deactivation is critical in safeguarding systems and data.

1.4 Objectives, Ratings and Scope

The overall objective of the audit is to provide the Global Fund Board with reasonable assurance over the design and effectiveness of the ITGCs in place to ensure the confidentiality, integrity, and availability of key Global Fund systems and information. Specifically, the audit assessed:

<table>
<tr><th>Objectives</th><th colspan="2">Rating</th><th>Scope</th></tr>
<tr><td>The adequacy of the design of ITGCs to address key information technology risks</td><td colspan="2">Effective</td><td rowspan="3">Audit period
January 2024 to June 2025

Scope exclusion
IT Office systems (including Outlook, MS Office, Teams) are not within the direct scope of the audit. However, our review of user access management indirectly covered these applications due to their reliance on a common authentication mechanism used across most Global Fund applications and systems, including those selected for testing</td></tr>
<tr><td rowspan="2">The operational effectiveness of ITGCs to preserve confidentiality, integrity and availability of data and systems</td><td>ITGC Design and Operational Effectiveness</td><td>Effective</td></tr>
<tr><td>Supporting Business Processes</td><td>Partially Effective</td></tr>
</table>

The OIG interviewed relevant stakeholders, including IT, HR, and system owners, and conducted walkthroughs of control processes. We reviewed policies, procedures, governance mechanisms, and related documentation, and tested key activities to assess the design and implementation of controls. The OIG placed reliance on other assurance providers' review (including Global Fund external audit and ISO certification) in line with the Global Internal Audit Standards (Standard 9.5 Coordination and Reliance).

Details about the general audit rating classification can be found in **Annex A** of this report.

2. Background and Context

2.1 Overview of IT General Controls at the Global Fund

The Global Fund Secretariat operates in a highly automated information technology (IT) environment. To safeguard IT systems and data, the IT Department has designed and implemented several preventive and detective controls, commonly referred to as Information Technology General Controls (ITGCs). These controls are designed to ensure the confidentiality, integrity, and availability of IT systems and data.

Global Fund ITGCs are categorized into five main areas:[7]

- **Access management controls** - ensuring that only authorized users can access specific systems and data, helping to prevent unauthorized access and data breaches.
- **IT operations** - focus on maintaining the reliability, performance and security of IT systems through routine monitoring, maintenance, and incident management.
- **Change management** - ensuring that changes to systems and applications are properly controlled, authorized, tested, and documented before being rolled out, minimizing the risk of disruptions or vulnerabilities.
- **Data security controls** - protecting information throughout its lifecycle, from creation and storage to transmission and disposal.
- **Network security controls** - defending the organization's infrastructure against cyber threats.

2.2 Overview of key Global Fund IT systems covered by the ITGCs

The Global Fund's IT environment comprises IT infrastructure, applications, platforms, and endpoint devices such as laptops and mobile phones. Together, these elements support day-to-day operations and enable the effective delivery of the organization's core functions.

Most IT systems at the Global Fund are cloud-based[8], and related risks are managed through structured vendor oversight and robust IT service management processes. Applications[9] within the IT ecosystem are grouped into three primary categories, based on their purpose and functionality:

Business application	Office application	IT Management Application
• GOS (Grant) • Kyriba (Payments) • Oracle Fusion (Finance) • Wambo (procurement) • Workday (HR) • Tableau (Data reporting) • TeamMate + (OIG) • TMS (Admin travel) • CMS/CSS (Case Mgt)	• Adobe Sign • Microsoft Teams • Office 365 - Exchange Online – GF • Office 365 - SharePoint Sites – GF • Outlook • SharePoint • MS Office Suite (Word, Excel, PowerPoint) • www.theglobalfund.org	• Active Directory • ADFS (SSO) • Azure Subscription • CyberArk Endpoint Privilege Manager • EnCase • MIM (Microsoft Identity Manager) • ProofPoint • ServiceNow

[7] While a key component of ITGC, Software Development lifecycle Controls (SDLC) are not listed because the Global Fund does not develop its own software in most instances but rather leverages systems, platforms and applications provided through cloud services.
[8] A cloud-based IT system is an integrated set of hardware, software, and networking resources hosted on remote servers and delivered over the internet to provide computing, storage, and application services without relying on on-premises infrastructure.
[9] The figure does not include the full list of Global Fund systems and applications.

2.3 Assurance review over ITGCs

In recent months, the Global Fund Secretariat has undergone several independent reviews aimed at assessing the design and effectiveness of its IT General Controls (ITGCs). These reviews play a critical role in strengthening the organization's internal control framework and ensuring the reliability of its IT environment. Key reviews include:

- **ISO certifications**: The Global Fund holds three ISO certifications, valid until 2028:
    - ISO 27001 - Information Security Management System
    - ISO 22301 - Business Continuity Management System
    - ISO 20000 - IT Service Management System

  These certifications provide assurance over the adequacy and effectiveness of controls and activities related to these three domains. A surveillance review is carried out by an independent certification body every year, while a full re-certification process is undergone every three years.

- **External auditor's ITGC review**: As part of the annual financial statement audit, the external auditor KPMG reviews the ITGCs supporting key financial applications and infrastructure. The 2024 report concluded that the relevant IT controls were adequately designed and operated effectively with few exceptions. The review covered areas such as user access management, change control, and IT operations.

- **SWIFT[10] Customer Security Programme (CSP):** The Global Fund undergoes annual assessments under the SWIFT CSP framework, which ensures that institutions using the SWIFT network comply with a baseline of mandatory cybersecurity controls. The assessment focuses on areas such as secure authentication, access restrictions, incident detection, and system integrity related to SWIFT-connected environments.

Each of the above reviews has its own distinct objective, scope, priorities and review approach, depending on the level of assurance they intend to provide. The OIG's audit complemented these existing assurance activities by focusing on ITGC domains where additional testing could be considered. A risk-based approach was applied to ensure comprehensive coverage while avoiding duplication of efforts.

[10] SWIFT is a secure messaging network that financial institutions use to send and receive information about financial transactions, such as international money transfers. The Global Fund uses a SWIFT-certified software (KYRIBA) for payments.

3. Findings

3.1 IT general controls are robust and well implemented across key domains such as network security, IT operations, and change management

The Global Fund Secretariat has established and effectively implemented IT operational controls and secure change management processes to ensure the continuous availability of IT services. Robust network security controls are in place to protect against cybersecurity threats.

Network security controls are robust, but room for improvement on security awareness training

The most recent ISO 27001 audit (March 2025) found that controls and monitoring tools are adequate to mitigate and manage point-of-entry risks that external attackers seek to exploit. These include adequate configuration of network devices (such as firewalls and routers), proper network segmentation, appropriate patch management process, vulnerability monitoring and remediation mechanisms, as well as regular security awareness training for users.

During the audit, the OIG verified that all endpoint devices had up-to-date antivirus signatures to protect against increasingly sophisticated cybersecurity attacks. The OIG also noted that security patches,[11] particularly for Microsoft Windows, were regularly applied to endpoint devices to maintain system integrity.

While both the OIG audit and ISO 27001 review acknowledge that the IT team provides regular security awareness training, there is room to enhance that process. There is a lack of consistent sharing of key IT policies with new joiners. Although the IT team has produced a presentation outlining IT policies and regulations, the Human Resources Department, responsible for onboarding of new joiners, has not included it in the onboarding package. Additionally, while new staff members are required to complete existing mandatory training courses upon joining, new consultants with Global Fund accounts are not systematically enrolled in these sessions as part of their onboarding. This contributes to limited awareness of cybersecurity risks among these groups. Since the next round of mandatory training may occur several months after onboarding, this delay creates a prolonged period of vulnerability.

Despite robust network security controls, external attackers may still succeed in breaching an organization's network. To mitigate this risk, the IT team has developed and enforced a comprehensive incident management protocol. This protocol has demonstrated its effectiveness by significantly reducing the impact of phishing attacks.

Change management[12] controls are well designed and effectively implemented

Reviews conducted under ISO 27001 (Information Security Management System) and ISO 20000 (IT Service Management System) in March 2025, and the external audit in 2024, found that the Global Fund's change management processes and procedures for key systems are adequate and

[11] A patch is a software update designed to fix a problem or improve a program
[12] A Change is the addition, modification or removal of anything that could have an effect on IT services. Change management is the process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services

effective. Specifically, there are controls in place to mitigate key risks throughout the change management lifecycle, from the initiation of change requests to post-implementation reviews.

IT operations controls are well designed and effectively implemented to ensure continuous availability of systems and data

IT operations controls encompass daily activities that help maintain IT system reliability, ensure data integrity, and support a rapid recovery from disruptions, all while minimizing risks of service interruptions. The IT team has developed specific procedures to address each category of operational activity. These activities are monitored monthly through reports and meetings involving IT senior management (including the Chief Information Officer and relevant senior managers), as well as relevant business owners.

The ISO 27001 (ISMS) and 20000 (ITMS) re-certification reviews have confirmed the adequacy and effective implementation of the incident management procedure. Most incidents are resolved within defined timeframes, contributing to a high availability rate (at least 99%) for the Global Fund's IT systems.

The organization employs real-time backup mechanisms for Microsoft Azure and Global Fund-owned applications. In addition, an immutable backup[13] system is in place to mitigate risks associated with data loss and ransomware[14] attacks. The ISO 22301 (Business Continuity Management System - BCMS) certification, conducted in March 2025, provides strong assurance over the effectiveness of these backup and recovery practices.

The Global Fund's IT environment relies heavily on third-party service providers, as key IT systems are cloud-based and certain key IT activities are outsourced. This reliance on external service providers introduces inherent risks, as vendor failures could significantly disrupt IT services. To mitigate these risks, the IT Department has established a dedicated IT vendor management function, supported by comprehensive operating procedures and tools. The OIG audit found that the vendor management process is well designed, with the use of innovative tools (e.g. portal for vendor management), and effectively managed throughout the vendor lifecycle. In assessing vendor risks, the IT Department also leverages the Systems and Organization Controls (SOC 2) audit reports which provide independent assurance on the design and operating effectiveness of controls that IT vendors maintain when delivering services to clients.

The design of ITGCs is adequate to mitigate key information technology risk. Therefore, no management action is required.

[13] An immutable backup is a special kind of backup that cannot be changed, deleted, or tampered with once created, for a set period
[14] A ransomware attack is a type of cyberattack where malicious software infects a computer or network and locks or encrypts the victim's files and data, making them inaccessible until a ransom is paid

3.2 While data security controls are well designed, inconsistent application of data classification requirements increases the risk of data privacy and confidentiality breaches

Although the Global Fund's data security controls are adequately designed, the OIG identified implementation gaps in the application of protocols on SharePoint sites that allowed unauthorized access to confidential and private information.

Data is one of the most valuable assets within any IT system and must be safeguarded against unauthorized access to preserve its confidentiality and integrity. To achieve this objective, the Global Fund Secretariat has designed and implemented a range of data security controls across its IT environment.

Controls are effectively designed to reduce the risk of compromising data confidentiality and integrity

Data protection begins with preventing unauthorized access to user accounts. To mitigate this risk, the IT Department has implemented a range of controls, including robust authentication mechanisms and comprehensive user account access management and monitoring, as detailed in section 3.3. In addition, network security controls have been enhanced to safeguard endpoint devices (such as laptops and mobile phones) from unauthorized external access. These measures help protect both the devices and the data they contain (see section 3.1).

Certain types of organizational data are particularly sensitive; unauthorized disclosure of personal, financial, or human resources data can pose significant operational, legal and reputational risks. To mitigate these risks, the IT team under the oversight and guidance of the Data Governance Council (DGC) has established data classification rules that categorize information into four risk-based groups: Public (low or no risk), Restricted (moderate risk), Confidential (high risk), and Highly Confidential (Very high risk). Automated classification has been implemented for Microsoft Office documents and Outlook emails, with confidential documents requiring appropriate labelling to control access and sharing. The IT team has introduced mandatory data protection training, emphasizing data classification, to raise staff awareness of these controls.

An additional layer of data protection comes through ensuring that data at rest (e.g. data stored in database) and data in motion (e.g. transmitted via emails or between devices) can only be accessed by authorized individuals. This is achieved through encrypting data, a process that renders data unreadable to unauthorized individuals or systems, to safeguard its confidentiality and integrity. The ISO 27001 certification audit confirmed that the IT Department has defined adequate procedures for managing the encryption process and enforces encryption methods aligned with industry best practices.

Inconsistent application of data classification on SharePoint has allowed access to personal and confidential data

While data classification and restriction rules are effectively enforced across Global Fund IT applications / platforms (e.g. Workday, GOS, GFS), similar controls have not been consistently applied to information stored in SharePoint folders. Because of the nature of document sharing platforms, it is incumbent on staff to apply an appropriate classification on their documents. However, the OIG found that sensitive documents could be accessed by Global Fund employees and consultants with internal user accounts. These include the following categories of documents that should have been restricted to preserve privacy and confidentiality:

- **Personally identifiable information of staff,** such as home addresses, nationality, marital status, and passport details, often found in uploaded passports and visa application forms.
- **Contact details,** including for senior external officials.
- **Personal, sensitive information,** such as health information of employees and consultants.
- **Confidential communications,** including Global Fund memoranda, and letters from in-country officials to senior management.

The following factors contributed to the unauthorized access to sensitive information stored on SharePoint:

- Limited features for applying data classification protocols: While data classification features are enabled for Microsoft Office documents and Outlook messages, they do not extend to PDF files, the format most used for sensitive documents on SharePoint.
- Inconsistent data restriction practices: Some departments or user groups have proactively created restricted folders for confidential data, while others have not. Recent mandatory data protection training aims to address this inconsistency but relies on individual staff following the procedures outlined in the training.
- Lack of compliance monitoring by user groups: Despite efforts to raise awareness through mandatory training, there is currently no mechanism in place to monitor compliance with data classification and access control policies.

The IT team has started engaging with several teams of the Global Fund's Secretariat to restrict and clean up sensitive and personal files, but some of the above-mentioned documents could still be accessed on SharePoint at the time of writing this report. Although the Global Fund is not subject to specific data privacy regulations due to its privileges and immunities, internal IT policies such as the Technology User Acceptance Regulation and Employee Handbook emphasize the importance of safeguarding data privacy and confidentiality. Failure to adequately protect personal data could expose the organization to reputational and legal risks, particularly if such information is misused.

Agreed Management Action 1

The Secretariat will take the following actions to address the different points identified by the OIG Audit:

1. Awareness and Training. A specific course on "Data and information protection" will be created and inserted in iLearn (in collaboration with HR). The course will be mandatory for all employees and consultants and repeated regularly. Contents will be updated as necessary.
2. The Chief Information Officer and Chief Ethics and Risk Officer will develop a plan to implement appropriate compliance monitoring to further mitigate this risk, including relevant consequences for non-compliance.
3. The Chief Information Officer in coordination with Divisions / Departments of the Global Fund Secretariat will launch a clean-up campaign on GF intranet "Engage" to restrict access to accessible personal data identified during the audit.

OWNER: Chief Information Officer and Chief Ethics and Risk Officer

DUE DATE: March 2026

3.3 Access management controls are well managed throughout user account lifecycles, except during consultant offboarding

Overall, access management controls at the Global Fund Secretariat are well designed and effectively implemented throughout the user account lifecycle. However, delays in deactivating consultant accounts after their departure increase the risk of unauthorized access to Global Fund systems and data. Additionally, there is an opportunity to strengthen authentication methods for external users accessing Global Fund systems.

Access management controls are essential for ensuring that system and data access is restricted to authorized users. Given their criticality, access controls are systematically included in the scope of reviews conducted by Global Fund IT assurance providers, including ISO 27001 certification review and external audits.

Adequate procedures are in place to effectively manage access controls from creation to termination of user accounts

The IT team has established robust processes and procedures to effectively manage the onboarding of new employees and consultants. Access rights are granted based on user needs, following the principle of least privilege.[15]

The IT team has implemented a robust authentication method to verify user identity before granting access. This process includes Multi-Factor Authentication (MFA), which requires users to set strong passwords aligned with best practices (e.g. complexity, expiration) and use an additional authentication factor.

To address risks associated with access rights, business owners such as the Procurement and Finance teams conduct an annual certification process to review and validate user access rights for their respective business applications (e.g. Wambo, GFS). The external auditor, KPMG, confirmed that this detective control is executed as designed with few exceptions.

The final phase of the user account lifecycle involves the deactivation or removal of accounts from the Human Resources system (Workday) and Microsoft Identity Manager (MIM) following the departure of employees or consultants. The OIG noted that user accounts of former Global Fund employees are deactivated in a timely manner.

Recurring delayed termination of internal user accounts in key IT systems increase the risk of unauthorized access to Global Fund data and systems

Despite the good practices above, some consultants retained active user accounts beyond their engagement period, thereby increasing residual access risks. IT security standards such as ISO27001[16] require the immediate deactivation of user accounts when employees or consultants leave the organization. This control is essential to prevent unauthorized access, not only by former personnel but also by external attackers who could exploit dormant accounts[17] to compromise system security.

The OIG observed that 50 out of 217 consultants' accounts (23%) whose contracts ended between January to June 2025 were deactivated with delays (ranging from 14 to 68 days) after their contract ended. Further analysis revealed that eight of these consultants accessed their accounts after their

[15] The principle of least privilege (PoLP) is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task
[16] Control AC-2: Account Management (NIST 800 – 53) and Annex A.5.18 Access Rights (ISO/IEC 27001)
[17] Dormant accounts refer to active accounts which have not been used for an extended period

official departure. This issue has previously been raised by the external auditor KPMG, highlighting a recurring control weakness in the offboarding process for consultants.

This issue is driven by an insufficient coordination between hiring departments and Human Resources regarding the notification of contract termination. The issue is particularly prevalent among consultants who leave the organization before the official end date of their purchase orders, either due to early termination or replacement by other consultants from the same company.

Although no incidents of unauthorized access resulting from delayed account deactivation have materialized at the Global Fund, similar control weaknesses have led to significant breaches affecting data integrity and system availability in other sectors.

There is an opportunity to strengthen the authentication method for external user accounts to reduce the risk of account compromise

During the review of external user accounts, the OIG noted that their passwords are not configured to expire, which is inconsistent with password security best practices.

Furthermore, the OIG acknowledges that, in line with the Management Executive Committee (MEC) approval of MFA activation for high-risk external users in 2022, not all external users are required to authenticate their access to the Global Fund's IT systems using multiple factors

In the Global Fund context, the potential impact of a compromised external user account, such as in the Grant Operating System (GOS), is generally lower than that of internal users, due to the limited scope of access to overall system data granted to external stakeholders.

Agreed Management Action 2
A specific educational material (called "journey") on "Staff & Consultant deactivation Process" will be created and inserted in Workday (Human Resources Information System). It will be mandatory and targeted to the managers who need it. It will be delivered as follows: 1. initial training; 2. each time a new consultant is onboarded; 3. annual refresh.
OWNER: Chief Human Resources Officer
DUE DATE: March 2026

Annex A. Audit Rating Classification and Methodology

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.

The OIG audits in accordance with the Global Institute of Internal Auditors' definition of internal auditing, international standards for the professional practice of internal auditing 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 safeguard the independence of the OIG's auditors and the integrity of its work.

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 is used to provide specific assessments of these different areas. 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.