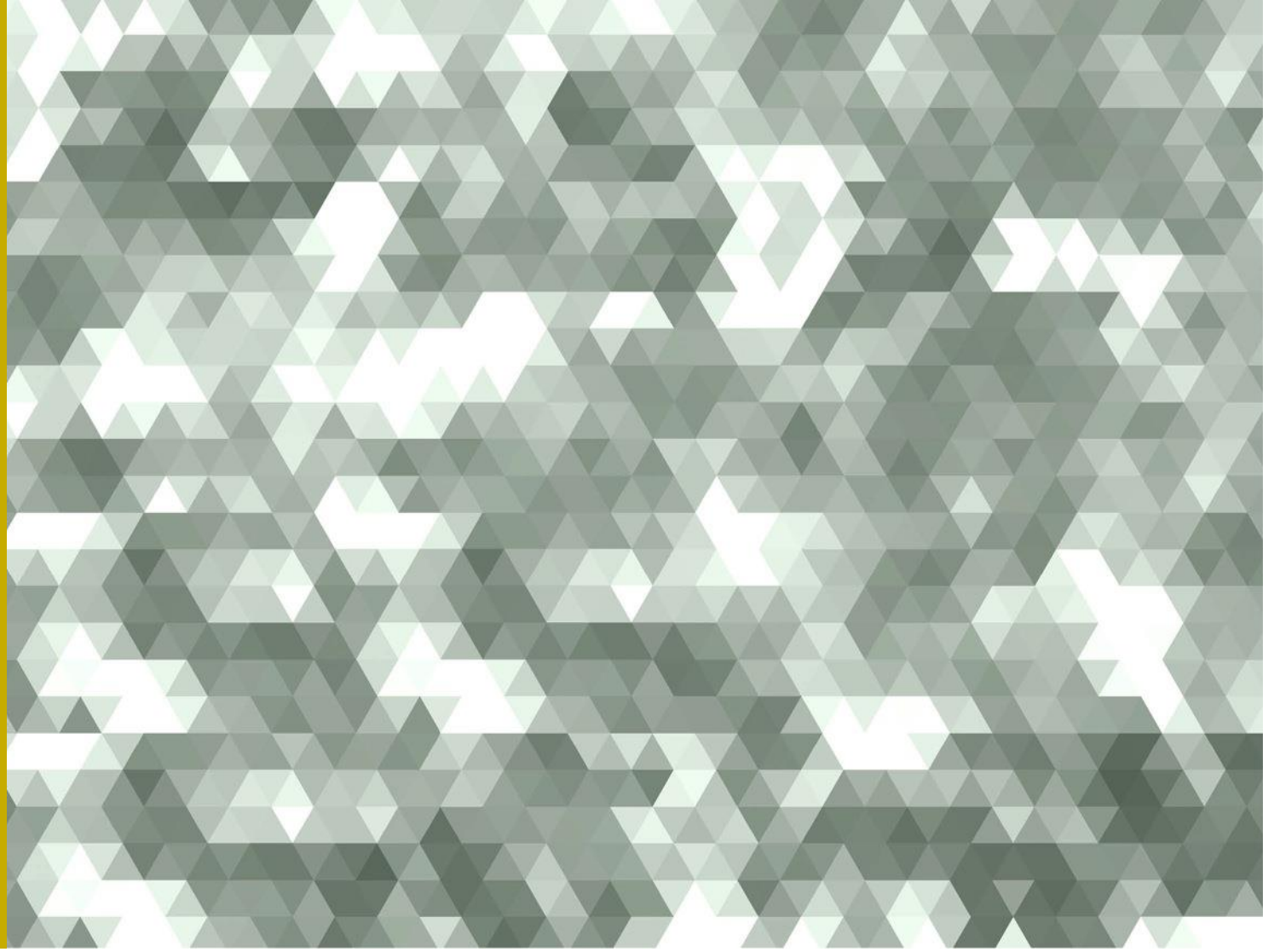


Audit Report

Global Fund Risk Management Processes

GF-OIG-17-010
16 May 2017
Geneva, Switzerland

The Global Fund
Office of the Inspector General

Table of Contents

I. Executive Summary

The Global Fund operates in over 100 countries which include some of the world's most challenging environments. The need for strong risk management at all levels is critical. The challenges faced by the Global Fund in achieving impact have been highlighted in several institution-wide reports since 2009.

This Office of the Inspector General (OIG) audit assessed the adequacy of design and operating effectiveness of risk management processes. It focused on three main aspects: (1) governance and oversight at the Board and senior management levels; (2) effectiveness of the Secretariat's risk management processes; and (3) the risk environment and culture.

Governance, oversight and accountability for risk management at Board and senior management level:

Risk management governance, oversight and accountability at the Global Fund have improved considerably over the past decade, in particular since 2012, following a five-year evaluation[1] in 2009 and recommendations from a High Level Review Panel in 2011.[2] The Board has approved a Risk Management Policy[3], which included the definition of its responsibilities for risk oversight, as well as a risk differentiation framework. The Board committees' roles and responsibilities have been clarified. A Risk Department, led by a Chief Risk Officer (CRO), was established in 2012. The team's headcount has recently been increased from four to 16 and its role in operational decision-making has been strengthened. Operational and Enterprise Risk Committees were established in 2012 and 2016, respectively. Risk is now a standing item on the Board and committee agenda and an Organizational Risk Register is reviewed quarterly by the Management Executive Committee and by the leadership of the Board and committees.

While recognizing these improvements, the OIG identified limits to the effectiveness of the governance and oversight. Risk oversight is one of the Board's six core functions. The Board is ultimately responsible for establishing and overseeing the organization's risk management strategy and its tolerances for risk.[4] Although challenging in the context of the Global Fund, risk thresholds and appetite remain undefined. The articulation of risk appetites enables explicit consideration of trade-offs across a spectrum of risk choices and desired level of impact. As a result, there is divergent understanding of acceptable risks between the Board, committees, senior management and Secretariat staff. This hampers a clear comparison of actual risks with acceptable levels, leading to ambiguity in accepting or mitigating risks, and inconsistency in risk responses across different teams and individuals. There is also insufficient communication around risk, reactive reporting on risk events by the Secretariat and friction at the Board level when risks materialize.

While risk-related roles have been defined, related accountabilities for risk decisions are generally not clearly documented. An accountability framework was outstanding since 2013, although an initial draft was presented to senior management in 2016. The gap in defined accountability has limited the ownership for risk-related decisions and compliance, and makes embedding a risk management culture difficult. The indicator on corporate risk oversight under the 2014-16 key performance indicator (KPI) framework has been removed from the 2017-22 framework. Whilst the previous indicator had its own limitations, the lack of any replacement KPI reduces Board and senior management visibility over performance in risk management, and as a result can weaken accountability for related results.

[1] The Five-Year Evaluation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria *Synthesis of Study Areas 1, 2 and 3 M*arch 2009. One of its main findings on risk management was the lack of a robust risk management strategy.
[2] The Final Report of the High-Level Independent Review Panel on Fiduciary Controls and Oversight Mechanisms of the Global Fund, 19 September 2011
[3] Global Fund Risk Management Policy adopted at the Thirty-Second Global Fund Board Meeting Decision Point GF/B32/DP11.
[4] Bylaws of the Global Fund to Fight AIDS, Tuberculosis, and Malaria, 28 April 2016.

Due in part to the high degree of fragmentation in risk reporting, the Board has had sometimes to rely on ad hoc measures such as the Prioritized Action Plan to obtain a consolidated view of key cross-cutting risks and a mechanism to oversee progress in managing them.
Overall, whilst significant improvements have been in risk oversight and accountability processes, operating effectiveness still "**needs significant improvement**".

Effectiveness of the Secretariat's risk management framework and processes

A strong risk management framework is now in place at the Global Fund, following the approval of a Risk Management Policy, the establishment and strengthening of a Risk Department, the initiation of Enterprise and Operational Risk Committees and the rollout of the operational policy note on risk management across grant life cycle mentioned above. The introduction of an Organizational Risk Register is an important advance, but there is a need for more structured analysis to support the identification of key risks, the assessment of their impact, and the prioritization of mitigating actions. In addition, the effectiveness of those mitigation actions is often not adequately monitored or assessed for course correction.

The Risk and Assurance project was initiated to implement a structured process for mapping and optimizing risk mitigations and assurances. The assurances and risk mitigations were systematically defined, and development partners were identified for providing various additional assurances. However, even after completion of the pilots during 2016, their actual effectiveness remains questionable. For example, despite apparent mismatches between the identified portfolio risks and the investments in assurance, no adjustments have been made for any of the pilot countries to re-align the type or scope of assurance funded by the Global Fund with the underlying risk profile of each portfolio. Furthermore, clear agreements or alternative documentation have not been made available to development partners for most pilot countries, to ensure provision of assurances assigned to them.

The primary indicator of aggregate risk in the grants, the Portfolio Risk Index (PRI), represents a positive effort to measure and report portfolio risks. However, the indicator has significant limitations such as limited independent challenge (68% have not been presented to the Operational Risk Committee for validation during the last two years), the lack of risk weighting across risk categories, and low portfolio coverage (only 20 countries were used in the analysis for 2016). The risk management framework and processes are **therefore also** rated as **"need significant improvement"**.

The overall risk management environment and culture

An organization's risk culture determines, and is also reflected in, how it manages risks. The findings on governance, oversight and processes of risk management have therefore been considered in analyzing their impact on risk culture, and vice versa.

Difficulties in clearly articulating and operationalizing risk appetite and tolerance have led to a different understanding of risk acceptance between the Board, Secretariat and the three lines of defense. Further, at individual level, incentives or consequences have been unable to enforce sound risk management processes, with divergent staff attitudes towards risk. This can impact risk management, as demonstrated, for example, by low compliance for the program risk tool, the Qualitative Risk Assessment, Action Planning and Tracking Tool (QUART). The ongoing work on the accountability framework is a first step in embedding an accountability culture, but compliance gaps will also have to be addressed, by systematically building compliance reporting and monitoring within operational policies, and linking reported results with the accountability framework. In addition, a common understanding of key concepts of risk is required across individuals and teams, with diverse backgrounds and experiences, to ensure alignment of all risk management efforts. A lack of such shared understanding and ambiguity on acceptable risk behaviors inhibit effective communication about risk across the organization. The overall risk management environment and culture of the Global Fund has therefore been rated as "**needs significant improvement".**

II. Background

Environment in which the Global Fund operates

The Global Fund currently operates in over 100 countries representing nearly all of the global disease burden for HIV, tuberculosis and malaria.[5] Significant risks in the operating environment affect the way grants are implemented, including the following factors:

- the portfolio includes 88 of the world's 100 most corrupt countries,[6] who receive US$12.8 billion of the US$14.7 billion current portfolio allocation;
- a high disease burden, complicated by increasing drug resistance;
- high levels of poverty with over 50% of the population living below the multidimensional poverty index[7] in the top 15 funded countries supported by the Global Fund;
- low capacity in human resources, systems and tools which affects the ability to implement programs in country;
- political instability with 47 countries rated as "high risk" or "very high risk" based on the Global Fund's External Risk Index (ERI). The ERI is an aggregate of ten indices that capture political, economic, governance and operational factors contributing to external risk.

Evolution of the risk management function

In 2009 a review of the Global Fund's progress over the previous five years,[8] noted that the Global Fund did not have an organization-wide risk management strategy.

In 2011, a High Level Review Panel convened to examine the Global Fund's financial oversight and risk management. The panel's report[9] noted that economic realities, new technologies, and new epidemiological patterns required the Global Fund to evolve in order to remain relevant. This resulted in a Consolidated Transformation Plan which was approved by the Global Fund's Board in November 2011.[10] Risk management was considered a key transformation area, resulting in the creation of a Risk Management Department.

The main focus of the Consolidated Transformation Plan regarding risk management was to "declare a doctrine of risk and manage to it" through the following:

- strengthening internal governance by identifying and refining the role of the Board, the committees structure and membership framework;
- developing the corporate risk management framework;
- developing an operational risk management framework;

Extracts from historical institutional reports related to Global Fund risk management

"The Global Fund does not yet have a strategy for organization-wide risk management, which sets, at the level of governance, the boundaries of responsible risk taking, the explicit acceptance of levels of risk as integral to the purposes of the Global Fund, the conditions for its effectiveness, and finally, an objective and rigorous examination of the costs of risk avoidance."

The Five-Year Evaluation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria
Synthesis of Study Areas 1, 2 and 3
March 2009

"If you do business in these countries, you expect [corruption and diversion] to happen" as a natural consequence of development assistance. The Global Fund experience has shown that responsible actors in recipient countries, even very poor ones, can manage money effectively by employing good governance and management, with appropriate and active oversight from staff and partners.

The Final Report of the High-Level Independent Review Panel on Fiduciary Controls and Oversight Mechanisms of the Global Fund to Fight AIDS, Tuberculosis and Malaria, September 2011

"The Consolidated Transformation Plan set out to address a number of important challenges to the Global Fund's mission… The main challenges were:

- Inadequate management of corporate and operational risks without adapting to variations in the risk environment;
- Increasing complexity in grant processes with inconsistent procedures and quality standards;
- Issues related to measurement of results without sufficient focus on outcomes; and
- Challenges relating to the engagement of stakeholders at country-level, including Local Fund Agents and institutional partners"

Consolidated Transformation Plan, 25th Board meeting, November 2011

[5] 97%, 90%, 99% of the HIV, tuberculosis and malaria disease burden respectively as per 2014 Global Fund allocation model

[6] 2015 corruption index as per transparency international http://www.transparency.org/cpi2015

[7] Multidimensional poverty index measures both poverty and human development factors

Source: http://www.ophi.org.uk/multidimensional-poverty-index/mpi-2015/mpi-data/

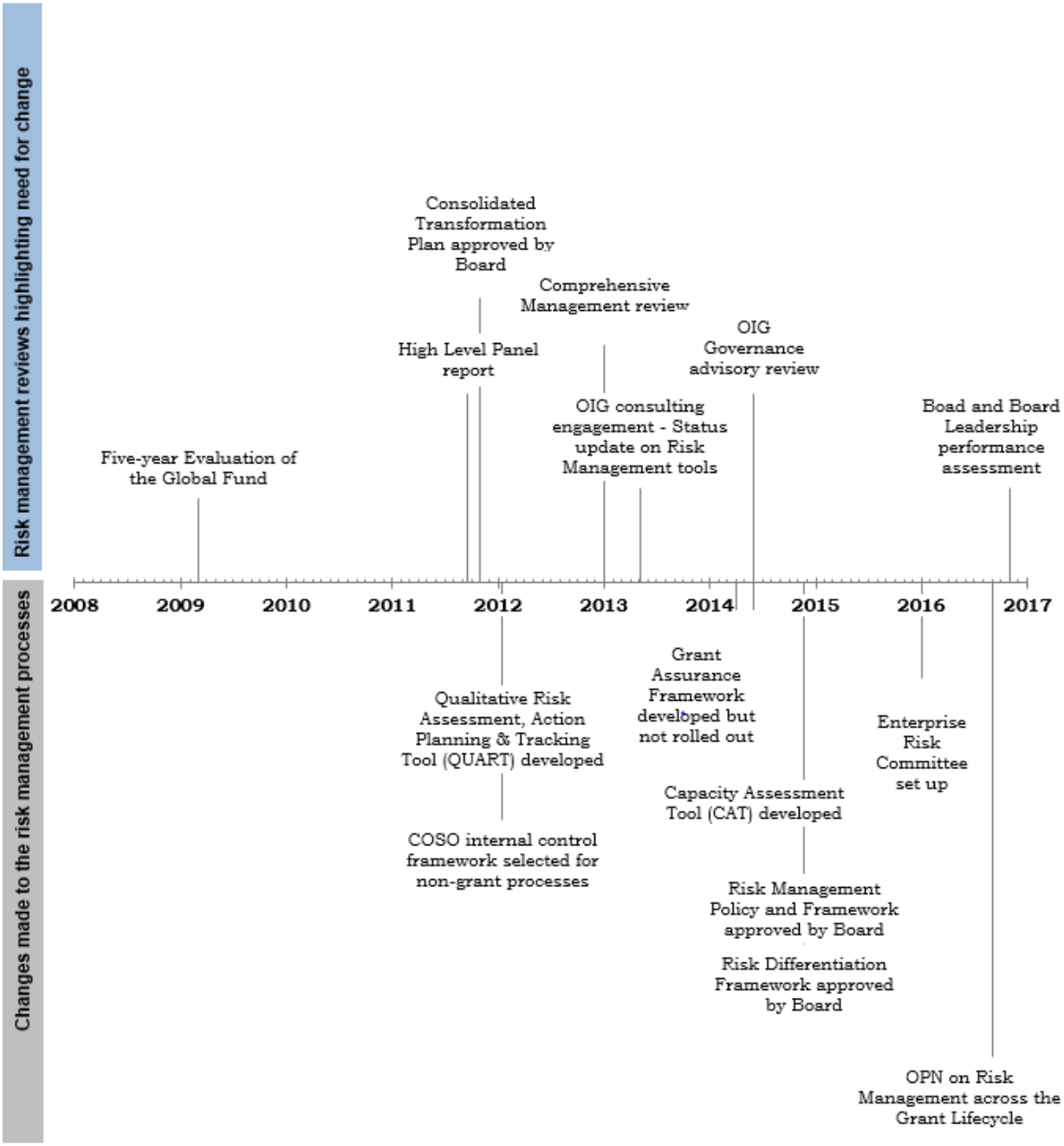
[8] The Five-Year Evaluation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria *Synthesis of Study Areas 1, 2 and 3 M*arch 2009

[9] The Final Report of the High-Level Independent Review Panel on Fiduciary Controls and Oversight Mechanisms of the Global Fund to Fight AIDS, Tuberculosis and Malaria issued September 19th 2011

[10] Decision Point GF/B25/DP6, 25th Board meeting

- segmenting countries and applying differentiated safeguards that focused on the risks in each portfolio;
- improving grant management processes, consistency of grant management deliverables and dissemination and generalization of best practices.

Figure 1: Timeline of risk management process milestones since 2008



In 2012, the Global Fund adopted the Committee of Sponsoring Organizations of the Treadway Commission (COSO) principles. COSO is a joint initiative of various private sector organizations[11] dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management and internal controls. COSO guidance is widely used for developing internal control systems to tackle organizational risks within operations.

[11] The organizations include American Accounting Association, American Institute of CPAs, Financial Executives International, the Association of Accountants and Financial Professional in Business, and the Institute of Internal Auditors.

Board's responsibility for risk management

The responsibility for risk management at the Global Fund is set out in the governance structure that defines the Board's responsibilities. As the supreme governing body, the Board has responsibilities to establish and oversee the following:

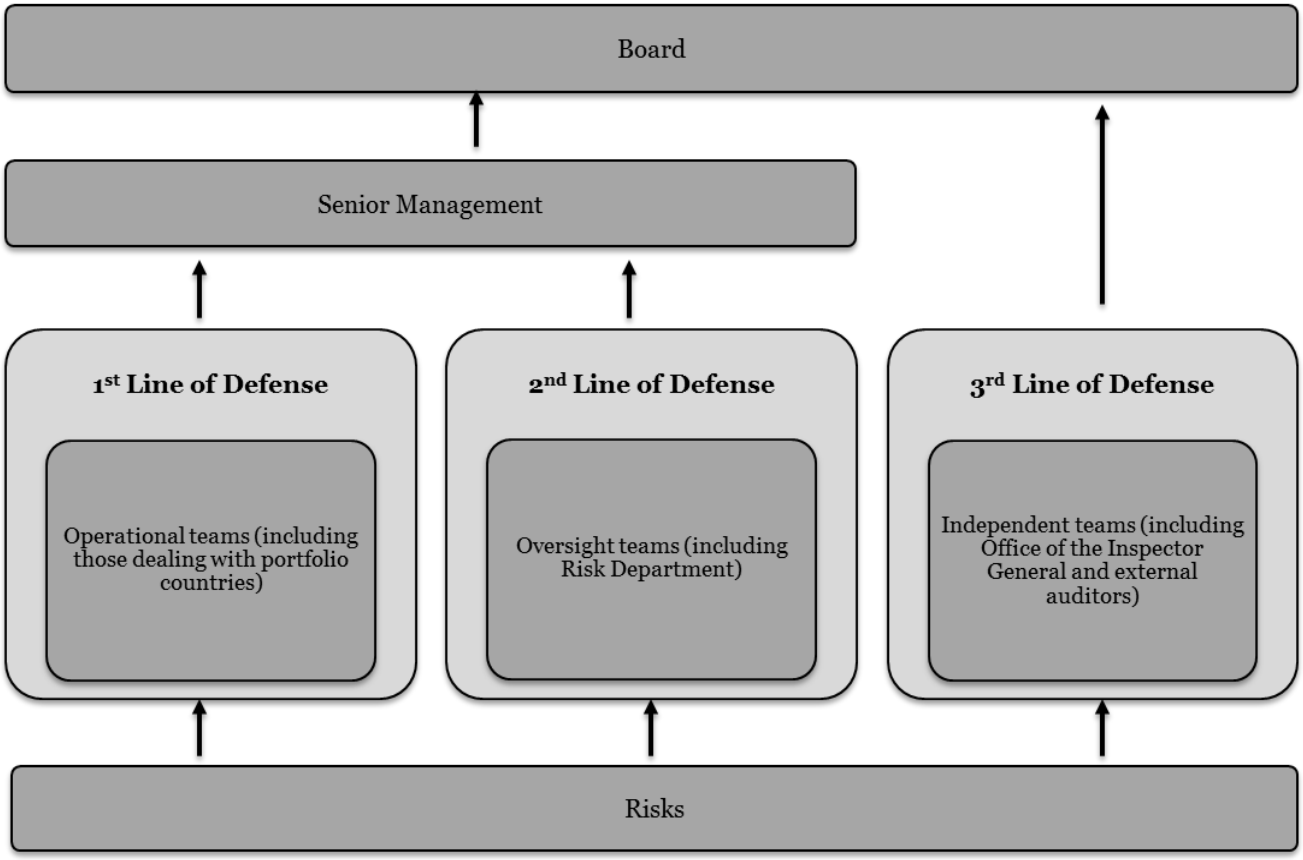
(i) a strategy for identifying and managing risk including but not limited to financial, reputational, legal, regulatory, operational and strategic risks;
(ii) a risk tolerance framework for the Global Fund.[12]

Specific roles and responsibilities on decision-making, oversight and advisory functions for risk management are divided amongst the three Board committees, with the Audit and Finance Committee taking the lead responsibility in coordinating risk issues.[13] A Coordinating Group, led by the Board Chair and comprising the Board Vice Chair, and the Chairs and Vice Chairs of all three committees, has been set up to support the Board's function.

Three lines of defense model

In 2014, the Global Fund adopted a three-line model of defense [14] for the management of risk. The model sets out the roles and responsibilities for risk management and internal controls. Management control is the first line of defense; risk, control and compliance oversight functions established by management are the second; and independent assurance is the third.

Figure 2 The Global Fund three lines of defense model



[12] Roles and functions of the Board as per the bylaws.
[13] Report of the Coordinating Group In-person meeting, November 2016, Decision item 1
[14] Three lines of defense model defined in the updated Global Fund Risk Management Policy 2014

Structure of the Risk Management functions in the Secretariat

Risk management functions at the Global Fund are delineated at the operational and senior management levels through the following committees:

The Enterprise Risk Committee (ERC)

The ERC was established in February 2016 to ensure that key enterprise-level risks are consistently and regularly reviewed by senior management. As per its terms of reference, the ERC is co-chaired by the Chief of Staff and the Chief Risk Officer and comprises:

- members of the Management Executive Committee,
- Head, Program Finance and Controlling,
- Head, Treasury,
- Head, Projects and Business Development,
- Head, Sourcing,
- Directors, High Impact Departments, Grant Management Division,
- the Inspector General (observer).

The primary role of the ERC is to:

- oversee the identification and prioritization of key enterprise risks;
- quality assure the strength and validity of associated mitigation actions and monitor their implementation; and
- ensure that appropriate assurance is applied to key enterprise risks.

Through its terms of reference, the ERC is empowered to delegate authority for risk oversight to individuals or committees, who are then required to report on progress to the ERC, as well as escalate cases.

Operational Risk Committee (ORC)

Although the ORC has been in existence since 2012, its role was revised in August 2016. The revisions aim to embed risk management throughout the full grant cycle through consistent and effective risk management. The ORC is co-chaired by the Chief Risk Officer and the Head of Grant Management Division. It comprises a total of eight voting members which include the heads of program finance, supply chain strategy, technical advice and partnerships and managers from the risk and legal teams.

The key responsibilities of the ORC are to:

- provide strategic direction on the risk management approach considering inherent and residual risks, and the effectiveness of both short term and long term actions; and
- facilitate more active and effective use of reprogramming and technical partners by challenging teams to adopt more strategic and solution-oriented approaches to key risks identified.

All high impact[15] and high risk[16] countries are subject to review by the ORC at least annually.[17] Other countries are included in this process at the discretion of the Head of Grant Management. This committee reviews the country risk dashboards and prioritized key risks and mitigations that are jointly prepared by the country teams and their risk focal point.

During the ORC meetings, the members discuss either of the following documents:

[15] Countries with an allocation above US$400million
[16] All countries indicated as high risk through the External Risk Index (ERI)
[17] Operational Risk Committee Terms of Reference updated August 2016

- ***Country risk dashboard*** – This summarizes the Country and Disease Program contextual information, key implementation arrangements and analyses of key stakeholders.
- ***Prioritized key risks and mitigation matrix*** – This summarizes the key strategic risks at the Country Portfolio level, and prioritized mitigation actions to address them.

The Risk Management Department

The Risk Management Department was set up in 2012 following the recommendation from the High Level Panel and is headed by the Chief Risk Officer. This department has as an approved headcount of 16 full time employees.

III. Scope and Rating

01 Scope

The overall objective of the audit was to provide reasonable assurance on the adequacy of design and operating effectiveness of the institution-wide identification and management of the risks to achieving the Global Fund's mission.

Approach and Scope

The audit included an assessment of:

- governance, oversight (including risk appetite and tolerances) and accountability associated with risk management at all levels, including the Board, its committees and management;
- the adequacy of the Secretariat's risk management framework and processes for the identification, assessment, response to and oversight of risks; and
- the overall risk management environment and culture.

02 Rating

The audit rating based on the findings are shown in the table below:

Operational Risk	Rating	Reference to findings
Governance, oversight and accountability of risk management at the Board and Senior Management levels.	Needs significant improvement.	01
Effectiveness of the Secretariat's risk management framework and processes	Needs significant improvement	02, 03
Overall risk management environment and culture	Needs significant improvement	04

IV. Findings and agreed management actions

01 Governance, oversight and accountability for risk management at Board level

Risk management structures have evolved considerably since 2012. The roles and responsibilities for risk governance and oversight have been allocated, a risk management framework and risk differentiation policy have been implemented, and a Risk Department has been established. However, weaknesses remain in the execution of oversight and accountability for risk management.

The Global Fund Board has an established governance structure with six core functions, one of which is risk management. The Global Fund By-laws make the Board responsible for establishing and overseeing the overall strategy for risk management, including defining tolerance framework for various risks.[18] To structure its risk management responsibilities, **the Board approved a Risk Management Policy**[19] in 2014, and adopted the definition of the Board's responsibilities for risk oversight from COSO principles.[20] The policy states that the Board is ultimately responsible to the Global Fund's stakeholders for overseeing the implementation of effective risk management and is required to:

i) understand the organization's risk philosophy and concur with the approach to risk differentiation;
ii) know the extent to which management has established effective risk management;
iii) review the portfolio of risk and consider it against the risk thresholds; and
iv) be informed about the most significant risks and whether management is responding appropriately.

Specific roles and responsibilities on decision-making, oversight and advisory functions for risk management are divided amongst the three Board committees, with the Audit and Finance Committee taking lead responsibility in risk coordination issues,[13] and support provided by a Coordinating Group[21]. The Board has approved the risk differentiation framework and directed the Secretariat to operationalize it, conduct annual reviews to update it, and report to the Board once a year on the outcome of such reviews[22]. This aims to guide the Secretariat's management of risks across a diverse, evolving and complex grant portfolio.

Although significant progress has been made in setting the appropriate structure and policies at Board level, the effectiveness of the Board's execution of its risk management responsibilities needs improvement in the areas highlighted below.

---

[18] Per the Global Fund bylaws, the Board has the responsibilities to establish and oversee the (1.) strategy for identifying and managing risk including but not limited to financial, reputational, legal, regulatory, operational and strategic risks; and (2.) risk tolerance framework of the Global Fund.

[19] Global Fund Risk Management Policy as adopted at the Thirty-Second Global Fund Board Meeting (November 2014) Decision Point GF/B32/DP11

[20] "Effective Enterprise Risk Oversight – the Role of the Board of Directors", COSO, September 2009

[13]

[21] Coordinating Group is chaired by the Board Chair and comprises the Board Vice Chair, and the Chairs and Vice Chairs of all three committees.

[22] Decision Point GF/B32/DP12, 32nd Board Meeting held on 21 November 2014

1.1 Defining risk appetite in the Global Fund context is challenging, but necessary.

Prior to the approval of the revised Risk Management Policy in 2014, the Board commissioned and accepted the results of the 2009 Five-Year Evaluation[23] and the 2011 High Level Independent Review Panel.[24] These reports, together with the Consolidated Transformation Plan[25] that resulted from the High-Level Panel, emphasized the need for the Board to set a risk appetite. After inclusion of related responsibility in the bylaws, the Board has signalled its desire to differentiate between risks taken in-country in its adoption of the Risk Differentiation framework in 2014. However, the Board's reluctance to define a risk appetite hinders its ability to oversee effective risk management by "understanding the organization's risk philosophy and concurring with the approach to risk differentiation,"[26] a key responsibility of the Board in the approved risk policy. Discomfort with the concepts of risk appetite and tolerance affects the Global Fund's progress in embedding a risk culture.

Risk appetite *is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style.*

- *Many entities consider risk appetite qualitatively, with such categories as high, moderate, or low.*
- *Risk appetite is directly related to an entity's strategy. It is considered in strategy setting, as different strategies expose an entity to different risks.*
- *Risk appetite guides resource allocation.*

Definition from COSO ERM Framework

The Secretariat sometimes receives conflicting messages from the Board and its committees: The review of Board and committee minutes sometimes indicated a reluctance to the use of language such as risk appetite and tolerance. For example, the Risk Differentiation Framework approved in November 2014 was initially presented to the sub-committees as a 'risk tolerance framework'. However three Strategy, Investment and Impact Committee members expressed "strong concern about the use of the words 'tolerance' or 'appetite' with the word 'risk', since it could "send the message that there is a tolerance or even an appetite for risk rather than zero tolerance."[27] All mentions of 'risk tolerance' were amended to 'risk differentiation' before the framework was presented to the Board for approval in November 2014. However, during the same period, the Audit and Ethics Committee challenged senior management and the Chief Risk Officer to provide details on risk management to enable the Board to explicitly define its risk appetite and tolerance levels.

Articulation of risk appetites allows an organization to explicitly consider trade-offs across a spectrum of risk choices and in relation to a desired level of impact. For example, in the case of the Global Fund, such trade-offs might involve the acceptance of a higher risk of over-stocked drugs expiring, and the related financial loss, in return for a desired lower risk of stock-outs that might lead to treatment disruption and potentially higher programmatic costs. In this hypothetical scenario, the organization would have consciously accepted higher risk in one area of its operations in order to reduce risks in another area deemed to yield better programmatic return. In general, a sound framework of risk appetite and tolerances allows the organization to explicitly consider these important trade-offs and to make informed decisions about its risk choices. In the absence of such a framework at the operational level, as is currently the case at the Global Fund, risk decisions can be inconsistent as different teams and individuals exhibit different behaviors and responses to similar risks based on their own level of comfort rather than based on a unifying set of organizational risk principles. At the governance level, the lack of clearly understood risk appetite and tolerances also mean that the Board can have divergent views of risk within its own body as well as in comparison to the Secretariat.

[23] The Five-Year Evaluation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria *Synthesis of Study Areas 1, 2 and 3 M*arch 2009
[24] The Final Report of the High-Level Independent Review Panel on Fiduciary Controls and Oversight Mechanisms of the Global Fund to Fight AIDS, Tuberculosis and Malaria issued September 19th 2011
[25] The Global Fund Consolidated Transformation Plan adopted in the 25th Board meeting November 21-22 2014 Board decision point GF/B25/4
[26] Global Fund Risk Management Policy as adopted at the Thirty-Second Global Fund Board Meeting (November 2014) Decision Point GF/B32/DP11
[27] 13th SIIC meeting held 7-9th October 2014

Defining a risk appetite can significantly enhance the Board's ability to hold senior management accountable for effective management of risks.

1.2 Development of a structured process for following up on risk issues is necessary to enhance the Board's effective oversight of risks.

The Board, Committees and Coordinating Group's process for recording and escalating key risk issues can be made more effective. This was previously highlighted in the OIG Advisory Governance review[28] and emphasized by the Working Group on Governance in its presentation to the Board in November 2014[29].

I Information about risk needs to be more tailored and aligned with the oversight needs of the Board and its committees. For example, at its 34th meeting in November 2015, the Board requested an update from the Secretariat on the integration of risk management into its operations and culture; however, the multiple challenges raised by the Board were incompletely addressed in the Secretariat's update at the following Board meeting.[30] In the October 2014 Audit and Ethics Committee meeting[31], the committee noted that the Risk Management Policy was a first draft and that significant additional work was needed to make it all encompassing of reputational, legal and other risks and to make it fit for purpose. The committee also asked the Chief Risk Officer to educate the Board on their roles and responsibilities as set in the policy. Despite requests from the Audit and Ethics Committee, there is no evidence of discussions of the Risk Management Policy at the previous Strategy, Impact and Investment Committee to review if relevant strategic risks had been considered.

Effective follow-up on these Board requests and concerns is needed to ensure that relevant issues are continuously tracked.[32] The lack of follow-up discipline was highlighted in the end-of-term reports issued by the outgoing committees, which noted the need for an action tracker to ensure that issues discussed by committees are followed up appropriately.[33] Follow-up processes have been strengthened lately and action trackers were developed in late 2016, but further improvements are needed in the tracking of areas such as the previously requested mapping of implementation risks for the new 2017-22 Global Fund Strategy. The Board self-assessment reflected a similar sentiment, with 33% of respondents mentioning that the Secretariat could more appropriately consider the opinions and perspectives of the Board members.[34] Despite the progress noted in risk management discussions at Board level, addressing these gaps would enhance the Board's ability to perform an effective oversight role as described in the risk policy and also bolster the trust between the Board and the Secretariat..

Agreed management action 1:

The Secretariat will present a paper to the Board recommending risk appetite for the key risks to delivering the 2017-22 strategy. The paper will include broad principles to operationalize the risk appetite. If approved by the Board, the Secretariat will implement the principles approved by the Board to use risk appetite in portfolio decisions.

Owner: Chief Risk Officer
Target date: 30 June 2018 (presentation of principles to the Board)
Target date: 31 December 2018 (implementation of the risk appetite principles)
Refer to AMA 3 below for actions related to risk reporting including trends in risk appetite.

[28] GF-OIG-14-008 Advisory report Governance review 6 June 2014
[29] 32nd Board meeting 21-21 November 2014
[30] 32nd and 34th minutes of the Board meeting.
[31] 10th Audit and Ethics Committee AEC meeting held on 8th October 2014
[32] Coordinating Group meeting held on 26th February 2016
[33] 9th Audit and Ethics Committee meeting held on 8th March 2014
[34] GF/B36/19 Results of Board and Board Leadership Performance Assessment completed by EgonZehnder and presented to the Board in November 2016

02 Oversight and Accountability at senior management level

The overall design of risk management structures at the senior management level is adequate; however there are improvements are needed in the definition of risk accountabilities and in the effectiveness of oversight processes.

Our review was split across three main areas: the design of risk management structures, the clarity of accountabilities over risk management, and effectiveness of oversight at the senior management level.

i) Risk management structures

The Risk Management function within the Global Fund has been strengthened through the establishment of the Risk Department and the creation of a Chief Risk Officer position in 2012. This was complemented by the establishment of the ORC to oversee grant-level risks. At the operational level, the Secretariat developed a country team responsibilities matrix in 2013, which defines the roles and responsibilities of different country team members. The Secretariat also started developing in 2016 a business process owner matrix, which aims to assign responsibilities for different business processes besides grant management to individuals/teams. In 2016, an Enterprise Risk Committee was created to oversee corporate level risks.

With these reforms, the design of risk management structures within the Global Fund is now generally adequate, with delineated roles and responsibilities at each level for appropriate risk management decisions.

ii) Accountabilities for risk management

The Global Fund's performance is measured through corporate and operational performance indicators, as well as internal performance measurement mechanisms used within different teams. At individual levels, staff responsibilities, as defined in their terms of reference, are considered in staff performance management. However, the OIG noted the following:

2.1 Risk accountabilities need to be clarified in order to strengthen risk management performance

While risk-related roles have been defined, related accountabilities for risk decisions are generally not clearly documented. The need for an accountability framework in the Global Fund was identified in 2013.[35] The framework is necessary to instill ownership for decisions taken and to assist in ensuring compliance among staff. The Secretariat prioritized the accountability framework in 2016, and it has been finalized and approved by the Management Executive Committee in early 2017.

iii) Effectiveness of oversight processes

With the establishment of the Risk Department, the Chief Risk Officer position, and the Enterprise Risk and Operational Risk Committees, the various responsibilities of senior management for risk are clarified through their respective terms of reference. However, the following areas need further improvements to enhance the effectiveness of management oversight:

2.2 Strong key performance indicators are needed to measure risk

Corporate and strategic objectives for the Global Fund are tracked through Corporate Key Performance Indicators (KPIs) with reporting on progress done at Board and senior management levels. In the earlier 2014-2016 Strategy, portfolio and grant risks were tracked at strategic level through a "Portfolio Risk Index" corporate KPI. This indicator had multiple gaps in its quality and content (detailed in Section 3.4), with only limited use and reliance by senior management in decision-

35 This agreed management action is from GF-14-006 High Level Audit of the Global Fund Assurance Model.

making. However, instead of improving or replacing this risk indicator with a better one, this risk indicator has been removed from the proposed performance indicators under the 2017-2022 corporate KPI framework, without any replacement at this stage, although the risk team is exploring solutions. Until an alternative is developed, clear metrics of risk at the portfolio level remain a gap in the risk management oversight framework.

2.3 The risk decisions at the ORC should be explicitly documented and consolidated into risk themes

Although the Operational Risk Committee has been in existence since 2012, its role was significantly revised in August 2016. This was done to embed risk management throughout the full grant cycle and ensure a consistent approach to risk management at the grant level. The committee provides an opinion on whether each country's risks have been appropriately prioritised and adequately mitigated. It is also supposed to comment on the risk management approach taken by grant managers and escalate significant and cross-cutting issues to the ERC for further review. This design is suitable for effective, tiered risk management of core operations. However, there are challenges in the ORC's effective implementation of its mandate:

- ***There is a need to enhance visibility of overall portfolio level risks***: The ORC process reviews risks at a grant level. Whilst this is consistent with the ORC mandate, it is also important that recurring risk themes or emerging trends across different grants be tracked and periodically evaluated to provide broader portfolio-level insights and inform higher-level risk analysis at the Enterprise Risk Committee level. The records for the five ORC meetings reviewed in this audit did not provide evidence of a process to aggregate and document these risk themes or trends. Enhancing this analysis and documentation, coupled with related improvements in the quality and content of risk reporting (see section 3.4 for details), would provide a clearer understanding of how the portfolio-wide risks are reviewed by the ERC, and how the ORC discussions inform the portfolio-wide risk decisions.

- ***Explicit decisions on acceptance, mitigation or escalation of risks should be documented****:* Although risk dashboards are prepared and presented by the country teams, the committees do not explicitly decide on risk responses. For example, at the Nigeria ORC committee in May 2016, the Country Team noted that the residual risk (that is the risk remaining after the impact of all risk mitigations applied) from capacity issues was high, with specific contextual challenges. However, the discussion did not determine how those risks would be escalated and monitored, whether the risks were acceptable, or how mitigation measures would be monitored and, if necessary, escalated to other governance bodies.

Addressing the areas of improvement noted above would both provide senior management with a more holistic view of risks and contribute to a more systematic embedding of risk management into the culture of the organisation.

2.4 Oversight by the Risk Department

The Risk Department has grown from four at the time of its establishment in 2012 to 16 full-time approved positions in 2016. This is accompanied by a corresponding increase in the Risk Department's role in enterprise and operational risk management. Besides representation on the Enterprise and Operational Risk Committees, the risk team has enhanced its involvement in various key stages of the grant management process, including their representation in the Grants Approval Committee, and their right to objection against disbursements where risks have not been adequately addressed.

In terms of skills and experience, there has been a concerted effort to recruit new risk resources and to improve the skills of existing staff on the risk management team. This includes new risk certifications by two members of staff after joining Risk department, with one more member of staff in the process. Other training courses have also been taken by the risk team. However, the Chief Risk

Officer is the only staff member in the department with directly relevant, specialist risk experience prior to joining the department. While other staff members have valuable grant management experience, including supply chain, programmatic and finance, their skills and experience in evaluating other risks, such as treasury, are low. In the absence of a competency framework against which the skills requirements for the risk team can be compared, the department may be unable to adequately assess its skills gaps.

The Risk Department has recently initiated a series of in-country reviews under the Risk and Assurance project. This is a significant development in the team's capacity to oversee grant management at the country level. However, the oversight of non-grant processes is not as effective as there is minimal formal monitoring of other enterprise risks such as finance, treasury[36] or IT activities, with the risk team dependent on information provided to them, and including these risks in coverage can improve the risk team's ability to effectively oversee these activities.

Agreed management action 2:

The Secretariat will design and implement a standard format for ORC discussions, and standard outputs, including justification of ORC risk ratings adjustments and risk responses, which can include mitigation or risk acceptance.

Owner: Chief Risk Officer, in conjunction with Head Grant Management Division
Target date: 30 September 2017 (for design of revised formats and outputs)
Target date: 31 December 2017 (implementation of the revised formats and outputs)

Agreed management action:

Refer to AMA 2 from GF-OIG-14-006-High Level Audit of the Global Fund Assurance Model for creation of the accountability framework clarifying roles and responsibilities on risk management.

Agreed management action:

Refer to AMA 2 from GF-OIG-17-01-Global Fund Treasury Management for Risk department guidance on review of Treasury business processes.

[36] OIG Audit of Global Fund Treasury Management, GF-OIG-17-001.

03 The adequacy of the Secretariat's risk management framework and processes

The lack of a comprehensive risk management strategy at the Global Fund was first noted in the Five-Year Evaluation[37] review in 2009 (see box inset). As a result, a risk policy and a related framework were completed by the Secretariat and endorsed by the Board in 2009.[38] The subsequent High Level Review Panel Review report[39] in 2011, noted that the framework developed in 2009 did not include a corporate and operational view of risks and recommended that the risk framework be updated. Subsequently, a number of improvements have been made:

The lack of a robust risk management strategy during its first five years of operation has lessened the Global Fund's organizational efficiencies and weakened certain conditions for the effectiveness of its investment model. The recent work to develop a comprehensive, corporate-wide risk management strategy is a necessary step for the Global Fund's future

The Five-Year Evaluation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria March 2009

- COSO framework principles were adopted in 2012 to assist with the evaluation and improvement of enterprise risk management and support a framework for controls;
- The **Organizational Risk Register was developed in 2013 to record entity level risks**; it is updated on a quarterly basis by risk owners and presented to the Management Executive Committee and the assigned Board committee;
- An updated risk management policy and framework were approved by the Board in 2014[40];
- In 2015, the 20 non-grant processes were identified for COSO compliance.[41] For this process, the respective owners were encouraged to develop risk and control matrices for the processes identified.

These tools and processes are now used for enterprise wide risk management at the Global Fund. However, despite these improvements to enterprise risk management, further improvements are needed in the Global Fund's approach to assessing, managing, mitigating and reporting of risks.

Assessment of Risks

3.1 There is a need for a more comprehensive, data driven approach to risk identification and prioritization.

Risk identification- For grants, the Secretariat mainly uses the Qualitative Analysis and Reporting Tool (QUART) to assess portfolio risks.[42] While the identification of various risks is generally effective, their consolidation across different, stand-alone risk tools has been challenging. Efforts are ongoing to integrate the QUART tool with various other documents and tools containing risk information, to minimize duplication and to ensure completeness of portfolio risk information.

However, for non-grant processes, the development of risk and control matrices does not always consider all key risks within the specific business unit. For example, in the OIG audit review of treasury processes, it was found that key processes and risks such as Asset and Liability Management were not considered in the approved initial risk and control matrix.

In addition, there is also need for a more structure and better documented process for the analysis and prioritization of risks included in the Organizational Risk Register.

---

[37] The Five-Year Evaluation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria *Synthesis of Study Areas 1, 2 and 3 M*arch 2009

[38] GF/B20/DP15 Approved by the Board on 11 November 2009

[39] The Final Report of the High-Level Independent Review Panel on Fiduciary Controls and Oversight Mechanisms of the Global Fund to Fight AIDS, Tuberculosis and Malaria issued September 19th 2011

[40] Global Fund Risk Management Policy as adopted at the Thirty-Second Global Fund Board Meeting (November 2014) Decision Point GF/B32/DP11

[41] Compliance with COSO internal control framework was required for supporting processes in the Risk Management Policy approved in 2014.

[42] Capacity related risks are identified through the Capacity Assessment Tool (CAT). The residual capacity risks are to be tracked through QUART during grant implementation.

Mitigation and assurance on Risks

3.2 Risk mitigation processes require increased focus on measurable actions, clear assignment of ownership for those actions and systematic monitoring of progress.

Risk mitigations have historically been documented and followed up through internal tools like the QUART, and external communications such as management letters to implementers. The following improvements are needed to enhance the effectiveness of risk mitigation::

- **Corporate mitigation initiatives should be translated into measurable actions.** For example, poor quality of programs and services are in the Q1 2016 Organizational Risk Register, with the current risk rating measured as high, and the target risk rating as medium. Corporate mitigations identified in the risk register include the development of holistic program quality and effectiveness strategy, routine monitoring and national surveillance, strengthened patient follow-up and expansion of public-private mix. However, these broad objectives do not translate into specific action points and clear targets that can be tracked and evaluated on a systematic basis. On the other hand, progress is being made in translating some organizational risk mitigation initiatives into operational targets. For example transition planning is being based on specific readiness assessments that will lead to country-level targets.

- Mitigations at grant level have in some cases **focused on symptoms, and should instead tackle root causes.** For example, the construction of additional warehouses did not resolve Tanzania's storage challenges. The root causes of the challenges were the country's decision to hold large stocks and its failure to dispose of large volumes of expired stocks, which should be tackled.[43] This issue is expected to be resolved through the ongoing Supply Chain initiative.

- **Complex mitigations have had joint owners, but clear individual accountabilities and effective monitoring are needed.** For example, supply chain related risks have been included in the risk register since 2013, but systematic solutions were not prioritized until 2016. The Risk and Assurance project (detailed later) targeted to address risk mitigation and assurance issues was initiated in 2014 and concluded in mid-2016. In both cases, the initiatives required efforts from both operational and functional teams, but the roles were not clearly defined. And, in both cases, effective monitoring likely would have lessened some of the noted delays in addressing the issues.

3.3 The Risk & Assurance initiative has mapped risks and assurances in pilot countries, and identified development partner organizations for providing additional assurances. However, efforts are needed to fully align assurances with prioritized risks, and remove gaps and duplications.

Acknowledging that the Global Fund had not historically mapped its controls, mitigations and assurances over portfolio risks in a structured manner,[44] the Secretariat committed to addressing these issues through the Risk and Assurance project. After earlier unsuccessful attempts, the project was reshaped and re-launched at the end of 2015 in six pilot countries[45] (representing 11% of the 2014-16 funding cycle allocation) and concluded in June 2016.

The assurances in the pilot countries have been assessed, and key risk matrices (KRMs) have been developed, to identify main risks, mitigations and assurances. For areas where assurance was missing or weak in the six pilot countries, development partner organizations have also been identified to provide additional assurances. In terms of benefits, four out of six countries noted improved

[43] Source: Diagnostic review of MSD in Tanzania
[44] Agreed management actions are from GF-14-006 High Level Audit of the Global Fund Assurance Model and GF-13-017 Advisory Risk Management Tools.
[45] The pilot countries are Zambia, Sudan, Somalia, Ethiopia, Indonesia and Cambodia.

prioritisation of risks resulting from the pilots. Despite this progress, the following adjustments in the Risk and Assurance project processes are needed to improve the effectiveness of the assurance framework:

- ***Assurances funded by the Global Fund need to be aligned with key risks or value for money.*** Despite indications of a possible mismatch between portfolio risks and investments in assurance, no changes have been proposed in the type, scope or coverage of the assurance products funded by the Global Fund, for any of the six pilot countries. For example, health products were rated as the highest risk for all six pilot countries, but the Local Fund Agent resources for assurance related to this function remain the lowest in all pilot countries, compared to other areas such as finance and data quality. The monetary value of spending in individual areas of assurance does not provide conclusive evidence of a mismatch with the distribution of risks in a portfolio. However, it may indicate potential gaps in the allocation of assurance resources and point to a need for adjustments.

- ***Improvements are needed to address duplications and to better coordinate assurance efforts at country level.*** The Risk and Assurance initiative, now being rolled out to the High impact and risk portfolios, seeks to coordinate assurances across functional risk owner teams[46]. However, this coordination needs improvement. For example, three of the six pilot countries are also included in the ongoing supply chain initiative. However, in the absence of an integrated framework by country, there is increased risk of the risk and supply chain teams duplicating efforts because supply chain issues also rank among the highest areas or risk.

  The Global Fund Finance team has incorporated finance measures like restricted cash policy, and fiscal and fiduciary agents in various high risk countries. However, standard tools should be used to review their effectiveness in addressing target risks, and to ensure their consistent application across the portfolio. Financial risk management guidelines are being developed to clarify application of these measures for ensuring consistency across the portfolio, and to measure their results. An integrated risk tool is currently being developed, which is targeted to integrate and simplify risk processes, leading to enhanced buy-in and compliance by operational teams.

- ***Need for formal agreements with Assurance Partners*:** For areas where assurance was missing or weak in the six pilot countries, development partner organizations were identified to provide additional assurances. However, a formal agreement with partner organizations, along with a structure for continuous monitoring and reporting, has not been secured. As a result, arrangements are not in place to ensure that assurance solutions assigned to partners have been effectively agreed and monitored. The Ethiopia pilot demonstrated that where formal agreements with partners are difficult to obtain, mutually agreed key risk matrices can be used as a realistic alternative.

[46] Functional Global Risk owners include Program Finance, Supply Chain Department/Health Products Management Hub, Technical Advice and Partnerships Department, Monitoring Evaluation and Country Analysis Team, and Legal team.

Reporting of Risks

3.4 Reporting on risk management at Board and senior management level has been enhanced to include operational risks, and annual risk management and assurance reports. However, reporting on risk management requires significant further improvement around quality, content and timeliness.

Before 2012, the Global Fund Board and senior management were not provided with any enterprise-wide information on risk. However risk reporting started in 2013 with the development of the Organizational Risk Register and the Operational Risk Report. Since then, the Chief Risk officer discusses the updated Organizational Risk Register with the Coordinating Group on a quarterly basis. The Chief Risk Officer also provides an Annual Risk Management Report and Assurance Statement to the Board[47] and risk is a standing item on the agendas of the Board and relevant committees. Risk presentations are made at every Board meeting and joint meetings are also held during committee sessions. However, there is room for improvement around the quality, content and timeliness of risk reporting:

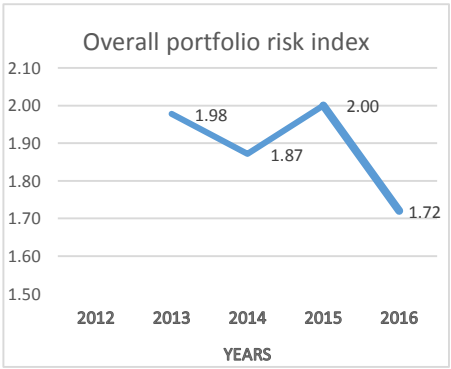
In terms of the quality of risk reporting:

- ***The Board should receive a complete view of prioritized risks and interdependent risks should be assessed together:*** The Coordinating Group has previously noted that the Risk Register, the document used to communicate risk status to the Board, contained several overlapping or 'complementary' risks. For example, the risk of low grants absorption is directly related to the risks of low staff capacity levels and poor country systems. They requested that such risks be viewed holistically; this means that the inter-linkages of various risks are clearly identified, along with how the measures to address some risks will affect others, for example how improving the country-level fund flow and other systems will improve grants absorption. The Coordinating Group suggested that this aspect be brought to the Board's attention in the Chief Risk Officer's report as well as the joint committee report. These requests need to be addressed.

- ***Risk reports should analyze risks taken against the returns (impact) to inform decision-making:*** the Strategic Investment and Impact Division has recently produced enhanced analyses on different disease intervention choices to help Country Teams prioritize investments within individual portfolios, and optimize impact. Some analyses have also been initiated to compare investments in different diseases and countries, and how that affects the overall impact achieved by the Global Fund, within the existing total funding. However, these analyses have not yet considered the business risks, and how portfolio investments or risks can be varied to optimize disease impact against portfolio risks.

In terms of the content of risk reporting:

- ***The Board and senior management need a reliable measurement of the Secretariat's performance on risk management at the grant management level:*** At the operational level, the Secretariat produces an Operational Risk Management report, which has been presented to senior management since 2012. This report includes the Portfolio Risk Index (PRI) which is derived by consolidating the country-level operational risk measurements performed by the Secretariat through the QUART tool. This PRI measure is reported to the Board in the Chief Risk Officer's annual

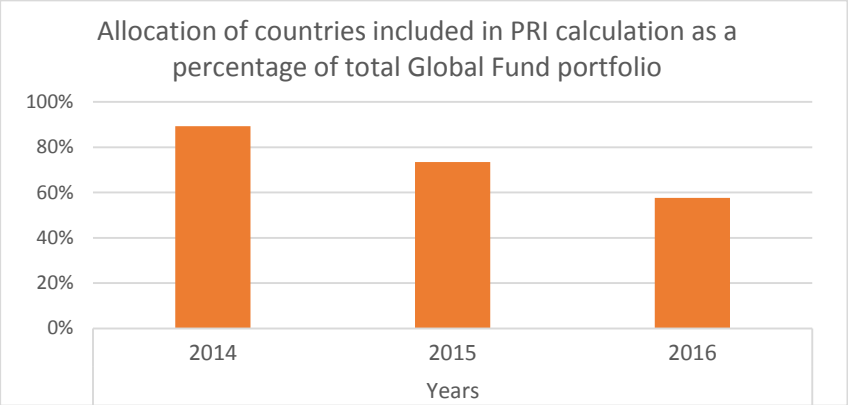


[47] The first Annual Assurance Statement was shared with the Board in its 34th Board meeting.

report.[48] The PRI is a positive effort towards informing decision-makers about the status and performance on operational risks. However, the following improvements are needed in process and methodology in calculating PRI:

- ***PRI uses a simple average of the 19 functional risks, regardless of their importance in the portfolio:*** Although the overall Global Fund portfolio is over 54% commoditized, the health products category has been assigned an equal weighting to other risks (such as data quality and Country Coordinating Mechanism governance) when calculating the PRI score.[49] For grant portfolios that are heavily commoditized, with mostly drugs being directly provided and little money actually disbursed to the implementers, a logical approach would require that health product risks be weighed differently than financial risks.

- ***The PRI calculation should be representative of the portfolio:*** Different grants and countries have been used for the year-on-year analysis. Only 20 countries were used in the analysis for 2016, compared to 44 in 2015 and 59 in 2014.



- ***Consistency is needed in the criteria to determine which countries should complete the QUART in order to facilitate year-on-year comparison*:** During the first roll-out of the QUARTs in 2012, only high impact countries were expected to complete a QUART. In 2013, non-high impact countries with an annual budget above US$10 million were added to the countries required to complete the QUART. In 2015, countries with very high external risk levels were also added.

The root causes of the issues noted around the quality and content of risk reporting are as follows:

- ***The importance of operational risk measurement needs to be re-emphasized at the Secretariat.*** Although the issue of low compliance of QUART was noted by the risk team and efforts were made by senior management to address it, compliance did not improve.[50] The KPI that monitored its completion has been retired, although the risk team is exploring alternate solutions. The processes were also seen by Country Teams as duplicative and not adding much value, which also contributed to low compliance.

- ***The Risk Department, second line of defense, reports PRIs based on risk ratings derived from the Country Team, the first line of defense, but stronger independent challenge is needed***. Although the ORC reviews the ratings presented to them, 68% of grant risks scores have not been presented to the ORC for validation during the last two years, a significant decrease from prior periods. As a result, the PRI reported by the risk function does not represent an independent view of grant level risks. Low risk team headcount has been one of the contributing factors. Independent challenging is likely to increase with recent increases in staff headcount. The Risk Department is currently developing a new tool which will separately record risk levels and their mitigations as per operational teams and as per risk teams.

[48] The measurement of the PRI is based on four functional and nineteen sub-functional risks, which are rated between zero and four (no risk to very high risk respectively).
[49] Commodities budget includes health products, equipment and procurement and supply management support costs, as per Business Analysis and Reporting Tool in November 2016.
[50] In 2014/15, CRO reported that only 67% of the countries required to complete the QUART actually did it.

- ***The Board should be further engaged in challenging the reporting of portfolio risks.*** Board members were trained on risk management in 2015, but not on the detailed methodology for calculation of the PRI. There was a lack of evidence of senior management and the Operational Risk Committee detailed review of the calculations and methodology.

The risk team recognizes the challenges in using the PRI for providing a reliable measurement of Secretariat's performance on risk management, and is exploring solutions to replace or improve the indicator.

Agreed management action 3 (related to Finding 01, 02 and 03):

The Secretariat will develop and implement an enhanced risk measurement and reporting framework which will:
- measure risks for countries while considering their materiality to disease impact,
- consolidate a holistic picture of risks across the Global Fund, and
- assess whether risks in countries are in line with the risk appetite, to inform decision-making.

The framework will ensure adequate portfolio coverage, and consistency of measurement approach across periods.

Owner: Chief Risk Officer
Target date: 30 June 2018 (development of the framework)
Target date: 31 December 2018 (implementation of the framework)

Agreed management action 4:

In conjunction with the Grant Management Division, the Secretariat will define a process to align assurances plans, including the assurance activities financed by the Global Fund, to prioritized risks, and use it for all countries rolling out the Risk and Assurance reviews.

Owner: Chief Risk Officer
Target date: 31 March 2018

04 The overall risk environment and culture

Risk culture describes "the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose".[51] An organization's risk culture both determines and reflects how it manages risks. The findings on governance, oversight and processes of risk management have therefore been considered in analyzing their impact on risk culture, or vice versa.

Common and aligned purpose, values and ethical standards –The Global Fund's mission and purpose are clearly captured in its vision and mission statement, and its business model is based on accepted principles.[52] The Global Fund Staff Code of Conduct also cites six key values[53] to guide employee behavior. All staff have a responsibility to promote these values, with performance assessed through staff performance management mechanisms. As a result, there are robust arrangements to align organizational and staff overall values and interests.

However, in relation to risks, finding 1.1 details the difficulties experienced by the Global Fund in clearly articulating and operationalizing a risk appetite, which have led to a different understanding of risk acceptance between the Board and the Secretariat. Similar differences exist between the three lines of defense. Without defined, agreed metrics around risks taken, staff and representatives for the Global Fund cannot manage risks on the same agreed basis.

Clear assignment of authority and responsibility at the individual and organization level –Findings 01 and 02 lay out where the Global Fund has made significant improvements on the allocation of individual and collective responsibilities for risk, at both the Board and senior management levels. However, these findings also articulate where individual or team responsibilities on monitoring, mitigating or accepting risks are not clear.

The ongoing work around the accountability framework is a positive, first step in embedding accountability in the organization's culture. Finding 3.4 highlights the low compliance with the QUART tool completion requirements, with accountability for non-completion and use of incentives or disincentives for risk actions and decisions being important to register improvements.

Transparent and timely information sharing and communications – this means that people within the Global Fund Board and Secretariat discuss risk issues openly, using a common vocabulary. As mentioned in finding 1.1, one of the challenges in defining a risk appetite is the divergent understanding of what it means. Similar challenges exist at the operational level on interpreting concepts of assurance, lines of defense and residual risks, as noted throughout the audit tests and discussions. These issues are due to a lack of a common understanding of various risk concepts.

[51] Definition from the Institute of Risk Management, see https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-culture.aspx. Despite its importance, there are no established standards or generally accepted practices for risk culture. For key characteristics of a well-performing risk culture, see also "Cultivating a Risk Intelligent Culture", 2015, Deloitte Development LLC; "Auditing risk culture - Art or science?" 2009, PwC Australia.
[52] Global Fund Principles per its Governance Handbook are partnerships, transparency, country ownership, and performance –based funding http://www.theglobalfund.org/en/overview/
[53] The core values guiding employee conduct are integrity, dignity and respect, collaboration, passion, innovation and effectiveness.

Individuals and teams with diverse experience and backgrounds interpret risk terms and concepts differently, and determine how to apply process guidelines based on their judgement. More clarity on acceptable risk levels can enhance open and transparent communication around risk information.

Established, embedded and monitored processes and controls –The Global Fund adopted COSO principles, a widely used framework for developing internal control systems to tackle organizational risks, in 2012.[54] One of the eight COSO components of enterprise-wide risk management is implementing control procedures to ensure risk responses are effectively carried out.[55] Improvements in the quality of operational policies have been registered in 2016 and many now include "checks and balances" to ensure that risks are considered. For example, the recently developed policy note on *Risk Management across the Grant Life Cycle* provides checkpoints for the risk team to object to grant signings or disbursements.

However, there is still room for improvement in embedding these practices into day-to-day operations. Nineteen OPNs have been updated since 2013, but risk management and compliance practices have not been systematically embedded within these operational processes.[56] For example:

- The OPN on risk management requires the Secretariat to consider the results of the risk analyses when making disbursement decisions, but it does not specify the process to do this, or how compliance with the OPN will be monitored and reported to senior management.
- The Program and Data Quality Operational Policy Note requires consideration of reported risks when determining the appropriate method/ tool for data quality reviews. The note requires documentation and approval of the rationale for method/ tool selected by the Monitoring and Evaluation team and the relevant Regional Manager. However, the level of compliance of this policy by country teams is not compiled and reported to senior management.

A focus on learning and challenge –At the Global Fund Board level, there has been a clear appetite for learning and challenge: it has commissioned several substantial reviews designed to strengthen its governance and operations (2004, 2009, 2011, 2015), and also initiated a series of periodic evaluations of the core business of the Global Fund (2007, 2011). At the Secretariat, a series of lessons learned exercises have driven improvements to the New Funding Model and grant allocation processes. However lessons learning and challenging ways of working could be further improved. For example, on embedding a series of risk-based check and balances into processes, finding 3.4 identifies that the only measurement of risk in the Global Fund, was based on ratings devised by the Country Teams, and needs enhanced independent challenge from the risk team.

Agreed management action:

Earlier AMAs on risk appetite, risk framework and the ongoing work on accountability framework will address the identified issues.

Agreed management action 5:

In conjunction with the Chief of Staff and Ethics Officer, the Secretariat will establish procedures for measuring and reporting the status of compliance of all key controls of key business processes.

Owner: Chief Risk Officer
Target date: 31 December 2018

[54] Compliance with COSO internal control framework was required for supporting processes in the Risk Management Policy approved in 2014.
[55] COSO's ERM-Integrated Framework component 6
[56] These OPNs have not been reviewed for their compliance with COSO internal control framework, which would have ensured strong internal controls and compliance practices.

V. Table of Agreed Actions

#	Agreed Management Action	Target date	Owner
1	The Secretariat will present a paper to the Board recommending risk appetite for the key risks to delivering the 2017-22 strategy. The paper will include broad principles to operationalize the risk appetite. If approved by the Board, the Secretariat will implement the principles approved by the Board to use risk appetite in portfolio decisions.	30 June 2018 31 December 2018	Chief Risk Officer
2	The Secretariat will design and implement a standard format for ORC discussions, and standard outputs, including justification of ORC risk ratings adjustments and risk responses, which can include mitigation or risk acceptance.	30 September 2017 31 December 2017	Chief Risk Officer in conjunction with the Head of Grant Management Division
3	The Secretariat will develop and implement an enhanced risk measurement and reporting framework which will: • measure risks for countries while considering their materiality to disease impact, • consolidate a holistic picture of risks across the Global Fund, and • assess whether risks in countries are in line with the risk appetite, to inform decision-making. The framework will ensure adequate portfolio coverage, and consistency of measurement approach across periods.	30 June 2018 (design of framework) 31 December 2018 (implementation of framework)	Chief Risk Officer
4	In conjunction with the Grant Management Division, the Secretariat will define a process to align assurances plans, including the assurance activities financed by the Global Fund, to prioritized risks, and use it for all countries rolling out the Risk and Assurance reviews.	31 March 2018	Chief Risk Officer
5	In conjunction with the Chief of Staff and Ethics Officer, the Secretariat will establish procedures for measuring and reporting the status of compliance of all key controls of key business processes.	31 December 2018	Chief Risk 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 Office of the Inspector General (OIG) performs its audits in accordance with the global Institute of Internal Auditors' (IIA) definition of internal auditing, international standards for the professional practice of internal auditing (Standards) and code of ethics. These Standards help ensure the quality and professionalism of the OIG's work.

The principles and details of the OIG's audit approach are described in its Charter, Audit Manual, Code of Conduct and specific terms of reference for each engagement. These help our auditors to provide high quality professional work, and to operate efficiently and effectively. They also help safeguard the independence of the OIG's auditors and the integrity of their work. The OIG's Audit Manual contains detailed instructions for carrying out its audits, in line with the appropriate standards and expected quality.

The scope of OIG audits may be specific or broad, depending on the context, and covers risk management, governance and internal controls. Audits test and evaluate supervisory and control systems to determine whether risk is managed appropriately. Detailed testing takes place across the Global Fund as well as of grant recipients, and is used to provide specific assessments of the different areas of the organization's' activities. Other sources of evidence, such as the work of other auditors/assurance providers, are also used to support the conclusions.

OIG audits typically involve an examination of programs, operations, management systems and procedures of bodies and institutions that manage Global Fund funds, to assess whether they are achieving economy, efficiency and effectiveness in the use of those resources. They may include a review of inputs (financial, human, material, organizational or regulatory means needed for the implementation of the program), outputs (deliverables of the program), results (immediate effects of the program on beneficiaries) and impacts (long-term changes in society that are attributable to Global Fund support).

Audits cover a wide range of topics with a particular focus on issues related to the impact of Global Fund investments, procurement and supply chain management, change management, and key financial and fiduciary controls.

Annex C: Executive Director Statement

Programs supported by the Global Fund have saved more than 20 million lives, by effectively preventing and treating HIV, tuberculosis and malaria. Our results, as reported in January 2017, include:

- More than 700 million mosquito nets to protect families from malaria;
- More than 16 million courses of treatment for TB;
- More than 10 million people on antiretroviral therapy for HIV

The impact of these efforts is clear, contributing to a 69 percent fall in mortality rates among children under five, and impressive decreases in the number of people who die from AIDS, TB and malaria. What many thought impossible 15 years ago has now been achieved.

Achieving those results requires daily decisions with a risk-benefit calculus, across the Global Fund partnership. When a community health worker decides whether or not to administer a diagnostic test; when a health provider chooses which prevention, treatment and adherence measures to select for a patient; when a Principal Recipient is chosen; when a procurement tender is awarded; when a fiduciary agent is placed to tighten control over a specific program – in every instance, risk management is an essential component of maximizing impact and achieving long-term success. Improving global health goes hand in hand with effective risk management.

Strategies to improve health systems are constantly developing, just as societies and economic progress continue to develop. We call it "development" for a reason. In all of our work, we encounter risk, and we do not ignore or shy away from it. Instead, we approach it in a proactive way, constantly strengthening measures to better address changing epidemiology and risk environments with a high degree of transparency and accountability.

As a partnership that invests a significant amount of public money for public good, the Global Fund has a special responsibility to make sure that every dollar, euro, pound or yen goes where intended. The Global Fund is committed to constantly improving risk management, from strategic planning to decision-making to our overall culture as an organization. We aim to identify and mitigate key risks to acceptable levels, and also to provide assurance that controls and mitigating actions are operating as planned.

With a fundamental change in our business model, implementing a new funding model, we embarked on more active risk management processes. Over the past four years, with strong guidance from the Board, we have established a risk management framework, a risk policy, and a Risk Department, while systematically leveraging work done by partners. We have taken strong measures to reduce financial management risk in programs, inserting fiscal agents or other additional safeguards where needed, with highly positive outcomes.

Equally important, we have built greater risk oversight and more rigorous assurance planning into the grant lifecycle. We are creating alignment with in-country partners on key risks and mitigations, and provided a greater focus on key organizational risks thorough a new committee Enterprise Risk Committee with clearer accountability of key players.

The Office of the Inspector General is a central and important part of providing assurance, conducting independent audits and investigations to complement the active risk management and controls put in place by the Secretariat with oversight by the Board of the Global Fund. The OIG's Audit Report on Global Fund Risk Processes validates our extensive work, recognizing the significant enhancements to risk processes and the overall culture of risk management, with considerable improvements in risk management governance, oversight and accountability, including a risk management framework and risk differentiation policy. The audit is aligned with the Secretariat's assessment as reflected in the recent Risk Report by the Chief Risk Officer, and also identifies areas where we can do better and

continue to improve. Establishing clear guidance on risk appetite, setting a better internal control environment, improving tools for programmatic and supply chain assurance, strengthening internal assessments, rolling out independent reviews, and continuously enhancing organizational culture – these are all areas we are pursuing.

Our Chief Risk Officer believes that if the momentum in operationalizing the results of the current initiatives is maintained, the development and operationalization of Risk Appetite and build-out of a robust internal control environment will enable the Global Fund to achieve an 'Embedded' state of maturity in 18 months. This will require leadership and governance from the Board and a continued change in culture. The Chief Risk Officer is also confident that the agenda set for 2017 on these matters is appropriate and achievable and that it will advance enterprise wide risk management at an optimal pace.

Following the findings of the Audit on Risk Management Processes, the Global Fund will accelerate the implementation of actions already identified, and with further steps will continue to strengthen and improve the effectiveness of our investments:

- The Secretariat will present a paper to the Board recommending risk appetite for the key risks to delivering the 2017-22 strategy. The paper will include broad principles to operationalize the risk appetite. If approved by the Board, the Secretariat will implement the principles to use risk appetite in portfolio decisions.

- The Secretariat will design and implement a standard format for ORC discussions, and standard outputs, including justification of ORC risk ratings adjustments and risk responses, which can include mitigation or risk acceptance.

- The Secretariat will develop and implement an enhanced risk measurement and reporting framework which will measure risks for countries while considering their materiality to disease impact, consolidate a holistic picture of risks across the Global Fund, and assess whether risks in countries are in line with the risk appetite, to inform decision-making. The framework will ensure adequate portfolio coverage, and consistency of measurement approach across periods.

- The Secretariat will define a process to align assurance plans, including the assurance activities financed by the Global Fund, to prioritized risks, and use it for all countries rolling out the Risk and Assurance reviews.

- The Secretariat will establish procedures for measuring and reporting the status of compliance of all key controls of key business processes.

The Global Fund partnership has made exceptional progress towards the global goal of ending epidemics, but we are not there yet. We need every dollar to get the job done. This is where an effective risk management approach, zero tolerance for corruption and a commitment to constantly evolve and improve play a vital role.

We are grateful for the suggestions for improvements and will pursue them.

Respectfully,

Mark Dybul