Aidspan
Independent observer of the Global Fund

Audit of Global Fund Fraud Risk Management

Background

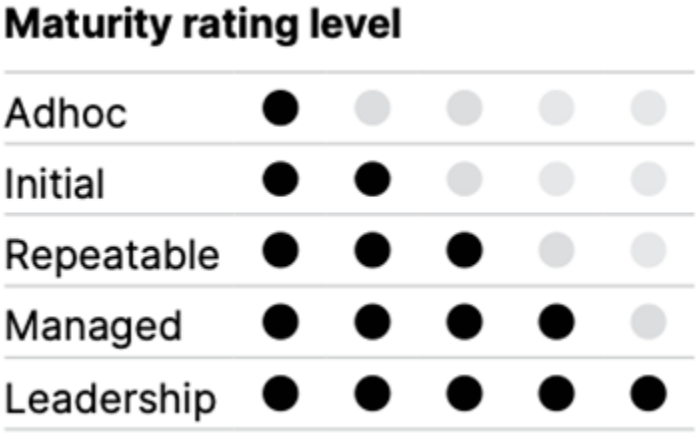
On 6 July the Office of the Inspector General (OIG) issued its audit report on Fraud Risk Management.

The OIG assessed the maturity of the Global Fund's fraud risk management framework against the five core components set out in the guide on fraud risk management published in 2016 by The Association of Certified Fraud Examiners (ACFE) and The Committee of Sponsoring Organisations of the Treadway Commission:

1. Fraud risk monitoring
2. Fraud risk governance
3. Risk assessment
4. Fraud control activity
5. Fraud investigation and corrective activity

The OIG also rated each component using the five-point scale from the Enterprise Anti-Fraud Maturity Assessment Model (in the Anti-Fraud Playbook: The Best Defense Is A Good Offense. 2020 Grant Thornton LLP and ACFE) – see Figure 1.

Figure 1: Anti-fraud Maturity Rating



The Global Fund operates in challenging environments which expose its programs to fraud and abuse. Most countries supported by the Global Fund are ranked below average on the Corruption Perceptions Index (CPI) published by Transparency International. About $6 billion of Global Fund monies go to countries in the bottom 45 of the 180 countries in the CPI report. Eligible Global Fund countries in the bottom half of the CPI score account for 83% ($10.3 billion) of Global Fund allocations.

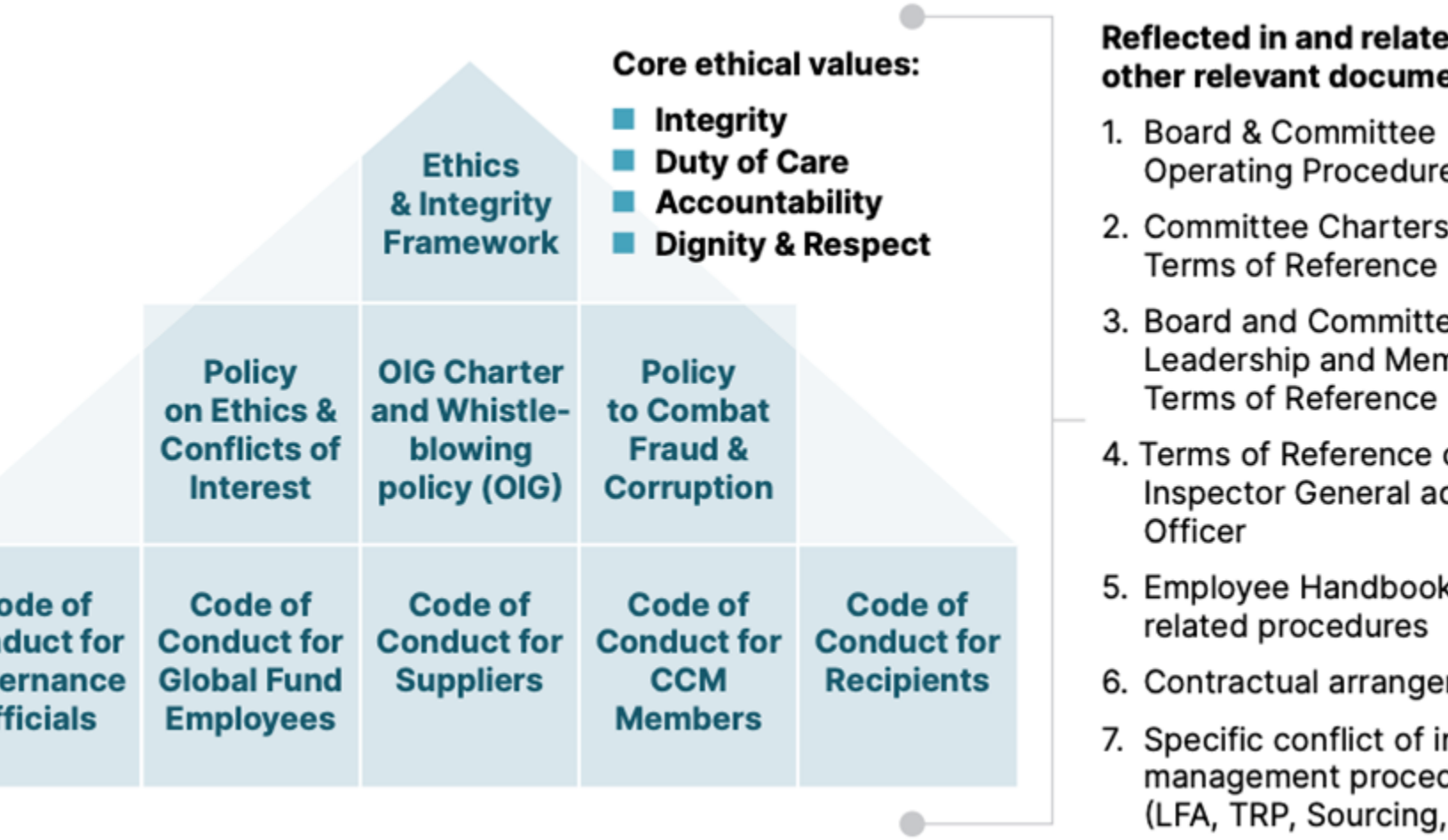
The COVID-19 pandemic and changes in working practices have increased opportunistic fraud in programs, requiring strong monitoring mechanisms.

In 2017, the Board, in approving the Policy to Combat Fraud and Corruption (PCFC), defined fraud as any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation. The definition of fraud risk was widened to consider programmatic as well as financial risks: specifically, section 3.3 of the PCFC states that “The Global Fund recognizes that fraud and corruption infiltrate not only financial management, but also strategic decision-making, governance, public health systems, program quality and reporting.”

Programmatic fraud refers to fraud other than financial frauds, such as “health product substitution and counterfeiting, as well as misrepresentation or manipulation of any information arising from or relating to Global Fund Activities such as proposals, plans, evaluations, performance data, epidemiological data, reports, and audits” (PCFC, section 4.3).

The Global Fund Board and its Committees have approved several policies and guidance documents relevant to fraud risk management (Figure 2 below).

Figure 2: Main Anti-fraud Policies and Guidelines at the Global Fund



Fraud risk management at the Global Fund

The Global Fund Integrated Risk Management framework is built on three lines of defence: (1) the Country Team and support of in-country assurance providers; (2) the Risk Department and other risk owners, such as the Technical Advice and Partnerships team, Finance Department and Supply Operations; and (3) the OIG and the external auditor, who report to the Board or its Committees.

Fraud trends: types of allegations and sources

During 2019-2021, the OIG opened 489 investigations into the following types of allegations:

- Theft of equipment, commodities and money, referred to as abusive practices (157 investigations, or 32% of cases);
- Fraudulent practices, which included data manipulation, misrepresentation and fraudulent documents (116 investigations, or 24% of cases);
- Price fixing, bid rigging and Conflicts of Interest, referred to as collusive practice (71 investigations, 15% of cases); and
- Corrupt practices including bribery (66 investigations, 13% of cases).

Fraudulent and corrupt practices therefore collectively accounted for 37% of cases investigated by the OIG in this period.

Not all investigations result in a published report; the OIG issues case closure memoranda when the investigation is inconclusive or an allegation is unfounded (the evidence does not support the allegations), not material, there has already been a proportionate response, risks have been mitigated, or deficiencies

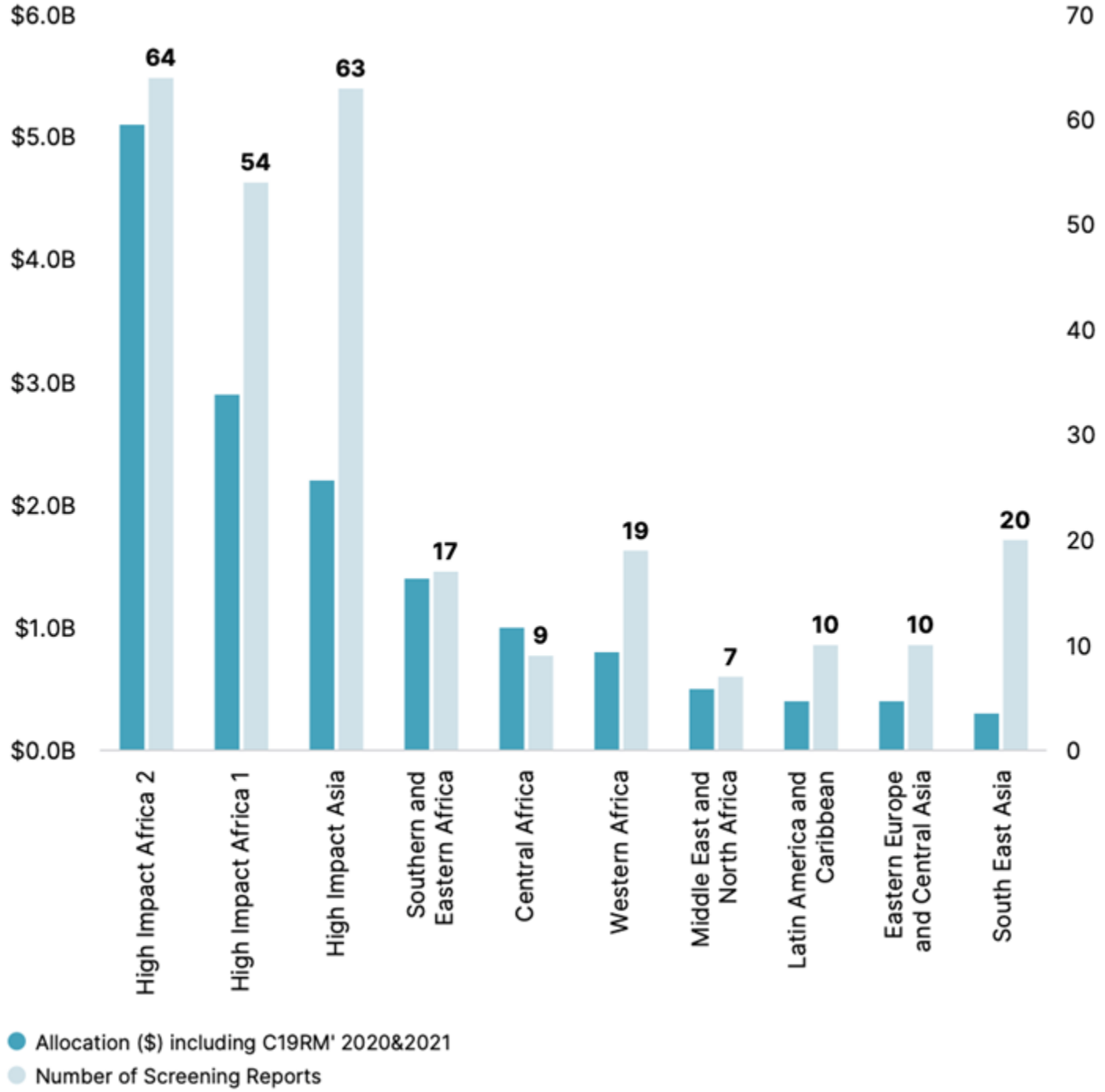
addressed.

OIG investigations produce Agreed Management Actions (AMAs) based on lessons learned from cases. AMAs included financial recoveries, sanctions of entities and individuals, and the strengthening of controls and processes.

The OIG identified non-compliant transactions totalling $143.2 million between 2019 and 2021, most of them due to fraudulent practices and theft. In the same period, the proposed recoveries of funds as a result of OIG investigations during that period was $14.4 million. Principal Recipients (PRs) and sub-recipients (SRs) are most frequently the subjects of OIG investigations, respectively accounting for 42% and 23% of investigations.

The number of allegations generally aligns with the size of funds allocated by region, with most allegations affecting grants in the Global Fund’s High Impact Africa 1, High Impact Africa 2, and High Impact Asia regions (see Figure 3).

Figure 3: Allocation and Number of Screening Reports by Region



As of 31 December 2021, the Secretariat had reported $26.7 million in outstanding recoverable amounts resulting mostly from non-compliance expenditures and mismanagement.

Audit objective, scope and rating

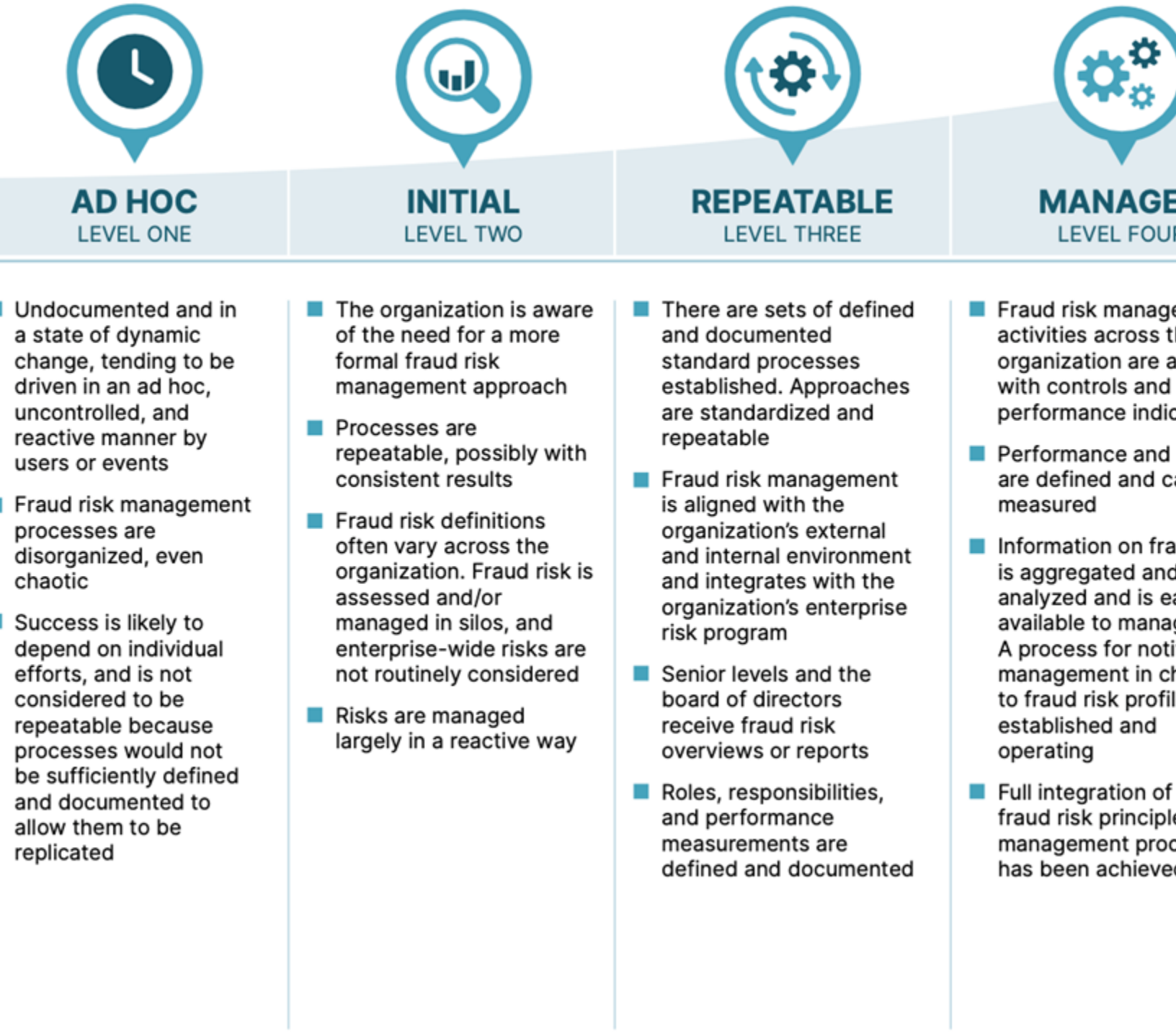
The audit sought to assess the maturity of the Global Fund's framework (including policies and procedures) on fraud and corruption and to position the organization in a rating scale for further improvement.

The Global Fund's fraud risk management framework was reviewed against the five components list under Background above.

Instead of using the standard audit rating scale, the OIG used the assessment model to rate the maturity of the Global Fund fraud risk management framework and its underlying processes. Maturity is split into

five stages – ad-hoc, initial, repeatable, manageable and leadership, as shown in Figure 4.

Figure 4: Enterprise Anti-fraud Maturity Model from Anti-fraud Playbook by ACFE/Grant Thornton

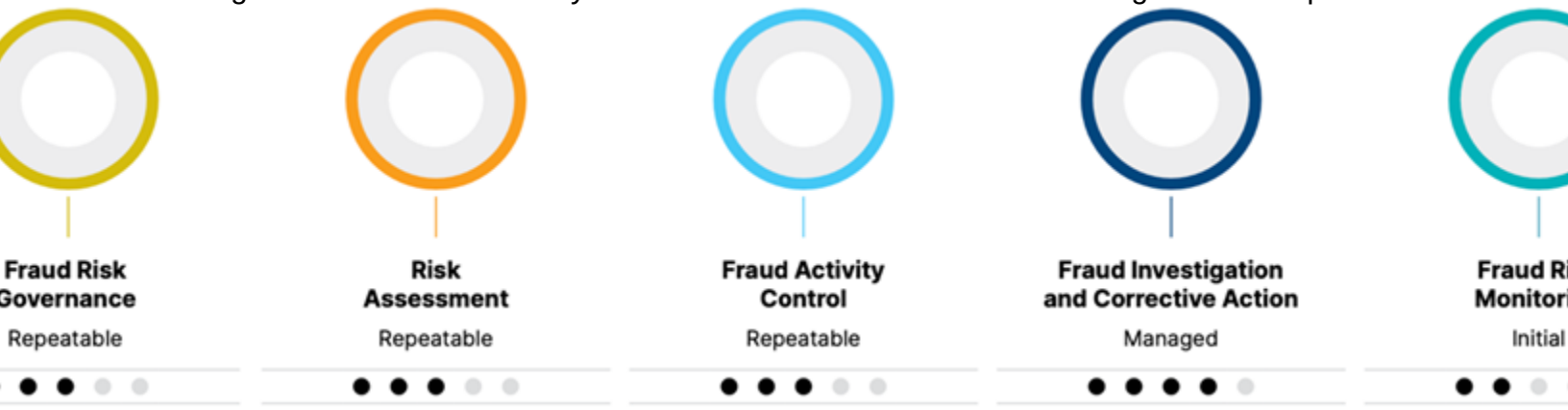


Audit conclusions on overall maturity

The COVID pandemic and changing work practices have led to increased fraud risk. Agile risk management is needed to anticipate and institute preventive and detection controls to respond to potential fraud. The various elements of the Global Fund's approach are at different levels of maturity. As the fraud risk landscape evolves, the organization will need to strengthen its preventive and monitoring activities, and to put more focus on non-financial fraud.

The maturity level for each component assessed by the OIG is shown in Figure 5.

Figure 5: Assessed Maturity Model of Fraud Risk Assessment Management Component



Audit conclusions on fraud risk governance

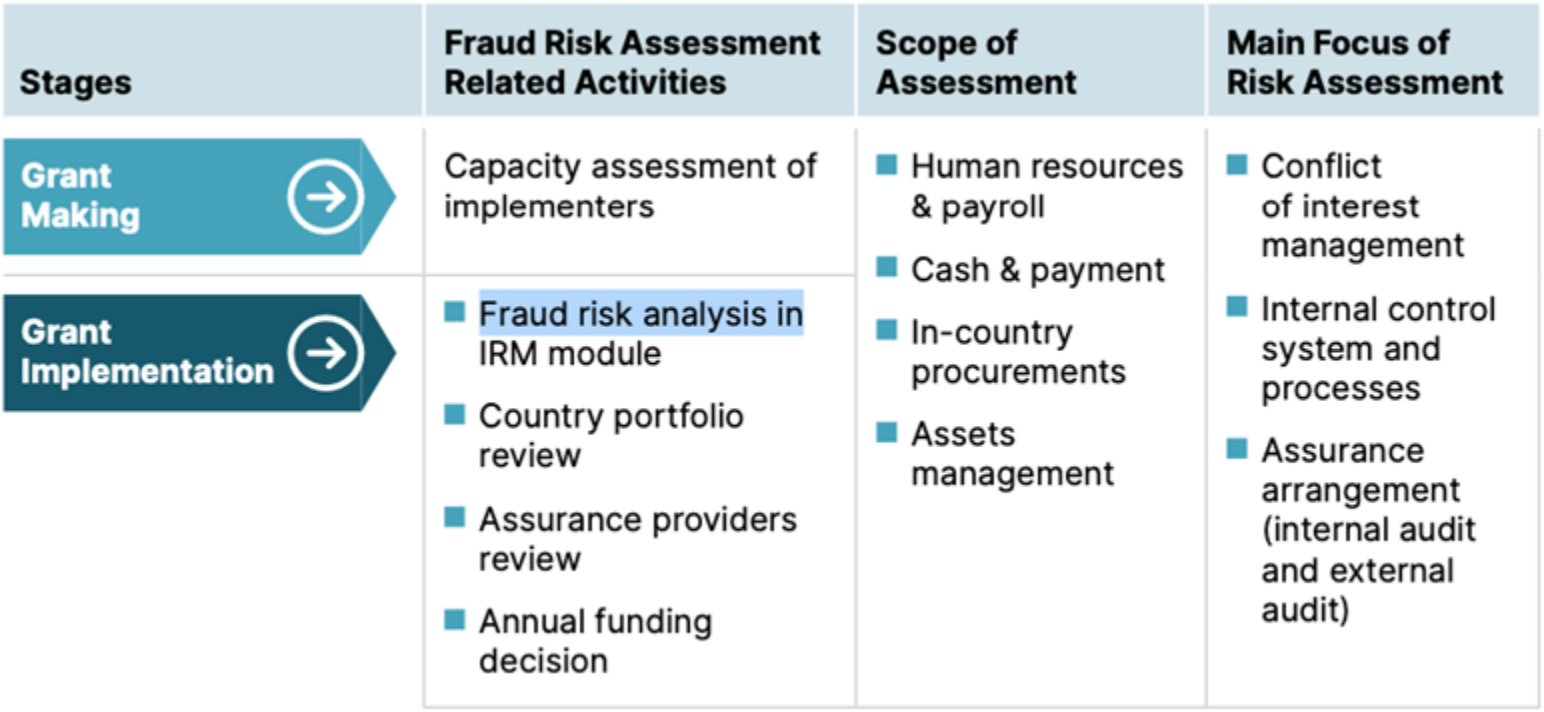
The Global Fund has defined frameworks, policies, structures and processes which direct the management of fraud risks and support its zero tolerance of prohibited practices. While significant progress has been made regarding financial fraud risks, there is less consideration of programmatic fraud risks. There is limited clarity in roles and responsibilities for programmatic fraud risks at Board, Committee and Secretariat levels. The Secretariat needs to define overall ownership and accountability for fraud risk and implement the PCFC plan.

Audit conclusions on risk assessment

Integrated Risk Management framework processes are generally aligned with the Global Fund's internal and external environments. Tools have been developed to support assessments in core functions, leveraging the work of assurance providers. To further mature, fraud assessment needs to proactively identify fraud scheme types, improve the implementation of mitigation measures, and consider grant-level programmatic risks.

At grant level, fraud risk assessment is considered at various stages of the grant life cycle, as described in Figure 6.

Figure 6: Process for Financial Fraud Risk Assessment



The Global Fund has created tools and guidelines to support capacity assessment of implementers, but their design and effectiveness need to be improved. The Capacity Assessment Tool (CAT) is not a fraud risk assessment tool and does not provide visibility on how risk could manifest at the implementer level. Rather, it focuses on whether an implementer has the capacity and systems to execute its role under the grant. Fraud risks could manifest in various forms including collusion, corruption, and management override of controls despite the implementer having capacity and systems in place. Hence, using the CAT to determine fraud risk ratings, particularly at the beginning of grants for new implementers, could underestimate the level of risk, or fail to identify the most significant risks.

The report emphasises the need to improve the documenting of fraud risk considerations during the grant life cycle:

- In eight sampled portfolios, 14 of the 20 implementers were found not to have undergone a capacity assessment in the previous and current funding cycle despite the assessment tool including specific-fraud risk requirements.
- In 24 of 34 sampled grants, the basis for fraud risk root causes and ratings in the Integrated Risk Management (IRM) Module was either not documented or the explanation provided was inadequate. Of the 24 grants, 12 did not consider fraud risk in subsequent portfolio decisions.
- Programmatic fraud is part of the predefined root causes in the IRM Module. However, Country Teams did not select it as a prioritized root cause in assessing fraud risk in 30 out of the 34 sampled grants for data management, and in 23 out of 28 grants for supply chain.

Only five of 20 mitigation measures related to portfolios with high fraud risk ratings had been implemented as of their due date of 31 December 2021. Two of the three mitigation actions to mitigate inherent fraud in the Secretariat's Human Resource Management processes have been outstanding since 2020. OIG concludes that this is due to insufficient prioritization of fraud risk mitigation measures.

Audit conclusions on fraud activity control

Defined controls exist, but preventive controls over programmatic fraud risks need major improvement. Controls over integrity risks are missing at the grant level. Assurance activities need improvement to

identify and escalate red flags and prompt reporting of red flags by assurance providers and Secretariat is needed.

Audit conclusions on fraud investigations and corrective action

Mechanisms have been established to enable stakeholders to report fraud cases. An independent investigation function exists, which was recently independently assessed as operating in line with adopted guidelines and industry practices. The Global Fund takes corrective action to address findings from investigations, and to recover losses from all assurance providers. The Board is regularly updated on the status of actions taken and recovery efforts. To further mature in this area, the Global Fund needs a structured approach to synthesize and learn lessons from suspected and actual fraud cases, and to strengthen its sanction processes.

Audit conclusions on fraud risk monitoring

Some established monitoring controls exist, but in the absence of a comprehensive fraud risk monitoring approach, they are not consistently performed. While the PCFC implementation plan is work in progress, the Secretariat has demonstrated alertness to changes in the risk landscape during the COVID-19 pandemic: an organizational Risk Framework includes routine monitoring activities of certain components of fraud risks, and the Secretariat has developed a monitoring and oversight framework for the COVID-19 Response Mechanism (C19RM) to identify and address programmatic and operational bottlenecks. Completing the planned evaluation activities in the PCFC implementation plan and leveraging the existing arrangements under C19RM will enhance the organization’s maturity in fraud risk monitoring.

Agreed Management Actions

The Secretariat will develop a roadmap to determine and implement its fraud risk management program in line with the operating risk environment within which it aims to deliver the 2023-2028 Strategy. As part of the process, the Secretariat shall:

1. By 31 March 2023, define a target maturity level for each component of the fraud risk management maturity model, considering the current level of exposure to fraud risks and the operating environment.
2. By 31 December 2022, agree on the overall responsibility to drive execution of the actions agreed in the PCFC implementation plan.
3. By 30 June 2023, review and enhance assurance arrangements related to programmatic activities, to ensure key fraud risks, particularly related to data reporting, are prevented, or identified early and mitigated.
4. By 31 March 2023, establish an overall approach to monitor the evolution of fraud risk at enterprise level, including oversight responsibilities of first and second-line functions.

Commentary

The report of the previous OIG audit of risk management, published in May 2017, rated the following three areas as needing significant improvement:

- 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.

It is a pity that this report does not show clearly what improvements have been achieved in these three

areas.

That said, here is OIG's response to the above comment:

"(1) There is a need to distinguish the enterprise risk management – ERM (audited in 2017) and the fraud risk management. Although the fraud risk management is integrated into the enterprise risk management (ERM), it has specific guidelines & policies (See figure 2 above VS Global Fund risk management guideline), different regulation bodies (ACFE for fraud risk and ISO for enterprise risk management, COSO works on both), different standards & requirements (COSO_ACFE fraud risk Guide VS ISO 31000 &COSO ERM framework), different maturity rating and components (component 4 "Fraud investigation and corrective actions" has no equivalent in ERM). There are specific structures to address fraud risk (e.g: OIG investigation Unit). As a result, this audit could not be a follow up of the previous audit on risk management ad address issues around overall risk assessment.

(2) This is maturity assessment unlike traditional audit the OIG used to perform. For any maturity assessment, the approach requires to identify components subject to assessment and the maturity rating. In both cases, the OIG always refers to most recognized international guidelines and standards. Kindly refer to similar exercise performed in 2020 Emergency Preparedness."

I hope that is clear to you; it isn't to me. The report clearly stated that "Instead of using the standard audit rating scale, the OIG used the assessment model to rate the maturity of the Global Fund fraud risk management framework and its underlying processes." Why do that? Why not be consistent? And who cares about a 'maturity assessment'? We are concerned about risk not maturity.

Instead, we have a confusing report. It starts and concentrates on the use of the ACFE guide published in 2016 and the rating using the scales shown in Figure 1. Unfortunately, without research and going into detail, the ratings in Figure 1 are meaningless to most readers; hence this article does not refer to those ratings in the above conclusions. Some explanation is available if the reader carefully reads all the content of Figure 4 above (which is Figure 7 in the OIG report). However, the maturity levels in the figure do not appear to be related in any way to the five assessment components on the left. According to OIG, "the report does not limit itself to giving a rating. For each assigned rating, the rationale is given in line with the definition of the selected rating. Therefore, there is no need for the reader to understand what each rating means; the ranking of the rating of the maturity scale together with the rationale provided are sufficient for understanding." So OIG considers that you, the reader, do not need to understand the rating; so why bother to read the report?

The report explains programmatic fraud, which is no less significant than financial fraud; yet the report only explains the processes for financial fraud risk assessment (Figure 6). What are the processes for programmatic fraud risk assessment and how do they differ from financial fraud risk assessment? According to OIG, "The approach for programmatic fraud risk management is not structured and consistent, unlike the one for financial fraud risk, and the reader should refer to the AMA #3 which addresses this concern". That is unsatisfactory considering OIG's own admission that this is one of the main issues of concern.

During 2019-2021, the OIG opened 489 investigations. The report provides information on the types of allegations for which 410 investigations (84% of the total) were opened. The remaining 79 investigations (16%) refer to other categories of wrongdoing (e.g. sexual harassment and abuse) what are not relevant to this audit.

Surprisingly, this report does not include a reference to the Board Decision on Risk Appetite at the 46th Board Meeting held 8-10 November 2021 at which:

1. The Board:
    1. recalled its ultimate responsibility to the Global Fund's stakeholders for overseeing the implementation of effective risk management;
    2. affirmed the Strategy Committee's concurrence with the amended Risk Appetite Statements under such committee's oversight;
    3. further affirmed the Audit and Finance Committee's concurrence with the amended Risk Appetite Statements under such committee's oversight; and
    4. instructed the Secretariat to provide greater reporting on emerging risk trends; and the effectiveness and results of the assurance measures, including the additional assurances put in place.
2. Based upon the recommendation of the Audit and Finance Committee, the Board approved the amended Risk Appetite Statements, including risk appetites, target risk levels and timeframes to achieve risk targets.

The OIG says that there have been references to it in two instances:

"(1). The Secretariat routinely adapts its response mechanisms to the changing operating context. The Secretariat has updated its risk appetite and assurance activities due to the increasing risks occasioned by the COVID-19 pandemic. The risk appetite for Grant-Related Fraud and Fiduciary was increased from "moderate" to "high", with the expectation of returning to "moderate" by end of 2022. The Secretariat proposed various mitigation actions and assurance activities to reach this target. (page 4).

(2). In September 2021, the Secretariat, through its update on Global Fund Risk Appetite, addressed to the Audit and Finance Committee (AFC) on how financial and programmatic issues are considered in risk trade-off decisions and on the link between financial and programmatic performance. While fraud risk appetite is expressly determined as part of financial and fiduciary risks, there is limited consideration of fraud risk regarding programmatic risks. (page 14)"

I still do not see how these refer to the November 2021 Board Decision, especially something that the OIG response to my article says happened in September 2021 before the November Board meeting!

Read More
