

# Thirty-Third Board Meeting

# Risk Management Report

GF/B33/05

Board Information

**PURPOSE:**

1. To provide information that enables the Board to fulfill its responsibilities with respect to risk management.
2. The report is provided by the Chief Risk Officer.

In accordance with the Board's oversight arrangements over Risk Management, the attached report from the CRO to the Board is submitted for information and discussion at the upcoming meeting.

# I. Executive Summary

1. This report on risk management is the second regular report that is provided to the Board by the Chief Risk Officer. It covers a relatively short period of time, of 3 months.
2. Due to the short period of time elapsed since the last report, there are relatively few changes to the overall risk profile and the significant individual risks facing the organization.
3. The Board's attention is drawn to the Office of the Inspector General's first annual opinion since it was established, which provides the Board an understanding of whether, in the judgment of the Office of the Inspector General, internal controls, governance and risk management processes at the Global Fund are adequate and effective to ensure that the organization's operational and strategic objectives will be met. This opinion is contained in the OIG's separate reporting to the Board.
4. During the period covered by this report, a 'risk event' concerning the Secretariat's IT systems occurred, as described in paragraph 14 (a). Fortunately, the impact of this event was able to be contained reasonably well. An independent assessment of the event will be carried out. Also, a previously reported risk around Secretariat culture has been downgraded as explained in paragraph 14 (b). Finally, foreign exchange risk has materially increased, as described in paragraph 14 (c).

## II. Introduction and Background

5. This report on risk management is provided to the Board twice each year. It is arranged according to the four responsibilities that the Board has with respect to oversight over risk management, as outlined in the next four sections. The fifth section presents other matters relevant to risk management. The last section presents a summary of the main outcomes of the discussions of this report in the three Board committees.
6. Due to the relatively short period of time since the previous Board meeting and report, in addition to the new requirement to first submit this report to each of the three Board committees, it only covers a 3-month period (November 2014 through January 2015). As a result, there is less information to be conveyed than usual and the report is relatively brief.

## III. Understanding the Organization's risk philosophy and approving the Framework for Risk Differentiation

7. The Board approved the Global Fund Risk Management Policy at the last Board meeting. At that same meeting, the Board also made decisions to improve its oversight arrangements over risk management. These decisions necessitated an update to the Enterprise Risk Management Framework, which accompanies the Risk Management Policy. Annex 1 contains the relevant text that has been inserted into the ERM Framework to reflect the current oversight arrangements, following the standard model for cross-cutting issues.
8. The Risk Differentiation Framework was also approved at the last Board meeting. It is being implemented by incorporating the various aspects into the risk management processes including in the work-planning of the Secretariat's Risk Committees. The external risk index, which categorizes the countries receiving funding according to their contextual risk levels, will be updated in March 2015 as stipulated in the Risk Differentiation Framework.

## IV. Knowing the extent to which management has established effective risk management

9. The Board relies on representations from management that effective risk management is in place, with independent views on those representations expressed annually by the Chief Risk Officer at the Board's fall meeting, and by the Office of the Inspector General at the spring meeting. Reference is made to the update report from the OIG (GF/B33/06) that, for the first time since the establishment of the OIG, expresses an opinion on organizational maturity from the OIG's perspective.

10. As reported to the Board in both of its meetings in 2014, the main aspect of grant management that needs to be improved further is the manner in which country teams, their managers, and the various risk owners across the Secretariat plan, obtain and evaluate adequate **assurance** with respect to how implementers manage their risks. This is referred to as the 'Risk and Assurance project', the central coordination and support for which was placed with the Risk Management Department following the conclusion of the first phase of the project at the end of 2014. Additional resources, including a Risk and Assurance Senior Manager / Deputy CRO, are being recruited into the department for this purpose. Pending this recruitment, a temporary individual has been retained. Planning for seven country pilots, where the new approaches will be validated, is underway. The Global Fund Risk and Assurance Committee, co-chaired by the Executive Director and the CRO, is overseeing the project.

11. As reported in the previous Risk Report to the Board, in order to satisfy itself that all important risks are appropriately identified, analyzed and mitigated in new grants created under the New Funding Model, the Risk Management Department is currently reviewing a sample of such grants. The results of that review will be reported in quarter 2 of 2015.

12. The Risk Management Department is currently in the process of planning to undertake between 12 and 16 in-country visits in 2015 in order to observe first-hand whether the assertions as to the identification, analysis and mitigation of operational risks in grants by the country teams and their managers are accurate and reliable. This work will, among other things, contribute towards the CRO's assurance statement to be issued to the next Board meeting.

## V. Reviewing the portfolio of risk and considering it against the approved risk thresholds

13. The Board reviewed the portfolio of risk at its November 2014 meeting, as documented in the organizational risk register and as measured by the Corporate KPI on Operational Risk Management ('ORM') that measures the level of risk in the grant portfolio. Since November, no significant shifts in the overall risk exposure of the organization have come to the attention of the Risk Management Department. At the next Board meeting, a full update, including the Q3 2015 risk register and Corporate KPI on ORM, will be provided.

## VI. Being informed about the most significant risks and whether management is responding appropriately

14. The organizational risk register shared with the Board at its November 2014 meeting contained 20 risks. The quarterly update of the register is currently in progress. However, the following developments can already be reported now:

- a) “Interruption of activities due to loss of data and dis-functioning operational and back-up systems in IT”. This was risk #16 on the risk register shared with the Board in November 2014, then rated as ‘Medium’. On December 12 2014, hard drive failures in the Secretariat’s IT systems caused very severe disruptions to access to data and systems that affected a number of Secretariat staff. During the completion of the recovery by Global Fund IT staff and the storage vendor, additional issues were encountered with the storage device that impacted more widely the Global Fund IT services. In the period from 19 December to 5 January 2015 the IT services hosted on the problematic storage device were recovered and transferred to alternative sites following the business impact assessment protocol that had been established in 2014. These were periodically released as services made available to users so that by the commencement of the working year on 5 January 2015, most services and all critical services were available. The one remaining item unrecovered was a large SharePoint 2007 database housing approximately 1.6 million documents. Multiple attempts to restore this data were carried out, including by specialized data recovery experts. During this period, there was significant uncertainty about whether some data might be lost forever. Fortunately, on 17 January 2015, the most serious issues were resolved within that database and all data was able to be recovered. The OIG in April 2014 had observed that while IT processes were generally adequate and back-up systems were in place, “no formal business continuity plan that includes a recovery site has been put in place. Based on the contractual arrangements with third party providers, it is estimated that it would take between two to ten days to restore system and data access once a recovery site is identified and activated.” IT agreed to put in place a “fully integrated business continuity and disaster recovery plan that includes a recovery site” by 1 October 2014. IT was aware that primary back-ups for this database were frequently failing (and causing others to fail) up to the end of 2013, and had put in place alternative back-up solutions. Through this unfortunate incident, these back-ups proved to be ineffective. The Chief Financial Officer is overseeing an independent assessment of this risk event to ascertain how it could have occurred and draw lessons for the future.
- b) “Management fails to deliver new Global Fund culture including embedding values and improved managerial accountability, as well as driving high performance”. This risk was rated as ‘High’ as of last November, and several initiatives were taken over the past two years to improve the culture. Two factors have now led management to downgrade this risk to ‘Medium’: the first is that we reached our target level for the key performance indicator ‘quality of management’ as per a recent survey among staff on this topic. The second is continued encouraging reporting from the Ombudsman when compared to recent years.
- c) Foreign exchange risk. As outlined at several meetings of the board and FOPC, the Global Fund is exposed to foreign exchange risk, as a result of a mismatch in the currency mix of uses and sources of funds. This risk was not on the organizational risk register as of September 30, 2014 because, in the judgment of management, at that time it had not risen to a high enough level. However, significant exchange rate movements during 2014 have led to realized exchange losses. In addition, there could be important future impacts on the ultimate value of contributions and pledges not yet received. Management has put in place reasonable risk mitigation measures, but the implementation of some of these is dependent on the establishment of relationships with commercial banks, which has been delayed by changes in the international financial regulatory environment.

## VII. Other matters

15. In January 2015, the third of a series of regional risk management workshops was held in the Eastern Europe and Central Asia (‘EECA’) region. In attendance were Board, Board Constituency and Board Committee members; representatives from civil society and government implementers; CCM

members; Local Fund agents; and OIG and Secretariat staff. Two earlier workshops were held in Bangkok and Cape Town. These workshops are made possible through funding by the Swiss Development Corporation, the German Back-up Initiative, and the OIG. Much of the rich discussions centered around key issues for implementers in the EECA region, including transition and sustainability, as well as the participants' experiences in mitigating these and other risks.

16. Key priorities for the Risk Management Department in 2015 include:

- a) the Risk and Assurance work described in more detail in paragraph 10;
- b) maintaining the operational risk management process;
- c) continued work on helping the Secretariat strengthen its internal controls;
- d) providing support to the Ethics initiative;
- e) continued support to the work to recover misused funds;
- f) facilitate the strengthening of **implementers' and CCM** risk management processes and practices. The workshops described in the preceding paragraph, as well as the risk management platform for risk management practitioners in global health that we established in late 2014 as reported to the last Board meeting, are among the activities that should help us reach a number of concrete goals by the end of 2015. Specifically, we aim to have collated a quality-assured set of risk management tools and best practices, and have begun to systematically make this 'toolbox' (similar to the already-existing PSM toolbox supported by the World Health Organization) widely available to actors in global health;
- g) prepare for the issuance to the Board, in its first meeting in 2016, of the first annual assurance report on the effectiveness of risk management.

## VIII. Discussion of this report at the three Board Committees

17. In February and March 2015, this report was discussed in the Strategy, Investment and Impact Committee, the Audit and Ethics Committee and the Finance and Operational Performance Committee. The main discussion points and outcomes were as follows:

- a) More attention to strategic risks is needed in the report – the Chief Risk Officer will work with members of the Strategy, Investment and Impact Committee in order to define the scope and depth of reporting that will provide the Board with the necessary information;
- b) In order to help each Committee focus on the risks that are within its particular mandate, and avoid overlapping discussions as much as possible, the information in future reporting will be segmented accordingly. Based on comments from the Finance and Operational Performance Committee and discussions with the Chair and Vice-Chair, the CRO will work with the committee to ensure the risks within their mandate are provided to support the FOPC's oversight;
- c) The Committees also discussed developments outlined in paragraph 14 above (changes in three specific organizational risks since last November); the update on the Risk and Assurance project; and the timing of the issuance of the first assurance report from the Chief Risk Officer.

This document is part of an internal deliberative process of the Global Fund and as such cannot be made public until after the Board meeting

## Text inserted into the Enterprise Risk Management Framework to reflect Board oversight arrangements over Risk management

The following text has been inserted, after paragraph 15, into the Enterprise Risk Management Framework, the explanatory document that accompanies the Global Fund Risk Management Policy, following the decisions taken by the Board at its November 2014 meeting to strengthen oversight arrangements over risk management. This text replaces the 'placeholder' in the document as provided to the Board last November:

- “16. The Board’s oversight arrangements concerning risk management are as follows:
- a) the standard Board governance model for crosscutting issues is applied (see figure 2 below) which means that all committees are involved in and contribute towards the management of risk and each has a full picture of the risk universe;
  - b) The CRO is responsible for the consolidation and presentation of risk report to the Board; such report includes an annual assurance statement, providing the CRO’s independent view on the robustness and effectiveness of the Secretariat’s risk management and mitigation steps taken and whether the risk profile is acceptable, is improving or deteriorating;
  - c) The CRO reports to the Executive Director (ED) while committee leadership provides input into the annual performance appraisal of the CRO. It is expected that the CRO will flag any material matters where the ED and CRO have a fundamental difference of opinion;
  - d) A training in risk management is actively offered as part of the induction provided to Board and committee members. Efforts are made to ensure that risk experts are recruited in the committee nomination and selection processes.”

**Figure 2:** Board standard model for cross-cutting issues applied to risk management:

Board	<ul style="list-style-type: none"> <li>▪ Risk Management is a standing agenda item at Board Meetings based on a report by the CRO</li> <li>▪ Review portfolio of risk and measure against risk appetite</li> <li>▪ Approve risk policies and frameworks and ensure that the Global Fund has the correct risk framework and practices in place</li> </ul>
Board Chair/Board Vice-Chair	<ul style="list-style-type: none"> <li>▪ Overall responsibility for ensuring that risk responsibilities are conducted effectively at the Board, and Committee level.</li> </ul>
Coordinating Group	<ul style="list-style-type: none"> <li>▪ Ensure that risk is being effectively addressed in each of the committees</li> <li>▪ Ensure coordination across the committees as needed</li> </ul>
3 Board Committees	<ul style="list-style-type: none"> <li>▪ Risk is a standing item on each committee meeting agenda (2x year)</li> <li>▪ Consider the overall risk from the respective lens of each committee</li> <li>▪ Identify any issues or concerns for Board consideration</li> <li>▪ Review risk policies and frameworks from the respective lens of each committee (but do not approve)</li> </ul>
Chief Risk Officer	<ul style="list-style-type: none"> <li>▪ Bi-annual report to the Committees on overall risk environment. (One consolidated report)</li> <li>▪ Annual Assurance Report to the Board on the effectiveness of risk management and mitigations</li> <li>▪ Create and manage a Comprehensive Risk Management Framework</li> <li>▪ Conduct regular in-country verification of risk assessments (min 6/year)</li> </ul>