FOR AGENDA

SM/13/195

July 9, 2013

To: Members of the Executive Board

From: The Secretary

Subject: **2013 Report on Risk Management**

Attached for consideration by the Executive Directors is the 2013 report on risk management, prepared by the Advisory Committee on Risk Management (ACRM), which is tentatively scheduled for discussion on **Friday, July 26, 2013**. Issues for discussion appear on page 29.

The staff does not propose the publication of this paper given its confidentiality and because it relates to the internal operations of the Fund.

Broad questions may be referred to Mr. Nelson (ext. 38132) and Mr. Meyers (ext. 35912) in OIA. Specific questions may be referred to Mr. Fisher, FIN (ext. 38755) and Mr. Muhleisen, SPR (ext. 38686) on Europe-related and governance and legitimacy risks; Mr. Hinderdael, TGS (ext. 38546) on IT security risks; and Ms. Stotsky, OBP (ext. 38541) and Mr. Alhusseini, HRD (ext. 37085) on human resources and budget risks.

This document will shortly be posted on the extranet, a secure website for Executive Directors and member country authorities.

Att: (1)

Other Distribution:
Department Heads

2013 REPORT ON RISK MANAGEMENT

July 9, 2013

EXECUTIVE SUMMARY

The Fund's risk management framework provides a systematic approach to identifying, assessing, and addressing key risks. In this context, this report provides an overview of risks faced, mitigation actions taken and planned, and prospects for FY 2014 and the period ahead, as assessed by the Advisory Committee on Risk Management.

Incidents as monitored and reported by Fund departments, along with communications to the Fund's Integrity Hotline, provide an indication of risk outcomes across a range of Fund operations. An increase in serious incidents, observed during April-September 2012, largely in the areas of staff security and business disruption, was followed by a return to the long-term average of two per month during October 2012–April 2013. Reports to the Integrity Hotline fell to 267 in 2012, from 285 in the preceding year, with most communications received relating to e-mail scams.

In reporting on risks faced by the Fund, on aggregate, departments and offices observed in a survey that strategic risks had moderated slightly, and core and noncore operational risks were viewed as having increased. Within the range of views reported, several departments signaled increasing concerns about strategic risks faced by the Fund, with the latter centering on governance-, credibility-, and finance-related issues. Risks related to Fund–supported programs, particularly in Europe, and tail-risks and focus in surveillance were highlighted in comments on core operational risks. Noncore operational risks were noted in the areas of staff morale, information technology (IT) security and reliability, the HQ1 Renewal Project, the employment framework, and ethics.

Risks to Fund-supported programs were concentrated in Europe, as were risks to global growth. Within the comprehensive set of measures to mitigate credit risk, the primary tool is the strength of Fund policies on program design and conditionality, as well as access. Available indicators suggest that near-term tails risks have moderated. Although a number of positive, program-related developments have also helped to mitigate the risk profile of the Fund's exposure, sizable-related risks remain.

A further intensification of crisis would add to the Fund's credit and liquidity risks. In light of this, the Fund's capacity to respond to the needs of all of its members has been substantially enhanced. Together, in 2012, the Fund's quota and NAB-based financing and temporary bilateral borrowing agreements brought the Fund's total potential lending capacity to over US$ 1 trillion. Remaining liquidity risks associated with lending operations would be partly mitigated by modalities agreed upon in the 2012 bilateral borrowings.

The Fund's failure to identify and address more clearly the seeds of financial crises in recent years has led to a stronger focus on risks in the Fund's surveillance and program work, including the Early Warning and Vulnerability Exercises. A number of global long-term trends, outside of the Fund's typical areas of concern, could define the next few decades. A process has been initiated for assessing the potential implications of these issues for the Fund's strategic focus, governance, and possible operations.

Improving IT security controls remains a top priority, while action has been taken to remediate reliability and performance issues. In response to an assessment prepared in 2012, a plan was established, and will be implemented in the coming months, to improve the Fund's information security posture, and prioritize high risks, taking the Fund's ability to absorb change and IT implementation capacity into account. Regarding reliability and performance, TGS accelerated the deployment of new computers, and steps have been taken to strengthen the quality assurance of all standard applications.

A framework has been put in place to address HQ1 Renewal Program risks, including steps to minimize the impact of construction on staff work, and the establishment of an Operational Health and Safety Management Plan, which responds to safety requirements under the program.

To address staff morale issues, a range of steps have been taken, including the introduction, in FY 2012, of the accountability framework for departments, expansion of the external mobility program, and internal mobility initiatives. Looking ahead, as noted in the corporate workforce planning paper that was presented to the Board in February 2013, increased training opportunities, greater research assistant support, and encouragement of job enrichment through increasing responsibilities will be targeted. The recently concluded 2013 staff survey will inform further steps to improve the working environment.

Approved By
Advisory Committee on Risk Management

Prepared by the Secretariat to the Advisory Committee on Risk Management

CONTENTS

INTRODUCTION

1. **As detailed in this report, in carrying out its mandate the Fund faces a wide range of risks of varying potential impact and likelihood.** The Fund's risk management framework, as described in Appendix I, provides a systematic approach to identifying, assessing, and addressing important risks. This report, in the context of the current risk management framework, presents an overview of developments over the past year, regarding the risks faced, mitigation actions taken and planned, strengthening of the risk management framework, and prospects for 2013-14 and the period ahead. The overview presented reflects the assessment of the Advisory Committee on Risk Management (ACRM).

2. **The previous annual report (SM/12/199) was discussed by the Executive Board on August 1, 2012 (BUFF/12/94)**. Directors broadly concurred with the ACRM's assessments of the main risks and the proposed mitigation measures. With regard to strategic risks, Directors emphasized the importance of making the 2010 governance and quota reforms effective by the 2012 Annual Meetings and complete the quota formula review by January 2013. Directors acknowledged that the risks related to lending to Euro-area members were more concentrated and correlated, raising the prospects of adverse regional and global spillovers. This led to an increase in credit, reputational and operational risks during 2011-12. But a number of Directors also considered that the report had overstated these risks in view of the risks that would have emerged in the absence of Fund financial support in Europe. Directors also considered that credit risks had been mitigated by the higher target for precautionary balances and by pledges of new bilateral resources. Focus was placed on the importance of an implementation of an IT strategy that mitigates IT risks, including security breaches. They also took note of HR-related and budget constraint risks and encouraged better work prioritization, streamlined surveillance products, and greater flexibility in resource allocation within departments. Directors looked forward to the proposals from the Working Group on the Fund's Risk Management Framework (WGRM) that was established by the Managing Director in March 2012. Some Directors called for an enhancement of the Board's engagement in risk management. Directors suggested that future reports could provide more integrated risk assessment with greater emphasis on mitigation strategies and reviews of past implementation measures.

3. **The WGRM was established to (i) make concrete proposals to address key recommendations of the external panel, and (ii) examine the potential role of quantitative analysis in the Fund's management of financial risks.**[1] In fulfilling its mandate, and in line with the guidance provided at the August 1, 2012 Board discussion, the WGRM contracted the services of experts with extensive experience in risk management in the private sector, and consulted widely with central banks, international organizations, and private sector institutions. Based on this review, the WGRM reported to the Managing Director, earlier this year, on options for strengthening the

[1] The high-level external panel comprised Guillermo Ortiz (chair), Jacob Frenkel, Malcolm Knight, and Thomas O'Neill.

Fund's risk management framework, including by bringing greater coherence to risk analysis and mitigation, and by broadening the applications of risk management tools and techniques that are well-adapted to the Fund's unique role and mandate. Once management has reached a conclusion on this matter the Board will have an opportunity to provide input.

4. **In the interim, the ACRM has continued to follow with interest the risk management developments in other major international and supranational financial institutions.** The periodic benchmarking by international financial institutions (IFIs) revealed that nearly all IFIs had developed—consistent with Basel principles—three lines of defense: (i) controls embedded in business units; (ii) a risk management function that is separated from the business units; and (iii) internal audit to provide objective assessments of both. For example, the European Court of Auditors has posted on its website its report on risk management by the European Central Bank (ECB).[2]

5. **This report is organized as follows**. The second section presents the main conclusions drawn from an analysis of incident reports. The third section presents the main results of the 2013 Departmental Risk Survey. This risk survey allowed the ACRM to identify the six principal risks identified as facing the Fund and to ask for further drill down by relevant departments.[3] The six identified risks are related to: (i) the financial risks associated with Fund–supported programs, with particular emphasis on Europe and the Middle East; (ii) governance and legitimacy; (iii) IT security and reliability risks; (iv) risks arising from human resource and budget constraints; (v) risks associated with the HQ1 renewal project; and (vi) risks associated with the current approach to addressing the longer term planning horizon. The fourth section provides a fuller discussion of each of these risks. The final section presents some issues for discussion. Appendix II provides an extended discussion of the survey results.

INCIDENT REPORTING IN FY 2013[4]

6. **The risk framework employed by the Fund follows a three-dimensional model that assesses strategic, core and noncore operational, and financial risks (Box 1).** The incidence of events corresponding to high-impact strategic and core operational risks faced by the Fund is limited, while the incidence of events related to noncore operations can be regularly monitored. In this regard, the Fund's incident reporting framework provides a snapshot of problems; sensitizes

[2] *Report on the Audit of Risk Management of the European Central Bank for the Financial Year 2010* http://eca.europa.eu/portal/page/portal/publications/auditreportsandopinions/specificannualreports

[3] Principal risks correspond to areas reported by at least one department as having the highest level of impact (serious), and almost certain or likely likelihood. Each principal risk was identified by multiple departments as having elevated impact and likelihood.

[4] Prior to the most recent six-month period, the incident reporting cycle was one month ahead of the financial cycle. Beginning with the most recent cycle, the periodicity shifted to coincide with the Fund's financial year. In light of this, coverage for FY 2013 corresponds to data for the 13 months covering April 2012 – April 2013.

staff to the importance of a rapid and tailored response according to the severity of an incident; de-stigmatizes the reporting of incidents; and helps to break down institutional silos and facilitate preventive actions. The operation of the framework hinges on comprehensive reporting by departments and offices and through the Integrity Hotline, which, in turn, depends on the ease of use of the reporting mechanism and the perceived institutional utility of the information provided. Reflecting this, as described in Box 2, the incident reporting survey allows departments and offices to establish practices for incident collection and classification that reflect their varying operational needs and styles.

Box 1. Summary of the Coverage of the Fund's Current Risk Management Framework

The risk management framework that the Fund has been using since 2006 is based on a widely-recognized framework that is used by organizations around the world.[1]

The Fund's risk management framework identifies three main categories: strategic, operational, and financial risks. A fourth risk, core mission, is considered an element of the three main risk categories. The three main risk categories covered are as follows:

- **Strategic**: the risk that medium- and long-term objectives and strategies will not meet the Fund's evolving needs;
- **Operational**: the risk that *core objectives,* including economic and financial stability in member countries, international macroeconomic cooperation, contributing to development initiatives in low-income members, and capacity building services, will not be realized; along with *noncore risks* arising from exposure of the Fund to direct or indirect losses resulting from failures in business processes, people, systems, and/or external events; and
- **Financial**: the risk of direct or indirect losses or other negative effects on the Fund's financial position.

A detailed description of the current risk management framework is presented in Appendix I.

[1] The reference framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)—a joint initiative of the Institute of Internal Auditors and four other professional associations. Background on the Fund's implementation of this framework can be found in the *Second Report of the Task Force on Risk Management—Task Force Proposals on the Implementation of a Risk Management Framework for the Fund* (EBS/06/74, 06/26/06).

Box 2. Incident Reporting: Methodology and Departmental Practice

- The cataloguing and subsequent analysis of incidents allow for an understanding of the probabilities associated with different kinds of risk incidents, a dissection of the factors that have been the source of such incidents, and the implementation of procedures to reduce the likelihood of future incidents. It enhances the risk management culture, and supports the sharing of experiences across the organization. At the same time, the benefit of a formalized incident reporting needs to be weighed against the costs. The low-cost approach that has been adopted, as described below, has provided a desirable level of flexibility.

- The ACRM has provided a tentative definition of an "incident" and three associated degrees of severity (serious, less serious, and near misses). The difference between serious and less serious incidents is a matter of degree. Departments are expected to report serious incidents to management and/or the Board, while less serious incidents are expected to be dealt with on a departmental basis (e.g., involving B-level staff at the division or front-office level). Near misses are events characterized by pre-emptive action that averted what would, or could, otherwise have been a serious or less serious incident.

- To obtain a comprehensive view of incidents, including for overseas offices, area departments are asked to report on relevant occurrences in offices of resident representative offices and Regional Technical Assistance Centers (RTACs), and the Institute for Capacity Development is asked to report incidents of the overseas training centers. Reporting guidelines encourage departments and offices to focus on major operational risks, including their involvement in remediation, if any.

- Departmental practices for incident collection and classification vary. For the most recent reporting cycle, incident collection practices were comparable to those observed during the previous periods. Several departments maintain regular incident logs, either web-based or on Excel spreadsheets, while others maintain alternate monitoring practices.

7. **During April 2012-13, serious incidents averaged 2.4 per month, compared to an average of less than two per month observed during the 12-month period that ended in March 2012.** Underlying this was a significant increase in reported incidents for April-September 2012 (to an average of 2.8 per month) that was followed by a return to the observed longer-term average (2.0 per month) during October 2012–April 2013. Regarding the increase observed during April-September 2012, staff security incidents were the main reason, with two fatalities (a long-term expert and a pedestrian hit by a driver employed by a locally-hired resident representative) and mission cancellations and the evacuation of Resident Representative offices dues to civil unrest and armed attacks in Africa and the Middle East. Business disruptions arose from false fire alarms and IT failures and connectivity issues that mostly impacted one office. During October 2012-April 2013, incidents related to the physical security of staff, which led to mission cancellation, incidents related to physical security of staff and business disruption, accounted for four-fifths of items reported. The rate for less serious incidents, which had been averaging between 22 and 30 per month during previous report periods, decreased to 12 per month in the most recent 13-month period. This change was driven almost entirely by a decrease in reported incidents by TGS, owing to tighter reporting criteria and to some extent by the completion of the HQ1 fifth floor

terrace renovation project. Incidents reported by FIN involved business disruption, financial or data reporting.

8. **A different form of incident reporting occurs through the IMF's Integrity Hotline**. The Integrity Hotline, established in 2008, provides a fast and discreet mechanism for staff to report (via an independent company) possible allegations of misconduct. The number of reports received in 2012 (267) was slightly below those received in 2011 (285). Categories of reports included the following: requests for information (57), email scams (162), substantive allegations (18), and other miscellaneous reports (30). Substantive allegations covered a range of misconducts, including harassment, personal conflicts of interest, household obligations, and misuse of Fund resources.

THE 2013 DEPARTMENTAL RISK SURVEY

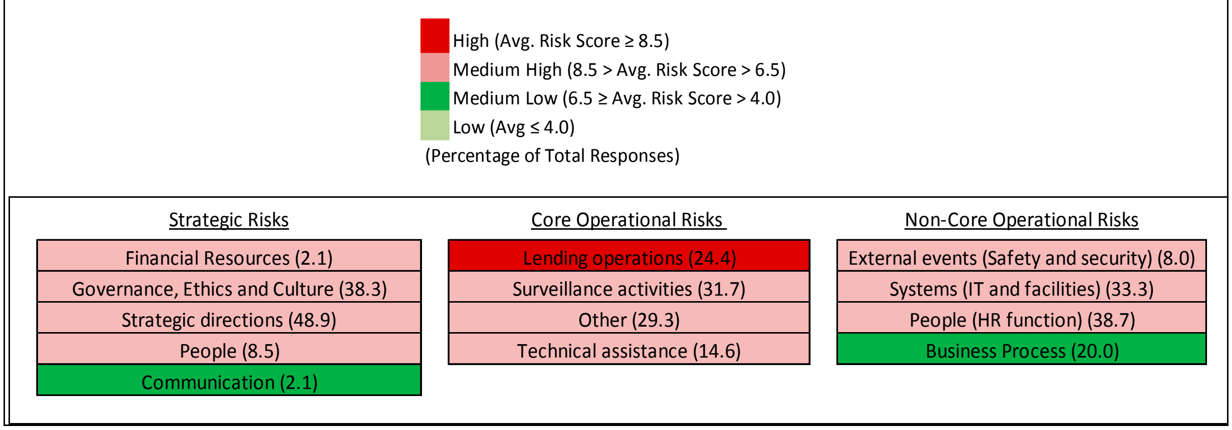
9. **Following the practice resumed in 2012, the ACRM conducted a streamlined departmental risk survey in early 2013**. Departments and offices were asked to identify the three most important risks facing the Fund using the risk categories described in Box 1. The survey questions were presented in an open-ended manner, with a principal focus on the most important risks. As in 2012, financial risks were excluded from this survey for two reasons: (i) the ACRM's terms of reference specifies that FIN provides the assessment of financial risks; and (ii) to maintain consistency with previous departmental surveys, which also excluded financial risks for the reason already given.[5] Each self-identified risk was assigned both a rating for the degree of impact of severity and a rating for the likelihood of occurrence, using a four-point rating scale, and taking account of any mitigating actions that had been implemented. Based on this, a four-by-four matrix was produced, setting out each of the severity-likelihood combinations, as well as an ordinal ranking for each identified risk, calculated as the product of its severity and likelihood ratings, which ranged from 1 to 16. Information was also sought on any steps already taken, or planned, to address the various risks as well as any proposed or necessary mitigation measures—both at the departmental or Fund-wide level—and, to the extent possible, on changes perceived on the residual risks (that is after mitigating measures) relative to previous years.

10. **The survey responses from 21 departments and offices identified 163 individual risks.** (Appendix II, Table 1) Given the open-ended format, some responses, while not identical, clearly overlapped. The results indicate that the range, severity, and likelihood of risks facing the Fund are broadly similar to those reported last year. Perceived strategic risks have moderated slightly, while core operational risks are seen as having increased somewhat. Several area departments however, signaled increasing concerns regarding strategic risks, while also viewing noncore operational risks as having risen.

[5] As defined in Box 1, the survey excludes risks as they relate to the Fund's financial position. However, program-associated risks, including governance, institutional effectiveness, and reputation, while closely correlated with financial exposure, were included in the survey.

11. **As regards their distribution, strategic risks slightly exceeded core operational risks** (47 relative to 41); as in 2012, noncore operational risks were more prevalent, totaling 75 entries. In terms of risk intensity—the product of both severity of impact and likelihood (Figure 1), only lending operations achieves a high-risk intensity score of over 8.5, in contrast to 2012 where governance was also rated as having high intensity.[6] As noted, these risks relate to the various ways in which the Fund's involvement with lending to Europe could adversely affect the Fund's strategic, core, financial and reputational interests. Next in risk intensity are the strategic risks associated with delays in Fund governance reform (7.7); weaknesses in the Fund's capacity to think about medium- to long-run challenges facing the global economy and in proactively assessing short-run vulnerabilities (7.65); systems vulnerability, which includes both the potential for IT security breaches as well as for unreliable IT systems to constrain operations and/or compromise integrity as well as delays and cost overruns associated with the renovation of HQ1 (7.3); and the human resource challenges and budget constraints (6.9) that could jeopardize the Fund's ability to carry out its responsibilities. Two other risks were also mentioned by at least one respondent as having serious or medium-high risk intensity: (i) personal security risks (7.8) and (ii) the adverse effects associated with external financing of TA (7.5). Finally, some expressed concern about key-person risks associated with a sudden, unanticipated change to the Fund's management team.[7]

Figure 1. 2013 Risk Intensity Map
(Risk intensity is the product of the scores for impact and likelihood)



12. **Decomposing these risk intensity measures according to perceptions of severity and likelihood** (Figure 2), **the viability of the Fund's role in lending was seen as most severe in terms of its potential impact** (3.5**) and greater likelihood** (2.5). While governance risks are seen on average as of similar potential severity of impact (3.4), their likelihood of occurrence are seen as

[6] For each risk, the intensity rating is calculated as the average of the risk intensities reported by departments.

[7] Of the listed areas, those identified as "principal risks", as set out in paragraph 5, are detailed in the following section of this report. In addition to the mitigation steps detailed in this report, the risk survey results are used as inputs in the development of the Office of Internal Audit (OIA) and Inspection's annual audit plan. In this regard, personal security risks were addressed in the Review of Field Security that was recently issued by OIA.

Figure 2. Perceptions of Severity of Impact and Likelihood

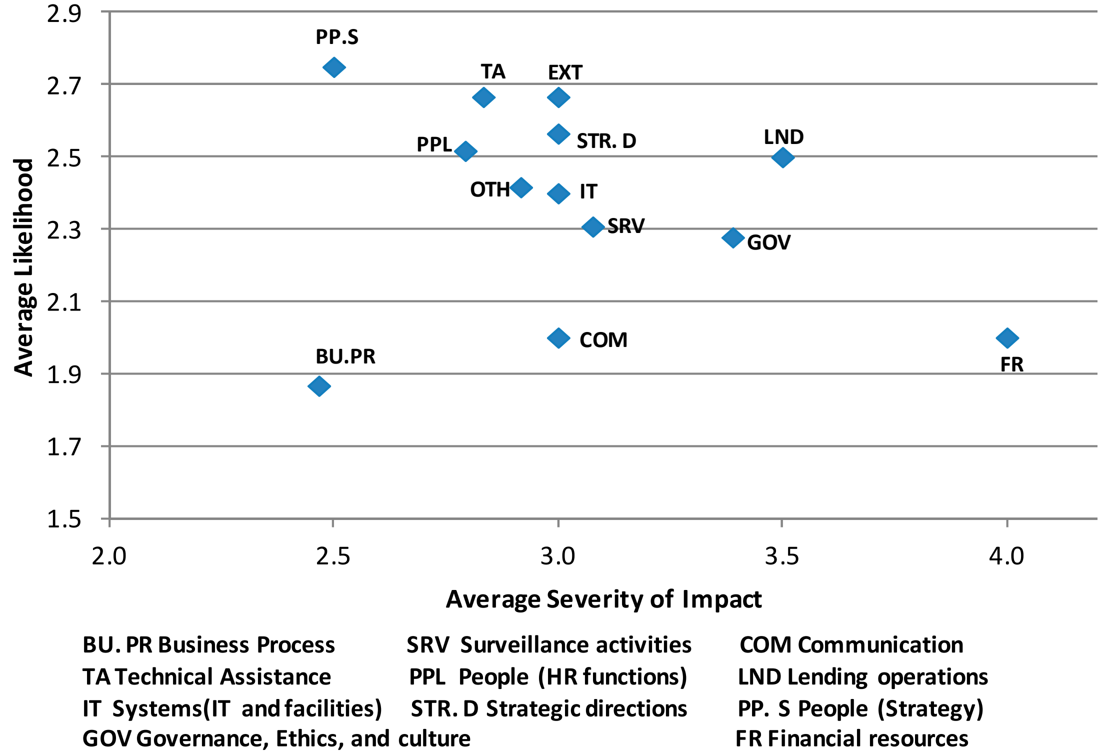
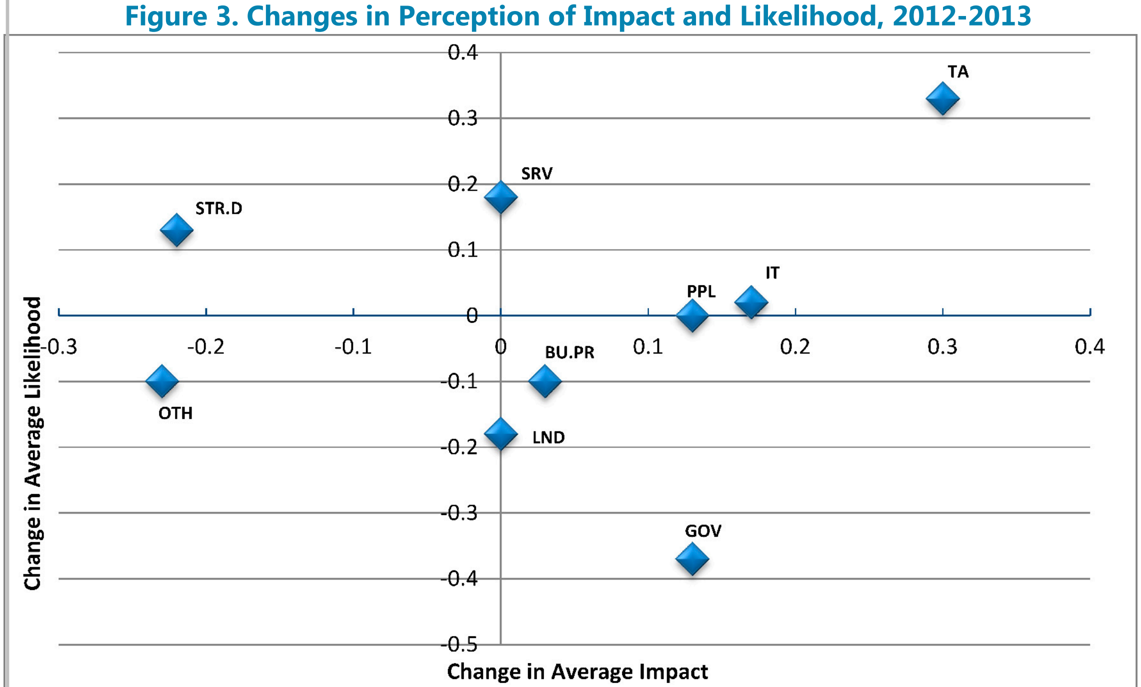


Figure 3. Changes in Perception of Impact and Likelihood, 2012-2013



Note: Since COM, EXT, FR, and PP.S were not ranked categories in the 2012 survey, related changes are not presented in this figure. A summary description of associated risks is set out in Appendix II, Section E.

marginally lower (2.3). The precedence accorded to these two risks largely mirrors the perceptions found in the 2012 survey. Other risks that are also perceived as of comparable likelihood—strategic directions, surveillance, IT and external events, are seen as discretely lower in terms of the severity of their potential impact.

13. **While current risk perceptions are broadly similar to those reported in 2012, potential impacts have increased in a number of categories, while the average likelihood increase in a number of cases** (3) , **and declined in** (4) **others** (Figure 3.) Perceived potential impact fell only in the areas of strategic directions and other core operational risks, and only in the latter category were both impact and likelihood seen as having fallen. Taken together with the addition of two previously noted relatively high potential impact risk areas, financial resources and communications (which are not shown in the figure), the rise in the perceived risk intensity for technical assistance financing and increases in potential impact, in particular, for information technology and human resource functions, and the increased likelihood of surveillance risks provide an indication that the risk environment has, if anything, become more challenging.

14. **Departments also provided more detailed characterizations of their perceived key risks**. [8] A composite of these views is summarized as follows:

Strategic Risks

- The perception that the Fund is overly focused on Europe was seen to be associated with risks that the Funds traction would be reduced in other regions, and that its reputation could be harmed. Delays in the implementation of the 2010 quota and voice reforms further contribute to the severity of these risks. Relative to 2012, one can observe a perception of a higher severity of impact from the latter risk.

- Departments expressed concern that the failure of a Fund-supported program or the perception of weakened or ill-conceived policies could lead to losses in credibility, effectiveness, legitimacy, and reputation. Further, if programs failed, this could jeopardize the Fund's finances. There is also the potential of inadequate access of larger LICs to Fund resources in the event of severe adverse shocks.

- Two departments noted the risk of inadequate financing of the Fund in the event of another crisis. Other departments expressed concern about an inadequate workforce and employment strategy.

[8] The perceived risks summarized in this section reflect survey responses provided by departments early in 2013. Changes in the risk environment and/or steps that have been taken to mitigate the noted risks are reflected in the section on Key Risks and Mitigation Strategies.

Core Operational Risks

- Fund-supported programs could fail. Moreover, difficulties in coordination with partnering institutions could lead the Fund to lose clout in its policy advice. Some departments were particularly concerned that Middle East programs would fail to stabilize economies and restore growth, a risk seen as both severe in impact and highly likely. Similarly medium-high risks (though unlikely) were associated with some high-profile Asia programs due to political factors. Concerns were expressed about the impact of the crisis on euro periphery countries.

- Surveillance could miss critical risks (both tail risks and insufficient focus on long-term issues). Other risks included lack of policy traction in surplus countries; the potential for the crisis to spread to Japan; the Fund not enunciating a strategy to promote jobs and growth; and mixed Fund messages on key multi-surveillance policy issues. Human resource constraints could challenge the quality of output and constrain the Fund's capacity for identifying future crises.

- Inadequate internal and external financing of technical assistance as well as limits on staffing were seen as key risks.

Noncore Operational Risks

- Deteriorating staff morale arising from pay constraints, limited promotion prospects, and excessive work pressures were highlighted. These factors may also impact on staffing, turnover, and the Fund's capacity to retain a skilled, knowledgeable, and diverse work force.

- There is a possibility of repeated IT breaches and the unreliability of IT systems resulting in both reputational and operational risks.

- Despite strengthened security policy, personal security risks arising from political instability or terrorist attacks are still of concern.

- HQ1 renewal project-related risks, including negative reactions to cost, potential delays, disruptions to the Annual Meetings, adverse effects on staff productivity and unanticipated issues (e.g., budget, security, and safety) were highlighted. These may expose the Fund to severe criticism and disrupt operations.

- There was concern about the potential for an ethics scandal (with a severe impact, though most see it as unlikely in occurrence).

- An outdated employment framework could result in the Fund losing trained staff and failing to deliver on its core work.

KEY RISKS AND MITIGATION STRATEGIES

Strategic and Core Operational Risks

A. Key Risks of Fund Programs and Mitigation Strategies[9]

15. **Risks related to Fund-supported programs continued to be heavily concentrated in Europe in 2012, as were risks to global growth**. As of end-May 2013, total credit outstanding and total commitments stayed at high levels by historical standards. Credit outstanding amounted to SDR 87.6 billion and undrawn GRA commitments reached SDR 105.3 billion (which compares with credit outstanding of SDR 92.6 billion and undrawn commitments of SDR 121.4 billion one year earlier). This credit exposure was highly concentrated, with commitments under current programs with European members accounting for 63 percent of current Fund arrangements and 79 percent of total GRA credit outstanding (compared with 56 percent and 68 percent, respectively, at end-December 2011). These levels of concentration in Europe were higher than the share of outstanding credit to Asia during the Asian crisis and Latin America during its debt crisis.

16. **As discussed in previous risk management reports, the Fund has in place a comprehensive set of measures designed to mitigate credit risk.** The primary tool is the strength of Fund policies on program design and conditionality, as well as access, which are critical to ensuring that Fund financial support helps members resolve their balance of payments difficulties in a timely manner.[10] These policies include assessments of members' capacity to implement adjustment policies and repay the Fund, and the exceptional access framework for larger access to the Fund's resources in terms of a member's quota. The framework also includes the structure of charges and maturities, safeguards assessments, financing assurances policy to ensure that Fund-supported programs are fully financed, the burden-sharing mechanism, precautionary balances, and the Fund's de-facto preferred creditor status. The Fund also sought to apply lessons learned from its involvement in the Asian and Latin American crises, including the need for more flexible financing, sufficient policy accommodation where possible, and streamlined conditionality to secure greater ownership.

Euro Area Risks

17. **A few large programs with Euro-area members, in particular, continue to present elevated operational, credit, and reputational risks.** These include reform fatigue and political ownership of fiscal adjustment and structural reform programs, employment and inflation dynamics, divergence in competitiveness, and risks of unsustainable debt dynamics. These risks would also be heightened by a protracted period of slower growth in the Euro-area.

---

[9] This section was prepared by FIN and SPR.

[10] As detailed in past reports (Box 3, page 14, SM/12/199, 7/20/2012), the Executive Board is closely involved in the monitoring and management of the Fund's exposure to financial risks.

18. **Nevertheless, available indicators suggest that near-term risks of a tail event have moderated**. This reflects, in large part, the political resolve within the Euro area to protect the currency union, as well as specific policy actions, notably: (i) the implementation of the European Stability Mechanism; (ii) the ECB's decision to introduce Outright Monetary Transactions (OMT); and (iii) the agreement on the Single Supervisory Mechanism—which Fund staff has consistently supported. Nonetheless, risks are likely to remain elevated for a prolonged period reflecting the likely pace at which the banking and fiscal union can be deepened and internal imbalances reduced.

19. **A number of positive developments regarding the programs in the Euro area have also helped to mitigate the risk profile of Fund exposure**:

- In **Greece,** private holders of Greek bonds volunteered to a significant debt restructuring, and European partners lowered interest rates on the Greek Loan Facility, lengthened maturities on all their lending, and transferred profits earned by the ECB on Greek debt back to Greece. Moreover, the new EFF program included a number of safeguards, including a contingent commitment from European partners to provide further relief if Greece meets program conditionality, and continued liquidity support by the ECB to Greek banks.

- In **Ireland,** the program has entered its final year with viable prospects for a successful return to reliance on market financing. A comprehensive agenda for restoring the capacity of the financial sector to support recovery, which includes resolving nonperforming loans, a rigorous asset quality review, and returning banks to profitability, has been put into motion. Most recently, Ireland successfully accessed the market with an oversubscribed € 5 billion 10-year bond at a favorable yield, reflecting strong policy implementation by the authorities together with European support such as extended maturities of EFSF/EFSM loans.

- **Portugal** has managed to successfully extend the maturity of its T-bill issue, secondary-market bond yields have declined substantially, and initial moves to regain access to the bond market have been successful, including a bond swap in October 2012 and a syndicated tap in January 2013.

20. **Nonetheless, sizable exposures remain**. Each of the three programs was approved on the basis of the modified second exceptional access criterion on debt sustainability, with the Fund contributing one-third of the overall financing (one-sixth in the case of the second Greece program).[11] This underlines the risk that Fund-supported programs will not achieve a sufficient improvement in the balance of payments to obtain external viability over the program period. It has also underscored the challenges the Fund faces in anticipating and quantifying the likely extent of international systemic spillovers, which should remain a key aspect of risk management work. The

[11] The modification allows the Fund to support arrangements with members where there is a high risk of international systemic spillovers and the analysis shows that the member's public debt is likely to be sustainable, but where this judgment cannot be made with a high probability (see 2012 Report on Risk management (SM/12/199, 7/20/12), Paragraph 21).

Board has since approved a request for an extended arrangement for Cyprus that will limit the Fund's contribution to one-tenth and not involve exceptional access.

21. **The Fund has also deployed non-financial means of assisting countries in the Euro area.** The monitoring of the Spanish financial sector reform program—which has contributed to a reduction in the potential for financial sector contagion in Europe—reflects a new modality of Fund engagement with European countries. This has not involved the Fund's balance sheet, although staff involvement in the design and implementation of the program poses some additional reputational risk. The success of this reform program would help limit tail risks. Moreover, Fund staff continues to provide significant TA resources, to advise on policy design and build institutional capacity in crisis countries.

22. **Through its regular surveillance activities, the Fund has continued to recommend policies aimed at fostering stability and growth in the Euro area as a whole**. In particular, it has emphasized the importance of orderly bank restructuring and financial support from European partners (including official sector debt relief, where needed) as well as progress toward a fiscal and banking union. These policies would boost program countries' capacity to repay the Fund, which hinges critically on their ability to regain permanent access to international capital markets, the prospects for which remain uncertain, as well as continued support from European partners.

Middle East and North Africa (MENA)

23. **The new programs being negotiated with several countries in the Middle East present significant reputational risks**. While likely to increase over time, credit exposures are on a much smaller scale than in Europe. Ongoing social and political uncertainty, however, has been limiting the room for much needed policy adjustments, with the need to reduce energy subsidies posing a particular challenge. Amid weakened fiscal and external positions, engagement in the region will therefore need to be calibrated carefully, taking into account the ongoing political transitions. If programs were to encounter difficulties or perceived to contribute to political upheaval, the Fund's reputation will be at risk. To limit these risks, the Fund is continuing to take a proactive role in communicating the need for adjustment under strong country ownership, and the supportive role played by IMF engagement.

Potential Spillovers, Credit and Liquidity Risks

24. **Amid a tepid global recovery, there are several scenarios where members may need recourse to the Fund's balance sheet.** For example, the Fund could be called upon to provide financial support to countries experiencing capital outflows in the context of volatility surrounding unprecedented liquidity support provided by major central banks. Even absent an acute crisis, there could be risks associated with a slow growth environment (for example, Box 3 describes possible spillovers from a prolonged European slowdown). Moreover, some existing Fund borrowers with already large exposures could face renewed difficulties, and the Fund could also be called upon to lend on an even larger scale within and potentially outside the euro area.

25. **To address these risks, the Fund's capacity to respond to the needs of all its members has been substantially enhanced.** The IMFC and G-20 Finance Ministers and Governors jointly

announced on April 20, 2012, an agreement to further enhance IMF resources for crisis prevention and resolution through a new round of temporary bilateral borrowing. Thirty eight members pledged US$461 billion in new bilateral resource commitments, equivalent to about SDR 307 billion. Of this amount, bilateral agreements totaling US$405 billion are either effective or have been submitted to the Board for approval. This borrowing is to serve as a second line of defense to the Fund's quota and New Arrangements to Borrow (NAB) resources and as a bridge to the Fifteenth General Review of Quotas. Together with the Fund's quota and NAB-based financing resources, resources pledged in 2012 bring the Fund's total potential lending capacity to over US$1 trillion.

26. **To mitigate risks associated with the scale of potential borrowing, modalities were adopted, which built on the framework adopted in 2009 and the subsequent agreed reforms of the NAB.** While stressing that the primary tool to mitigate risks is the strength of the Fund's lending policies, supported by adequate junior co-financing, Directors agreed on the need to protect the Fund against mismatches between its borrowing and lending maturities. Specifically, it was agreed that the maximum maturity of claims under the 2012 bilateral agreements should be 10 years; moreover, lenders should indicate that they stand ready to cooperate with the Fund as needed and appropriate, or as an alternative, for those lenders who are willing, the borrowing agreements should allow for an extension of the maximum maturity of claims for up to another five years with the lender's consent, following an Executive Board's determination that exceptional circumstances exist as a result of a shortage of Fund resources in relation to Fund obligations falling due. In addition, the borrowing guidelines stated that any quota increases under the Fifteenth General Review of Quotas are expected to be used to reduce and, depending on the size of the quota increase and the Fund's liquidity, eliminate the Fund's reliance on borrowing agreements.

27. **Nevertheless, the Fund continues to face some liquidity risks associated with its lending operations.** The encashment provisions in borrowing agreements, and the right of a member to repurchase its reserve tranche position upon the representation of a balance of payments difficulty would reduce the Fund's liquidity buffer, and in extremis could reduce the Fund's commitment capacity. In addition, the Fund could face liquidity risks if members face extended balance of payments pressures and become unable to make their scheduled repurchases in a timely manner. This risk is mitigated for lending financed by quota resources, which are the Fund's permanent resources. The modalities agreed for the 2012 bilateral borrowings will help to mitigate these risks in the event these resources are called upon. Comparable provisions do not apply to NAB credit arrangements, which have fixed final repayment terms.

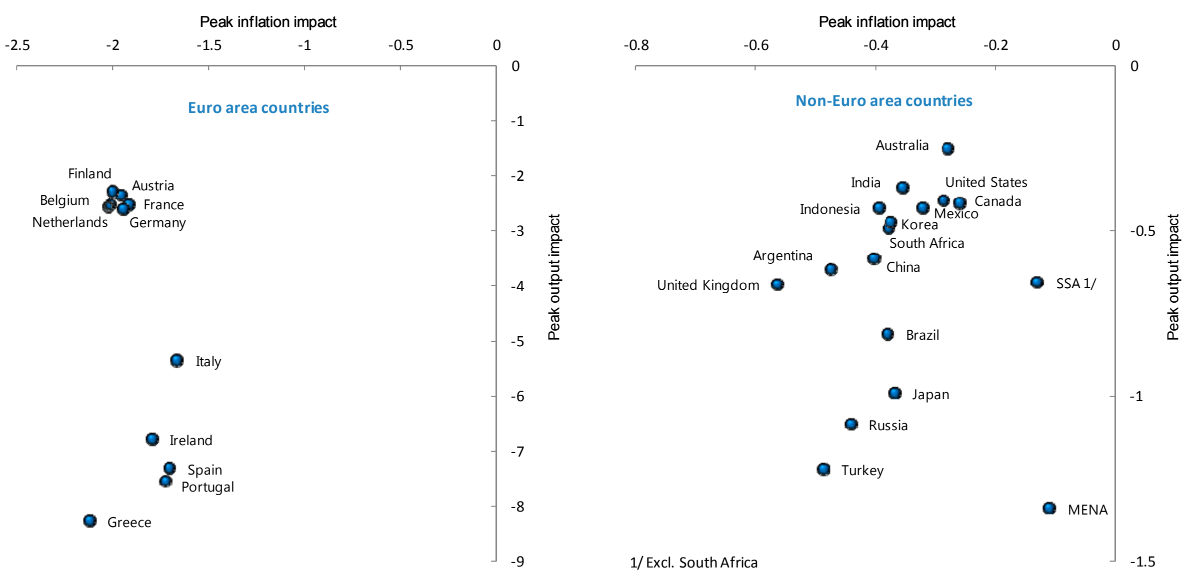
28. **Precautionary balances are being increased in response to the elevated credit risks.** At the last review of the adequacy of precautionary balances (April 2012) the medium-term indicative target was increased from SDR 15 billion to SDR 20 billion. This took into account the sharp increase in commitments and in actual and projected Fund lending. The increase in the indicative target also took into account the projected rise in individual exposures, in particular to European members, and the current limited capacity of the burden sharing mechanism. Precautionary balances at end-April 2013 totaled SDR 11.6 billion, significantly below the individual exposures of the three largest borrowers. On current projections, the proposed SDR 20 billion target would be reached in FY 2018–FY 2019.

Box 3. Protracted Slowdown in the Euro Area

One of the global risks identified by the Fund's multilateral surveillance exercises comprises the risk of a protracted period of slower growth in the Euro area. This risk is analyzed in a downside scenario presented in the April 2013 World Economic Outlook. In this scenario, ongoing public and private sector deleveraging depress private investment, with knock-on effects on private consumption. Lower than expected growth u**ndermines the anticipated fiscal adjustment, pushing up sovereign risk premiums, and prompting additional tightening in fiscal positions and credit conditions.**

Among the Euro area countries, which by scenario design would experience persistent stagnation, the countries in the periphery would incur the largest output losses. Outside the Euro area, countries with strong economic ties to the Euro area through trade and investment, such as Turkey and Russia as well as countries in the MENA region would see output drop by more than one percent relative to the baseline. While the impact is somewhat smaller, Sub-Saharan African (SSA) countries would on average incur a significant output loss.

Euro area slow growth scenario
(deviation from baseline, percent of GDP)



Souce: Fund staff estimates.

Souce: Fund staff estimates.

As slower growth translates into larger external financing needs, the realization of this scenario could result in additional calls on Fund resources. For the Fund itself, risks arise from a possible need for program redesign in existing arrangements and a possible need for new arrangements. To mitigate these risks, contingency planning should remain as a critical element in Fund programs and in surveillance work, especially for MENA and SSA countries.

29. **The capacity of the Fund's existing financial mechanisms for addressing an arrears situation would come under substantial strain if one or more large borrowers were to face difficulties in meeting their obligations to the Fund on a timely basis**. As repurchases on arrangements approved in 2010 start to fall due, repurchases which amounted to SDR 12.2 billion in 2012, are scheduled to rise to an average of SDR 18.6 billion a year over 2013–2014. By way of comparison, at the current SDR rate of 0.07 percent, the remaining burden sharing capacity is about SDR 11 million a year, which could cover overdue charges and surcharges (level and time-based) on overdue repurchases amounting to about SDR 0.3 billion.

30. **Reflecting growing inter-linkages within and across the global economy, the Fund has also enhanced its capacity to detect global trends and prepare member countries for economic and financial spillovers and risk of contagion.** The Integrated Surveillance Decision (ISD) adopted by the Board in July 2012 enhanced the legal framework for surveillance in a number of important ways. In particular, the Fund can discuss with a member country the full range of spillovers from its policies when they may have a significant impact on global stability. By setting clear expectations for the practice of both bilateral and multilateral surveillance, the ISD helps improve the quality, evenhandedness, and effectiveness of IMF surveillance, as well as foster a better integration of all surveillance activities.

Scope for Concessional Lending

31. **Progress is being made on the 2012 Board-endorsed strategy to place the Fund's concessional lending framework on a sustainable footing**. The strategy is based on securing agreement from members representing at least 90 percent of the agreed distribution of windfall gold sale profits to transfer those resources (or make an equivalent contribution) to the PRGT.[12] In October 2012, the needed assurances for the first distribution of windfall profits (about US$1.1 billion) were reached. Approvals for the second distribution (US$2.7 billion) still need to be secured.

B. Governance and Legitimacy Risks[13]

32. **In December 2010, the Board of Governors agreed on a package of quota and governance reforms to enhance the Fund's legitimacy and effectiveness.** These reforms built on a process of reform initiated in 2006 and included a doubling of quotas, a major realignment of quota shares in favor of dynamic emerging markets and developing countries (EMDCs), and protection of the voting power of the poorest members. The Board of Governors also supported an amendment to the Articles of Agreement that would facilitate a move to a more representative, all-elected Executive Board, and the reforms included a commitment to reduce the number of Executive

[12] The addition of these windfall profits to PRGT resources would imply a self-sustained base envelope of about SDR 1¼ billion in annual lending capacity – thus ensuring that the PRGT has the resources to meet projected demand for IMF concessional lending over the period 2013–2035.

[13] This section was prepared by FIN and SPR.

Directors representing advanced European countries in favor of EMDCs by two. The Board of Governors committed to using best efforts to implement the package by the 2012 Annual Meetings. The Board of Governors also requested that the timetable for completing the Fifteenth Review be brought forward to January 2014 and that the Executive Board complete a comprehensive review of the quota formula by January 2013.

33. **While considerable progress has been made, the necessary conditions for making the reforms effective are not yet in place**. Two of the three thresholds were met by the target date of the 2012 Annual Meetings—the required consents to quota increases under the Fourteenth review (70 percent of quotas) and the number of members needed to agree to the Board reform amendment (three-fifths of the membership). However, the required 85 percent of the voting power for the Board Reform Amendment to become effective has not yet been secured.[14] Notwithstanding the delay in implementing the Board reform amendment, a number of advanced European members have moved already to consolidate their representation at the Board in the 2012 election of Executive Directors—Belgium and Luxembourg moved to the Netherlands constituency, and a new Central and Eastern European constituency emerged.[15] The comprehensive review of the quota formula was completed in January 2013, but it was not possible to reach agreement on a new quota formula. Rather, it was agreed that achieving the necessary broad consensus on a new quota formula would best be done in the context of the Fifteenth Review.[16]

34. **The delay in implementing the 2010 reforms risks undermining the Fund's legitimacy and effectiveness, and these risks would greatly intensify in the event of a prolonged delay.** As long as the Fourteenth Review quota increases are not in place, the rebalancing of quota shares and voting power agreed in 2010 to better reflect changing global realities cannot come into effect, and the Fund will also continue to rely heavily on borrowed resources to finance its lending operations, thereby departing from the principle that the Fund is and should remain a quota-based institution. Moreover, a prolonged delay would put in jeopardy the timetable for the forward-looking elements of the 2010 reforms, including agreement on a new quota formula and concluding the Fifteenth Review by January 2014. Such developments could compromise the effectiveness of the Fund's engagement with its members across a broad spectrum of its surveillance and crisis prevention activities.

35. **Given the above concerns, staff and management have been actively engaged with country authorities to secure the necessary consents and acceptances in close collaboration**

[14] As of June 3, 2013, 139 members having 75.35 percent of total voting power had accepted the proposed Board-reform amendment, while 151 members having 78.44 percent of total quota had consented to their proposed quota increases. Real-time updates on the status of acceptances are posted on the IMF's external website at http://www.imf.org/external/np/sec/misc/consents.htm.

[15] Switzerland and Poland have also agreed to rotate a chair every two years starting in 2014, conditional on the implementation of the 2010 quota and governance reforms.

[16] See *Report of the Executive Board to the Board of Governors on the Outcome of the Quota Formula Review* at http://www.imf.org/external/np/pp/eng/2013/013013.pdf .

with the Executive Board. The Board continues to be updated on a monthly basis on the status of acceptances. The work program includes an update of the quota database in early June, with an informal Board discussion on the data update and the reform of the quota formula planned for later in the month. However, the above risks cannot be fully mitigated, given that the process of acceptances of the 2010 reforms lies in the hands of the membership.

C. Longer Planning Horizon[17]

36. **Identifying Vulnerabilities in a Changing World**. Since its establishment, the Fund has demonstrated remarkable adaptability in supporting the international monetary and financial system. The complex and rapidly evolving post-crisis global environment pose new challenges to the Fund's resilience. In this context, there is a critical need for the Fund to look beyond the current crisis, to identify new sources of global and economic financial vulnerabilities, and to enhance our understanding of spillovers and interconnectedness. This will entail assessing tail risks, and assuring an adequate focus on emerging market economies and long-term issues.

37. **Risk mitigation tools**. Since the 2008 crisis, the Fund has taken a number of steps to increase its capacity to detect risks, including cooperating with the Financial Stability Board on the Early Warning Exercise, widening the scope of its internal vulnerability exercise to advanced economies and low-income countries, and adopting a new process to coordinate and consistently communicate staff views on risks in bilateral and multilateral surveillance products. There have been new approaches to study contagion and risk transmission channels, including several global spillover reports and interconnectedness papers that applied novel methodological approaches in this area. The Fund will also think more systematically about the longer-term challenges facing the institution and implications for operations and governance; deepen its ongoing analysis of inter-linkages and spillovers; and continue to strengthen work on financial sector repair and reform.

Noncore Operational Risks

D. Information Security[18]

38. **TGS continues to make good progress on addressing the risks and issues identified from the post-breach activities**. In response to the 2011 Working Group on Selected IT Security Controls and other post-breach recommendations, TGS has ongoing efforts related to:
(i) remediation and improvements to IT security controls that were already underway; (ii) the independent Comprehensive Information Security Risk Assessment conducted by PwC; (iii) the development of new Information Security Policies; and (iv) raising staff's information security awareness through training and communications.

[17] This section was prepared by SPR.

[18] This section was prepared by TGS.

39. **Improving the state of our IT security controls has remained a top priority in FY 2013. To address some of the risks related to unauthorized access to the Fund's network; reducing the potential for unauthorized access to Fund Information; reducing impact in the event of compromise; and improving monitoring, detection, and preventative controls, TGS has implemented:** (i) Network Access Control—a system that only allows authorized and compliant systems to access the Funds internal network; (ii) Application Whitelisting as part of a staged laptop refresh deployment—a system that only allows safe and known software to execute on users' machines while blocking unknown and malicious code; (iii) Restriction of Local Admin Rights as part of the aforementioned staged laptop refresh deployment—a means to minimize exposure in the event a user's system or account is compromised; (iv) Advanced Malicious code detection and intrusion disruption solution—a system that monitors email and web traffic, correlates activity, and disrupts attacks similar to that experienced in 2011; and (v) Mobile Device Management of Fund-owned mobile devices—a system that enforces minimum security configuration standards on mobile devices that process Fund information.

40. **A Comprehensive Information Security Assessment was completed by PricewaterhouseCoopers (PwC) in May 2012**. This report delivered an independent assessment that concluded with recommendations to further improve governance of IT security activities, acquisition of needed skills and capacity, and critical security processes. The PwC recommendations defined a three-year plan of action to execute 22 projects, hire 20 new personnel, and provide further backing for in-flight projects focused on implementation of technology, process improvements, raising awareness, and policy-based controls.

41. **In response to the PwC assessment, TGS developed and proposed an alternate risk-based Enterprise Information Security Program (EISP).** The plan aimed to improve the Fund's information security posture, prioritize high risks, and take into account the Fund's ability to absorb change and capacity to implement. The EISP, executed over five years at a reduced cost, and with fewer personnel, would close the gaps identified by the assessment. The effort would significantly improve foundational information security capabilities and deliver measurable security improvements. Given the increasing sophistication of information security threats targeting the Fund, even with the EISP investment, the Fund will remain at risk for attacks that could result in security breaches. However, the EISP will position the Fund to better detect and respond to these breaches and significantly reduce the cost of business disruption. On February 22, 2013, management approved the five-year EISP and the hiring of 12 personnel over a two-year period. This approach will allow TGS to build the necessary capability to address the issues identified and execute 26 projects.

42. **An important step during FY 2013 was the development and approval of a new Information Security Policy Framework. The Security Policy Group, chaired by Mr. Shinohara,**

approved six new Information Security Staff Policies.[19] The policies were developed in close collaboration across Fund departments and sought to clarify roles, responsibilities, and raise awareness of the role personnel play with regards to protecting the Fund's information assets. The policies were approved and communicated officially by management on March 7, 2013, including the Information Security Policy—"what everyone in the Fund needs to know and do to protect the Fund's information assets." The efforts to improve and communicate IT security policies allowed management to set clear expectations for staff. To protect Fund assets and tighten the acceptable usage of Fund systems, Information security is the shared responsibility of all Fund personnel.

43. **Raising information security awareness and promoting information security risk-aware culture at the Fund has also been a focus during FY 2013.** The Security awareness campaign launched post-breach on July 11, 2011, had reached a completion rate of 75 percent by May 2012. To further improve the completion of the course, management, on September 10, 2012, communicated that the completion of the course was mandatory and regular progress reporting would be required. The completion rate as of end-April 2013 was 89 percent. Providing additional support, management required recipients of high-performance laptops to have completed the information security awareness course as a prerequisite to receiving a new laptop. Future efforts and focus will include (i) encouraging greater security awareness training completion rates across departments, and (ii) continuing and expanding the targeted communication and awareness training plan to cover awareness of new Information Security Policies.

44. **Implementation of the aforementioned solutions brings the Fund's systems into closer alignment with the new Information Security Policies.** The results have already delivered value by detecting and preventing a large number of Fund targeted security threats. In January 2013 alone, 320 users were targeted with email containing malicious code, where one instance would have resulted in a significant breach if undetected. Between March and April of this year, the advanced malware detection and prevention solution stopped seven significant attempts, indicative of an escalating targeted campaign, to gain unauthorized access to Fund systems. The Network Access Control system has already detected numerous instances of personnel inadvertently installing software and changing configurations that subvert many layers of security protection leaving computers accessible to external parties. Approximately 30 instances of these types of activities are detected every month. In addition, the application whitelisting solution blocked 257 malicious files from being executed by users within the first year of implementation.

45. **Despite significant focus on information security, risk remains due to ever increasing types and levels of attacks.** The Fund continues to face attacks of varying degrees of severity, from many different vectors. The risks from such threats leads TGS to believe, as PwC highlighted, and in alignment with the views that departments have expressed in the 2013 Departmental Risk Survey,

---

[19] Information Security Staff Policies may be found on the Fund's intranet: http://www-intranet.imf.org/aboutIMF/Pages/InfoSecGuide.aspx

that the likelihood of such an event is medium to high. TGS also believes that continued focus on executing the EISP will contribute greatly to a stronger defense against high probability and high-impact information security events which better positions the Fund to respond to unknown and sophisticated cyber-security events.

46. **EISP Priority activities for FY 2014 include:**

- **Remediation of PwC identified vulnerabilities** – a year-long vulnerability remediation program has been initiated to address the remaining critical, high–, and medium-risk vulnerabilities by the end of FY 2014.

- **Hiring IT security personnel (four staff and four vendors)** – to address the priority capability gaps identified by PwC focusing on Information Security Operations management (Security Monitoring and Incident Response), Security Architecture, Information Security Risk Management, Identity and Access Management engineering.

- **Improving Information Security Governance, Risk and Compliance management processes, and defining strengthened technical control requirements** – projects have been initiated to deliver by mid-FY 2014: a Security Charter; stronger risk and compliance management processes that will instill rigorous and consistent approaches to risk management; compliance to information Security policies; new technical security standards; and a better defined and stronger information security posture, aligned to new Information Security Policies.

- **Continuation of Security awareness** – raising efforts to execute an agreed annual security awareness campaign and further target security awareness and training efforts.

- **Enhancing critical security processes** – such as security incident and vulnerability management, a metrics program to measure the performance of security processes/risk reduction efforts, and consistent application of controls.

Reliability and Performance

47. **In response to widespread performance and reliability issues experienced with Vista PCs, TGS has taken several steps to remediate the problems, including the implementation of improved monitoring of PC performance**. This monitoring led to improved performance and reliability, including (i) the replacement of the Fund's software distribution system with a top-rated solution (due for completion in FY 2014); (ii) reduction of tasks which run automatically when staff "start-up" their workstation (a factor in slow start-up times); (iii) upgrading the antivirus application; (iv) executing a utility to defragment hard drives; and (v) adjustments to Outlook based on guidance from Microsoft.

48. **TGS has accelerated the deployment of new Windows 7 laptop and desktop machines.** Deployment of the new PCs began with the laptop refresh at headquarters in January 2013, and will continue with regional and remote offices (completing by the end of Q1 FY 2014). Immediately following the laptop deployment, the desktop deployment will begin with a projected completion,

including remote and regional offices, in Q3 FY 2014. As part of the renewal project, TGS has reduced the number of applications in the base image configuration, which are installed Fund-wide. This will prevent applications, which are only needed by a subset of staff from negatively impacting workstation performance. All applications will still be available to download as needed in Software Self Service. Initial staff feedback regarding the new PCs has been very positive.

49. **TGS recognizes the importance of maintaining the performance and stability improvements delivered by the PC refresh and other initiatives.** To achieve this, work has been done to strengthen the quality assurance of all standard applications, proactively testing for performance and stability impacts. In addition, various security initiatives, such as limiting Local Admin Rights and moving application whitelisting to block mode are intended to not only improve security, but to minimize the impact of non-standard applications on overall performance. A third related aspect is a longer-term strategy to package all widely used business applications and make them available in Software Self Service. This approach should lead to fewer conflicts between unknown and untested applications, more standardization of applications, improved software licensing compliance, and ultimately reduced calls to the help desk for support. Risk remains with this approach as it represents a significant change for staff in how they use Fund owned PCs.

50. **Finally, in response to increased risks and departmental concerns, TGS will replace the off-site vendor model with an on-site vendor model for highly complex applications beginning in FY 2014**. Based on material and increasing delivery risks identified by the Human Resources and Finance departments, a working group, composed of selected business sponsors and TGS staff, proposed the replacement of TGS' resources assigned to six applications with on-site vendors for a limited set of highly complex applications. The intent is to build a cadre of on-site, highly-skilled vendor resources with extensive business knowledge that would provide a basis to address the significant deficiencies in the offshore model and would reduce application support risks to more acceptable levels. The working group further proposed that the new model should be implemented using a risk-based phasing approach, moving urgently to address the two applications (iFIN and HCM) that are most complex and carry the highest risk should failure occur. Following a stock taking exercise at the end of the year to confirm that the on-site model is achieving the desired results, the model would be extended to the remaining four applications (DMX+, ICS, FACTS, and PATS) in FY 2015. Management approved this recommended approach on February 26, 2013, and additional resources were provided for this purpose in the FY 2014 budget.

E. Human Resource and Budget[20]

51. In 2012, workload pressures and low morale were identified as the main drivers of budget and human resource risks. Updates on these two areas are provided below.

[20] This section was prepared by HRD and OBP.

Workload pressures

Workload pressures, along with general budgetary concerns, were cited as a key risk. The limited or no growth in the real administrative budget in an environment where there is still substantial crisis-related work has contributed to continued high rates of overtime, compared to historical norms, and concern that progressively, these work pressures will lead to low morale and an impaired quality of work. A few departments also expressed concern that the budgetary limits were constraining the ability of the IMF to address the needs of all members and to focus on all of its core areas of work. The FY 2013 budget tried to address these concerns by directing additional resources to crisis areas, including European program countries. The addition of some 31 FTEs and 67 contractual employees throughout the institution, bringing Fund total employment above pre-downsizing levels, was intended to address workload pressures, but overtime remains high. Finally, departments agreed on some streamlining of multilateral surveillance products.

Low morale

52. **Low morale of staff was cited as the key HR risk. Low morale stems fro**m limited promotion prospects, the possible negative impact of workload pressures, and an uncertain compensation outlook. Measures have been put in place in response to the 2010 staff survey, when the issue of low morale first came to the forefront. The accountability framework for departments is now in its second year; in part, it promotes more effective management of budgets and people. Mobility concerns of staff have resulted in the expansion of the external mobility program (the number of slots were doubled to 60), while internal mobility bottlenecks are being addressed by the B1–B3, A15, and A14 internal mobility initiatives which to date have resulted in around 40 transfers of staff who had been in their previous departments for at least seven years. The Diversity Office has undertaken an extensive program to enhance communication and education on diversity and inclusion; a performance management support team has been set up to provide more tailored guidance to departments; a statement on workplace values was adopted; and an improved dispute resolution system has been implemented, which includes the appointment of the Fund's first Mediator. Looking ahead, the corporate workforce planning paper, which was presented to the Executive Board this past February 25, sets out a path to further boost staff morale through increased training opportunities, greater research assistant support, and encouragement of job enrichment through increasing responsibilities, especially at the senior economist level.[21] This year's compensation round resulted in a better outcome for staff; and the 2012 recruitment and retention experience suggests that the Fund remains a reasonably attractive employment option for economists. The broader HR community has been actively engaged in the development and implementation of this strategy and continues to assist in monitoring effectiveness at the departmental level.

[21] The corporate workforce planning paper also suggested revisions to the employment framework in the Fund to strengthen retention of institutional knowledge, another HR risk identified in 2012, and this will be taken up in greater detail in the forthcoming Executive Board paper on the employment framework planned for November 2013.

53. **The FY 2014 budget includes a number of steps to address work pressures**. First, it will provide for significant additional personnel resources notwithstanding a flat overall budget: the budget will have space for about 40 new staff positions compared to FY 2013. Some of these staff positions will be targeted specifically to departments with high overtime and others to where new needs are emerging. In addition, departments were asked to continue streamlining their activities. Thirdly, henceforth departments will be allowed to hire A-level professional staff above their FTE staffing limits, as long as they remain within their dollar budget ceilings. The intention is to reduce excess overtime substantially by maximizing the use of the allocated staff resources and reducing vacancy lags. Finally, managers are being asked to enhance their monitoring and management of workload to ensure that work is being allocated within departments to minimize the number of staff with extremely high overtime.

54. **The recently concluded 2013 staff survey provides insights into on-going or new staff concerns, while signaling improvements to date in the work environment at the Fund since the 2010 survey**. Survey results show strong overall staff engagement, on par with survey comparator organizations. However, the survey indicated that there remain morale issues stemming from perceived career opportunity limitations and the fairness of managerial practices. Based on the advice of the Gelfond Group, who managed the survey for the Fund, Management has identified career enhancement as a key post-survey focus area, and is engaging departmental leadership and staff to discuss avenues to address this concern by the time of the 2013 Annual Meetings.

F. Management of Risk Related to the HQ1 Renewal Program[22]

55. **The HQ1 Renewal Program is the largest capital project undertaken by the Fund and will be conducted over the course of 3.5 years while the building remains occupied**. TGS is committed to minimizing and mitigating risk from several perspectives, including (i) disruption to work; (ii) health and safety concerns; and (iii) strengthened project controls.

Disruption Framework

56. **A Disruption Framework has been designed to provide answers to several key questions: (i) how will I get my work done?; (ii) how will I access the building?; and (iii) what services will be available?**[23] TGS will communicate the timing, details, and potential impact of the HQ1 Renewal project activities to staff, and is focused on ensuring that all staff concerns are received and acted upon in a timely manner through such steps as the expansion of the Fund's Facilities Help Desk.

57. **Staff will be kept informed of construction schedules, sequencing, changing building access routes, security plans, environmental and ambient comfort issues, as well as other**

[22] This section was prepared by TGS.

[23] DM#5060380, HQ1 Renewal Program, *Working with the HQ1 Renewal: An Insider's Guide to Office Access and Service.*

developments. This will be accomplished using a variety of communication channels, including (i) the program website http://HQ1; (ii) intranet notices and postings; (iii) intranet news articles; (iv) program signage; (v) Fund-all emails and desktop messaging; (vi) periodic presentations to staff; and (vii) feature videos and the HQ1 Exhibit.

58. **Throughout the duration of the program, TGS will work to minimize the impact of construction on staff work.** A variety of approaches will be used including (i) segregation of construction activities from Fund operation; (ii) off-hours work for activities involving the removal of asbestos or excess noise; (iii) establishment of maximum allowable noise levels during business hours; (iv) vibration mitigation; (v) air quality monitoring; (vi) alternative work arrangements (e.g., telework and opting out of HQ1); (vii) requests for work stoppage, as provided in the Program's Disruption Framework; and (viii) implementation of swing space seats in HQ2.

Health and Safety

59. **The Fund is committed to protecting the health and safety of staff and other building occupants, with the objective of safeguarding health and operating in an environmentally sustainable manner, including by exceeding best practices in certain areas.** To promote excellence in health, safety and environment (HSE), the Fund is committed to voluntarily comply with applicable government regulations, international standards, and best practices as appropriate. These regulations not only apply to the HQ1 Renewal, but to day-to-day operations as well.

60. **The Operational Health and Safety Management Policy that has been in place at the Fund since 2011 involves multiple controls.** [24] These controls will continue to be followed throughout the HQ1 Renewal project and are implemented through various governance groups, including the (i) Health, Safety and Environment Committee (HSEC); (ii) Emergency Operations Response Team (EORT); and (iii) Crisis Management Team (CMT).

- The HSEC is a cross-departmental committee (HRD, SAC, three divisions in TGS and the World Bank Health Services Department) that oversees all aspects of staff health, safety, and environment issues by developing and implementing HSE strategy and monitoring performance. The primary objectives of the HSEC are to (i) provide a framework that protects Fund staff's health, safety, and improve the Fund's work environment; (ii) direct and oversee the overall HSE program strategy; and (iii) address health and safety issues affecting staff.

- The EORT is composed of members from TGS and HRD who are empowered to immediately respond to emergencies of all kinds. The EORT determines the seriousness of an event and, when appropriate, recommends the activation of the CMT based on the potential impact to the Fund's personnel, assets, operations and reputation.

[24] DM#4515286, *International Monetary Fund Environmental Health and Safety Plan*, June 23, 2011.

- The CMT is an inter-departmental committee that manages events that warrant a higher level of response in order to minimize the adverse impact on Fund personnel, assets, operations, and reputation. Members take a Fund-wide view of issues, ensuring that the strategic and operational needs of the Fund are fully reflected in managing the event.

61. **The Fund's Operational Health and Safety Management Plan details requirements for safety related to hazardous waste management, indoor air quality, and water hygiene management.** The detailed plans stipulate specific monitoring periodicity as well as the standard to be achieved for each type of program. For example, hazardous materials will be removed at night and on weekends following strict international best practices as well as U.S. regulations for health and safety. Staff will be notified prior to removal of these materials and air quality will be monitored on a regular basis. Water hygiene management relies on annual drinking water assessments, quarterly testing of water for legionalla, and the use of filtered drinking water throughout HQ2. A filtered water system is included in the plans for HQ1.

62. **The HQ1 Renewal project meets, and in some cases exceeds, international best practice for operational health and safety management.** In addition to the various safeguard that were already planned, in April 2013, the Staff Association Committee (SAC) was authorized to secure consultancy services to provide an independent peer review of the HQ1 Renewal project removal protocols for hazardous material, including asbestos. The independent consultant hired by the SAC, is of the opinion that the removal protocols for hazardous materials, inclusive of additional recommendations, properly implemented, would eliminate potential exposure risks to Fund staff and other building occupants.[25] There are a number of ways staff will be notified of work involving the removal of hazardous material. For example, staff will be notified (i) at least a month in advance of the general schedule for asbestos removal; (ii) seven days in advance for specific work; and (iii) an all-clear will be given each day after asbestos removal is completed. To accommodate those staff who remain concerned for their health and safety, alternative work arrangements for staff wishing to opt out of HQ1 during construction have been identified and are being implemented.

Control Framework

63. **An extensive HQ1 Renewal Program control framework has been vetted by members of the HQ1 Renewal Program Review Team (FIN, LEG, OBP, and TGS) and the Project Controls Team (FIN, LEG, OBP, and TGS) and compiled into an Operations and Procedures Manual.** The manual provides the project team necessary information for (i) controlling the scope of the operations; (ii) ensuring value for money; and (iii) enforcing strict adherence to budget, schedule, and costs.[26, 27] The policies and procedures in the framework have been largely adapted from the

---

[25] A link to the BHS report can be found on the IMF Staff Association website at: http://www-intranet.imf.org/sites/sac/Pages/Default.aspx#JQueryZoneTabs_7

[26] DMSDR1S-#4924333, *HQ1 Renewal Program Operations and Procedures Manual*, Prepared by the Technology and General Services Department, Reviewed by the HQ1 Renewal Program Review and Control Teams, Version 2, April 19, 2013.

Fund's existing capital budget management control framework. Certain additional control mechanisms for administering the HQ1 Renewal program have been specifically incorporated to mitigate unique project-specific risks.

64. **Three elements make up the control framework for the HQ1 Program: (i) governing directives and policies for administering the renewal; (ii) processes and procedures for the Program's operations; and (iii) controls that ensure that the operational processes and procedures comply with the policies.** These directives currently provide additional checks and balances to the Fund's existing capital budget processes/procedures and promote responsibility, and accountability, and safeguard the integrity of the renewal. In addition, a collaborative procedural approach has been adopted that includes emphasis on controls and leverages the expertise of both external consultants for program support as well as internal Fund staff to administer the program. For example, the Projects Control Team, whose mandate is to provide oversight of all aspects of the Fund's financial and administrative control framework for the renovation of HQ1 and the Concordia building, meets regularly to assess control effectiveness, issues and enhancements. This collaborative approach will enable the Fund to: (i) effectively and efficiently oversee all project activities; (ii) appropriately retain control over critical financial management systems; and (iii) adequately ensure that the Fund has access to project management best practices and short-term technical support on an as-needed basis.

65. **The principal objective of the risk management framework is incorporated into the overall control framework to identify, assess, and proactively manage risks associated with the HQ1 Program**. The risk framework is designed to provide assurance on the availability and operation of mitigating controls that would detect and deter risks from materializing. Consistent with the guidance issued by external consultants, the risk management framework establishes a risk appetite and risk tolerances for the program.[28] It also provides the reporting criteria for incidents which deviate from the established controls and /or risk mitigation strategies.

ISSUES FOR DISCUSSION

Executive Directors' views are sought on the following issues:

1. Do Directors agree with the risk assessments in this report? Are there any significant risks that Directors find missing or alternately over stated?

2. What are Directors' views on the analysis and mitigation measures?

---

[27] *HQ1 Renewal Program and Concordia Renovation Project Administrative and Financial Controls – Procedures and Operations*, Prepared by the Finance, Technology and General Services Departments, and the Office of Budget and Planning in consultation with the Legal Department. December 22, 2011. EBAP/11/131.

[28] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) in their report entitled "Enterprise Risk Management-Understanding and Communicating Risk Appetite," dated January 2012. COSO is a joint initiative of five private sector organizations representing accountants, auditors and CPAs and is dedicated specifically to providing guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extend to fraud in organizations.

Appendix I. The Fund's Risk Management Framework

The Fund's risk management framework was established in 2006 following extensive work by a Task Force and various discussions with Executive Directors.[1] The Fund's framework uses the ERM concepts promulgated by COSO.[2] As part of this framework, the ACRM was established to assist Fund management in: analyzing, synthesizing, and reporting risks; enhancing the awareness in departments of risk management; reporting to the Board on risk management matters; and monitoring progress in the implementation of proposed mitigation measures, based on departmental submissions.

The Fund's risk management framework, which initially incorporated four risk categories, now has three main risk categories as the elements of the fourth risk—core mission—have been distributed amongst the remaining three risks:

- **Strategic risk**—The risk that the Fund's medium- and longer-term objectives and formulation of its strategies does not meet the evolving needs of the Fund's membership. Strategic risks include the following subcategories: strategic directions, financial resources, people, ethics (with governance and culture) and communication.

- **Operational risk**—Core operational risks are that the Fund will not achieve macroeconomic and financial stability in member countries, promote international macroeconomic cooperation, contribute to development initiatives in low-income countries, and provide capacity building services. Specific subcategories of core operational risks include: surveillance activities, lending operations, technical assistance, and liaison to counterparts. Noncore operational risks arise from the exposure of the Fund (and individual Fund organizational units) to direct or indirect losses or negative effects, including reputational, resulting from failures or inadequacies in business processes, people (the HR function), or systems (IT and facilities), as well as from external events (safety and security).

[1] Report of the Task Force on Risk Management (EBS/06/4, 1/09/06 and BUFF/06/24, 2/06/06), Second Report of the Task Force on Risk Management—Task Force Proposals on the Implementation of a Risk Management Framework at the Fund (EBS/06/74, 6/26/06), Statement by the Managing Director on the Second Report of the Task Force on Risk Management (BUFF/06/07, 6/19/06), and Risk Management—Further Considerations (SM/06/386, 12/04/06).

[2] ERM (Enterprise Risk Management) is an integrated framework to manage risks across the organization, and COSO (The Committee of Sponsoring Organizations of the Treadway Commission) is a leading organization in risk management.

- **Financial risk**—The possibility of direct, or indirect, losses or other negative effects on the Fund's financial position arising from risks in the areas of credit, income, liquidity and investment and budget management.

Reputational risk was not included as a separate category but is implicitly covered in the other categories, as it can materialize as a consequence of adverse events in any or all of them. Compliance with national legislative and regulatory requirements, which is typically included among the four broad risk categories, was deemed less material to the IMF. Therefore, it is covered instead under the operational risk category.

Annual assessments of risks have been conducted to: (i) inform management and the Board of perceived residual risks by departments, after taking account of mitigation measures; and (ii) apprise departments of risks and of efforts to mitigate risk in other areas of the Fund. These assessments also recognize that the risks associated with achieving the Fund's various objectives depends in part on the external environment, in particular, actions by member countries.

Annual reports on risk management were discussed by the Executive Board in 2007, 2009, 2010, 2011, and 2012. In addition, since 2007, updates, informal briefings and interim reports have been prepared.[3]

[3] 2007 Report on Risk Management (SM/08/90, 03/06/07, BUFF/07/42, 03/23/07 and BUFF/07/65), Report on Strategic and Core Mission Risks in the Fund (SM/07/90, Supplement 1, 03/09/07), Report on Financial Risk in the Fund (SM/07/90, Supplement 2, 03/09/07), Risk Management—Update (FO/DIS/08/7, 01/16/08), Risk Management—Interim Update (FO/DIS/08/53, 06/02/08; BUFF/08/79), 2009 Report on Risk Management (SM/09/44, 02/13/09; BUFF/09/42), 2010 Report on Risk Management (SM/10/115; BUFF/10/65), 2011 Report on Risk Management (SM/11/101); BUFF/11/87) and 2012 Report on Risk Management (SM/12/199; BUFF 12/94).

Appendix II. 2013 Survey Results

Introduction

1. **The responses from the departmental survey consisted of three forms:** (i) a description of the risk and slotting into a risk category; (ii) a quantitative measure indicating the department's view on the degree of severity of impact as well as the likelihood of occurrence of the risk; and (iii) a written qualitative characterization of the perceived risk. While the quantitative results provide a relatively hard measure of the degree of risk involved for each sub-risk category, the qualitative results provide a clearer, more nuanced picture of the precise risk that was intended to correspond to the label of a sub-risk category. Often, these descriptions reveal an overlapping of a risk across the different categories of risk—strategic, core operational, and noncore operational—as well as across specific subcategories within each grouping. Also weighing in as a factor in interpreting the results, are the obviously different capacities of different Fund departments to make judgments about specific kinds of risks, particularly those facing the Fund in general. Particularly problematic in interpretation were the results on noncore operational risks, since departments were asked to characterize risks bearing on their own operations, so any aggregation of responses across departments at best identifies some broad commonalities in the types of risks faced. The following attempts to describe both what the statistics seem to suggest about the risks faced by the Fund, and, just as importantly, the qualitative messages about these risks provided by departments.

2. **The ratings for the degree of severity of impact are**:

- Rating A: Minor: This rating would be consistent with a low-impact, requiring only minor corrective action.
- Rating B: Medium-Low: This rating would involve moderate or modest impact and may require remedial measures, but not necessarily the involvement of senior management.
- Rating C: Medium-High: A medium-high rating would often imply significant impact or disruption, requiring speedy action; some involvement of senior management may be required.
- Rating D: Serious: Such a risk would typically involve a major disruption to work, a crisis, or a major deleterious impact, financial or otherwise, on desired outcomes; require urgent action by senior management; and have a major impact on the Fund's reputation.

The likelihood ratings are:

- Rating 1: Very unlikely but not negligible

- Rating 2: Unlikely but possible
- Rating 3: Likely
- Rating 4: Very likely/Almost certain

Broad survey results

3. **As noted above in the text of the report (and as shown in Appendix Table 1),** while respondents were cautious in their assessment on the likelihood of occurrence of a risk, with less than nine percent of responses suggesting that a risk would occur with a very high likelihood or certainty, this represents an increase relative to six percent in 2012. Few risks (less than 11 percent) were seen as very unlikely. Slightly more responses were characterized as "unlikely but possible" rather than "likely" (75 vs. 56). For those risks characterized either as highly unlikely or highly likely, they were predominantly among the noncore operational risks to which the Fund is exposed (business processes, IT, and human resource related). Of risks seen as likely or almost certain, noncore operational risks dominate with strategic risks closely following as a share of such risks.

In contrast, departments proved increasingly more prone to express concern that the occurrence of a risky event might have a serious impact, with more than 25 percent viewed in this way (relative to 20 percent in 2012), and more than 75 percent of responses characterizing the impact of such risk occurrences as at least of medium-high impact or as entailing a potentially serious impact (relative to 68 percent in 2012). Noncore operational risks represent about 40 percent of risks viewed as of medium-high or serious impact, with strategic (principally governance) and core operational risks each representing about 30 percent of such risks.

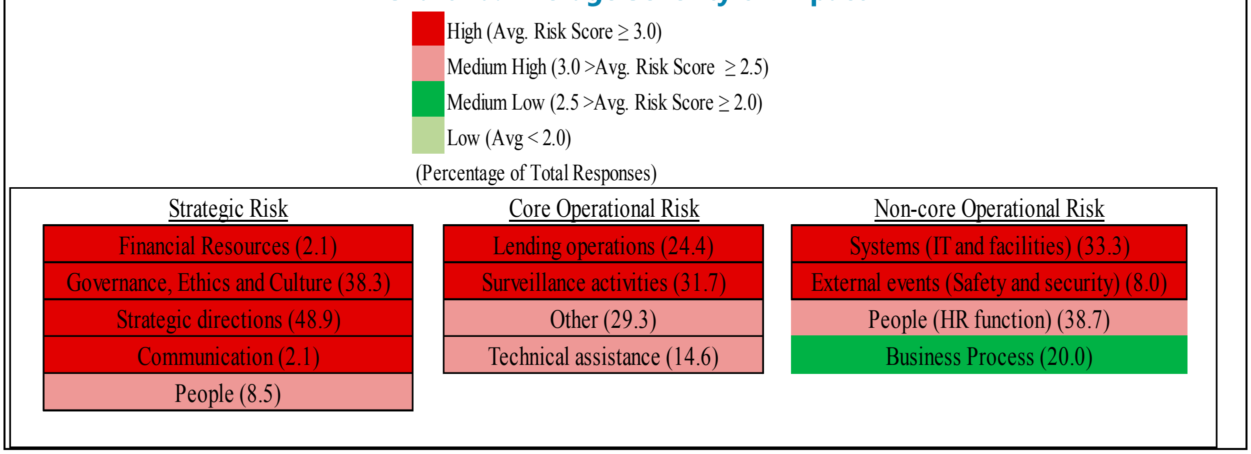
Table 1. Summary by Risk Categories, Severity of Impact and Likelihood

Severity \ Likelihood	1 -Very unlikely but not negligible	2 - Unlikely but possible	3 - Likely	4 - Very likely/Almost certain	Subtotal
A: Minor Impact	**2**				**2**
Non-core Operational Risk	***2***				***2***
Business Process	2				2
B: Medium-Low Impact	**3**	**18**	**15**	**3**	**39**
Strategic Risk		***4***	***6***		***10***
Governance, Ethics and Culture		2	1		3
People			2		2
Strategic directions		2	3		5
Core Operational Risk	***1***	***3***	***3***		***7***
Other	1	1	1		3
Surveillance activities		2	1		3
Technical assistance			1		1
Non-core Operational Risk	***2***	***11***	***6***	***3***	***22***
Business Process	1	3	1	1	6
External events (Safety and security)				1	1
People (HR function)		5	5		10
Systems (IT and facilities)	1	3		1	5
C: Medium-High Impact	**11**	**32**	**33**	**7**	**83**
Strategic Risk	***2***	***9***	***8***	***2***	***21***
Communication		1			1
Governance, Ethics and Culture	1	3		1	5
People		1	1		2
Strategic directions	1	4	7	1	13
Core Operational Risk	***1***	***10***	***11***	***1***	***23***
Lending operations		3	2		5
Other		3	3	1	7
Surveillance activities	1	2	3		6
Technical assistance		2	3		5
Non-core Operational Risk	***8***	***13***	***14***	***4***	***39***
Business Process	4	1			5
External events (Safety and security	1	1	2		4
People (HR function)	1	5	6	3	15
Systems (IT and facilities)	2	6	6	1	15
D: Serious Impact	**2**	**25**	**8**	**4**	**39**
Strategic Risk		***12***	***3***	***1***	***16***
Financial Resources		1			1
Governance, Ethics and Culture		7	3		10
Strategic directions		4		1	5
Core Operational Risk	***1***	***6***	***3***	***1***	***11***
Lending operations		3	1	1	5
Other	1		1		2
Surveillance activities		3	1		4
Non-core Operational Risk	***1***	***7***	***2***	***2***	***12***
Business Process		1		1	2
External events (Safety and security)			1		1
People (HR function)	1	3			4
Systems (IT and facilities)		3	1	1	5
Subtotal	**18**	**75**	**56**	**14**	**163**

A. Average Severity of Impact

4. **Chart 1a illustrates the subcategories of risk that were of the highest concern in terms of the severity of impact**. Although eight subcategories suggest an average severity at least of medium-high impact, five carry particular weight in terms of the frequency of responses: governance, strategic directions, lending operations, surveillance activities, and systems (IT and facilities) with the first four among strategic or core operational risks. Human resource issues are seen as of medium-high impact, principally among noncore operational risks.

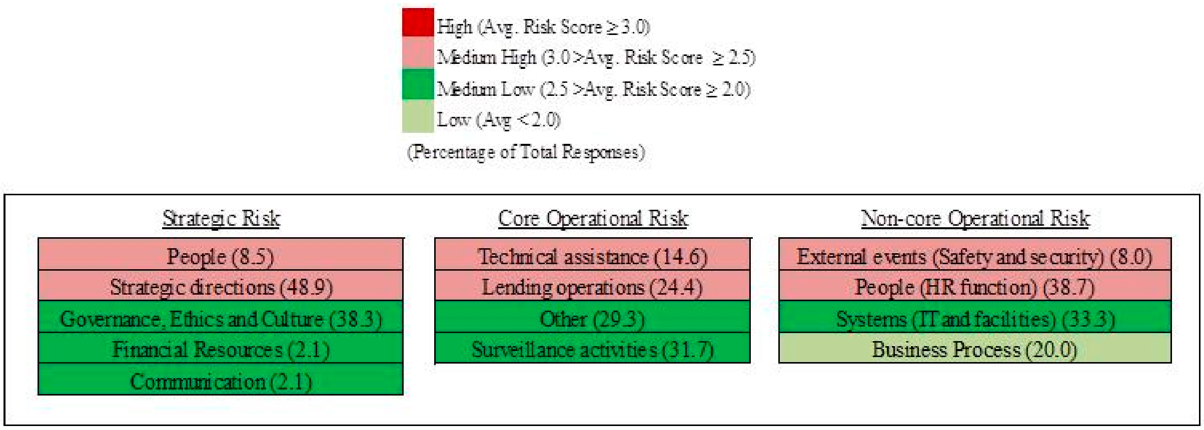
Chart 1a. Average Severity of Impact



B. Average Likelihood of Occurrence

5. **Chart 1b illustrates that none of the subcategories of risk are perceived, on average by all respondents**, as very likely or almost certain. However, six subcategories are rated as of medium-high likelihood (not seen as "likely" but more than "unlikely but possible") among the sample of respondents. In terms of frequency of responses, four subcategories are most frequently cited—strategic directions, lending operations, human resources, and technical assistance. Such risks that were seen above as particularly severe in impact, particularly surveillance, governance, and IT were viewed, on average, as of medium-low likelihood.

Chart 1b. Average Likelihood



C. Average Risk Intensity

6. **Drawing on these results to estimate average risk intensity (the product of the measures of likelihood and severity, as seen in Figure 1 in the text**), only lending operations achieves a high-risk intensity score of over 8.5, in contrast to 2012 where governance was also rated of high intensity. As noted, such lending risks relate to the various ways in which the Fund's involvement with lending to Europe could adversely affect the Fund's strategic, core, financial, and reputational interests. What is striking however is the number of other risks across the spectrum of the Fund's operations that are seen as of medium-high risk intensity. Within strategic risks, the two most frequently cited relate to governance and strategic directions (with risk intensities of 7.72 and 7.65), and with the frequency of responses largely mirroring that observed in 2012. Among core operational risks, in addition to lending, surveillance, technical assistance, and other issues (human resource challenges, etc.) are all cited with significant frequency (and with risk intensities of around 7-7.5). Among noncore operational risks, human resource and IT risks are also cited (with risk intensity of around 7-7.3). Personal security risks (7.8) receive a high-risk intensity measure, though noted by only eight percent of respondents with regard to noncore operational challenges. Finally, some expressed concern about key-person risks associated with a sudden, unanticipated change to the Fund's management team.

D. Perspectives on Risk across Department Types

7. **Among strategic risks, the principal difference among department types is the magnitude of the risk intensity that they attach** to the two principal strategic risks—governance and strategic directions—and the frequency with which these risks are mentioned. While area departments are particularly seized by the concern that the Fund may be missing key strategic risks

and see this as a high risk, functional and support departments perceive the level of risk intensity as lower. Though the frequency of expressed concern about governance was similar across departments, again area departments saw the risks as having much higher risk intensity (with functional departments next in terms of their perception of risk intensity). Support departments were more likely to see human resource risks as posing a strategic risk to the Fund, though with only medium-low risk intensity (though such risks are also seen by most departments as independently posing a noncore operational risk).

8. **Among core operational risks, there was again substantial convergence on the risks associated with the Fund's lending programs (see Chart 2b),** with functional departments more concerned (with risk intensity over 8.5) than area and support departments. Equally, the different departments responded with about the same frequency in expressing concern about the risks associated with surveillance, but again with marked differences in the perceived risk intensity (with area departments least concerned and support departments most concerned). Not surprisingly, the functional departments were more frequently commenting on the risks associated with technical assistance, and seeing these risks as of medium-high intensity. Interestingly, area departments attached a high-risk intensity to "other core operational risks." The most severe of these were associated with "budget and staffing constraints eroding their ability to conduct timely and effective bilateral surveillance and crisis prevention work." As one department noted, there is a risk "that we will overpromise and under deliver."

9. **Since departments were asked to identify those noncore operational risks that bore principally on their own departmental functioning**, a greater variance in perspectives would not be surprising (see Chart 2c). Area departments emphasized the high-risk intensity associated with safety and security issues. IT risks were noted by all department types, but again with area departments emphasizing that these are both likely and severe in impact. Half of area and functional departmental responses as to noncore operational risks were associated with human resource constraints, which are universally seen as of medium-high risk intensity. Though less frequent (12-25 percent of responses by each department type), business-process risks are equally seen as of medium-high risk intensity.

Chart 2a. Strategic Risks by Department Type

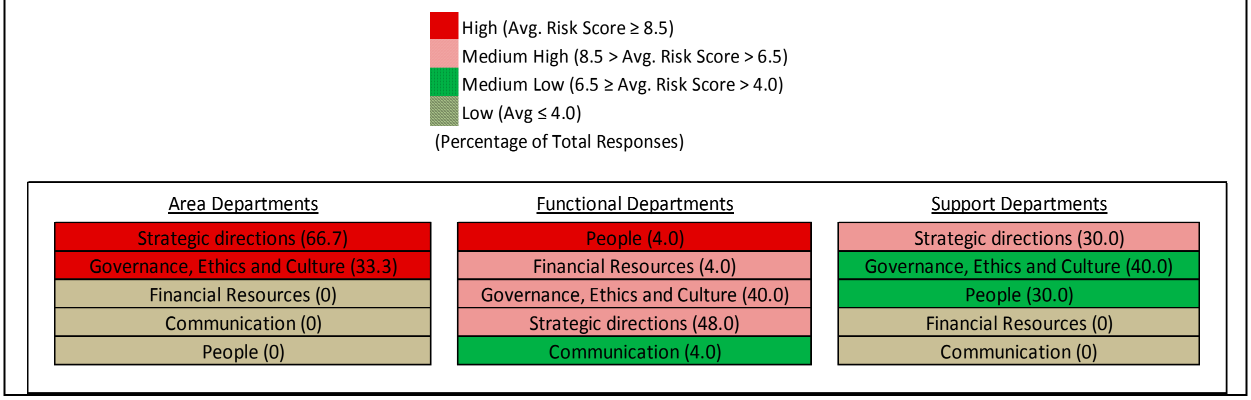


Chart 2b. Core Operational Risks by Department Type

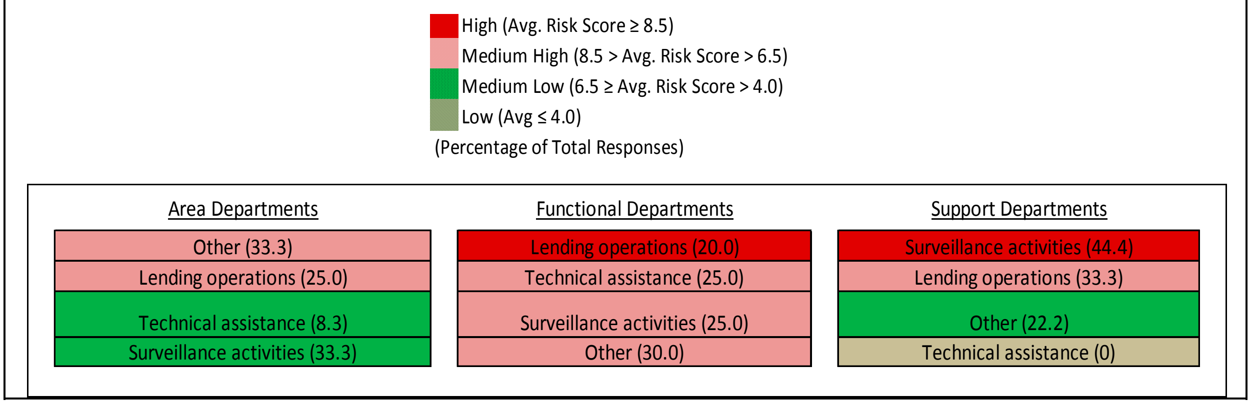
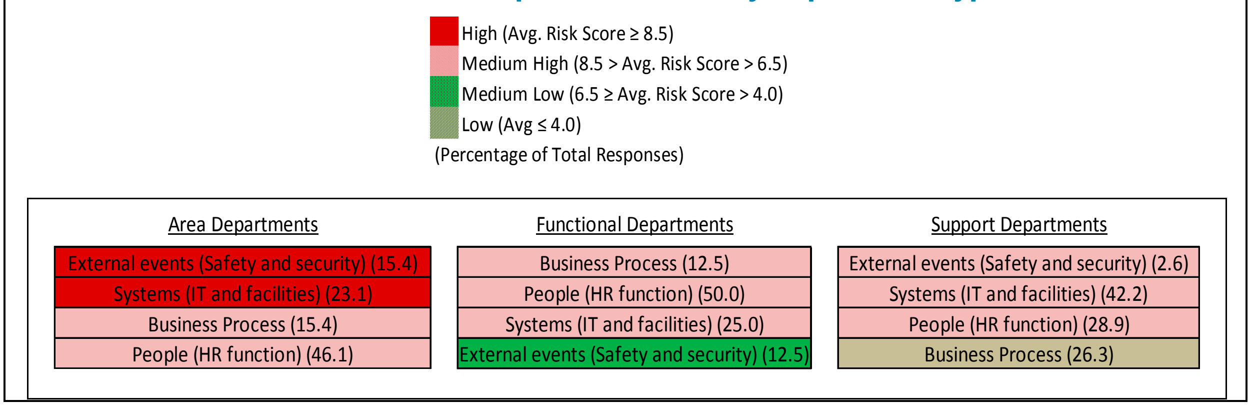


Chart 2c. Noncore Operational Risks by Department Type



E. What are the Substantive Dimensions of the Key Risks Perceived by Fund Departments?

10. **This section elaborates on the discussion of perceived risks identified by departments in the survey and briefly summarized earlier in the text**. Some of the responses are specifically quoted, in order to yield a better sense of the texture of the expressed concerns. These risks often overlap. Human resource constraints are often mentioned as contributing to the Fund's weakness in addressing strategic risks. Equally, risks associated with how the Fund responds to evolving global challenges appears as much in the category of strategic risks as in the category of core operational risks.

Strategic Risks

- **European members are seen as having excessive weight in the Fund's decisions relative to their global economic power**. This can create perceptions of a lack of evenhandedness, provoke doubts about the Fund's legitimacy, and lead to a perception of unresponsiveness to the interests of other members. Weak governance may also lead to poor policies, if they are determined less by economic merit and more by voting weight. The longer these governance issues remain unresolved as the economic weight of emerging market countries grows "divisions among Board members could threaten the consensus-based culture of the Fund and make it more difficult to adjust its policies to new challenges."

- **Concerns that the 2010 quota and voice reforms** are off-track further contribute to the severity of the above risk. Relative to 2012, one can observe a perception of a higher severity of impact from this risk.

- **The failure to adjust the governance structure** may constrain both the Fund's mandate and its capacity from evolving in response to the changing nature of the international economic problems confronting the global economy (e.g., financial sector interconnectedness, the economic risks associated with climate change; inadequate job growth).

- **Departments expressed concern that the Fund could lose credibility and legitimacy** if Fund-supported programs fail; already the Fund suffers from perceptions that these programs are "ill-conceived, harsh, and off track, with a squeezing of the resource envelope for work on "traditional clients." Further, the possibility of failed programs could jeopardize the Fund's finances. There is also the potential of inadequate access of larger LICs to Fund resources in the event of severe adverse shocks.

- Increasing public doubts about the efficacy of macroeconomic policy tools could impair the "Fund's standing and effectiveness," given that it is seen as the world's prime macroeconomic institution.

- Two departments noted the risk of inadequate financing of the Fund in the event of another crisis; others expressed concern about an inadequate workforce and employment strategy.

Core Operational Risks

- **Fund-supported programs, particularly in Europe, are at risk of failure**; in addition to the issues noted above, difficulties in coordination with the EU could lead the Fund to be sidelined and lose clout in its policy advice for euro area countries. Concerns were also expressed about the impact of the European crisis on the economies of euro periphery countries.

- **A severe and almost certain risk was also noted** if Middle East programs fail to stabilize economies and restore growth; similarly medium-high risks (though unlikely) are associated with some high-profile Asia programs due to political factors.

- **Surveillance could miss critical risks:** the most severe and likely being the failure to be ahead of the curve in considering the economic challenges from key tail risks (e.g., the possibility of a hard landing in China risks) or the implications of long-term issues. Other surveillance risks include a lack of policy traction in surplus countries; the potential for the ongoing fiscal/financial crisis to spread to Japan; failure of the Fund to play a prominent role in enunciating a strategy to promote jobs and growth; and mixed messages from the Fund on key policy issues in the context of multilateral surveillance. Human resource constraints challenge the quality of output and constrain the Fund's capacity for innovative thinking in identifying future crises.

- **The crisis has weakened the Fund's analytic capacity to think about the "next crisis.":** As one department noted, "crisis fatigue, ongoing resource constraints, and overworked staff with limited prospects for career development are challenging the quality of output and constraining the innovative thinking needed to develop tools to identify channels of future crises."

- **Technical assistance:** Some respondents also noted the medium-high impact associated with inadequate internal and external financing of technical assistance as well as limits on staffing. Disruptions in ongoing TA delivery can arise due to shifts in or withdrawals of external financing (e.g., reflecting changing donor priorities or donor funding constraints). These factors may limit the Fund's ability to meet additional TA demands from new and existing crisis countries attempting to implement IMF structural reform objectives. Effective backstopping of TA delivered by RTACs is seen as particularly challenging.

Noncore Operational Risks

- **Deteriorating staff morale:** many respondents noted the consequences of poor staff morale arising from pay constraints, limited promotion prospects, and excessive work pressures and the impacts on staffing, turnover, and retention of a skilled, knowledgeable and diverse work force. One department viewed the impact of budget constraints in constraining its ability to deliver core outputs as a severe and virtually certain risk.

- Loss of sensitive material, reputational risks, and operational risks associated with a possible repeated **IT breach from cyber attacks** and **unreliability of IT systems**.

- Despite strengthened security policy, **personal security risks** are still of concern from political instability or terrorist attacks. Volatile political security and social conditions in some countries could both expose staff to life-threatening situations and result in significant financial costs to the Fund.

- **HQ1 renewal project-related risks**, including highly likely negative reactions to cost, potential delays, disruptions to the Annual Meetings, the impact on staff productivity, and unanticipated issues (e.g., budget, security, and safety) may expose the Fund to severe criticism and disrupt operations.

- **There remains the potential for an ethics scandal** (with a severe impact, though most see it as unlikely in occurrence).

- Risks arise from an outdated Fund **employment framework**, in particular, the four-year limit on contractual employees presents the risk that the Fund will lose trained staff and fail to deliver on core work