FOR AGENDA

SM/12/199

July 20, 2012

To: Members of the Executive Board

From: The Secretary

Subject: **2012 Report on Risk Management**

Attached for consideration by the Executive Directors is the 2012 report on risk management, prepared by the Advisory Committee on Risk Management (ACRM), which is tentatively scheduled for discussion on **Wednesday, August 1, 2012**. Issues for discussion appear on page 23. The circulation of this paper has fallen short of the three-week circulation period owing to competing work priorities of the ACRM's various contributors delayed preparation of this paper.

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

Questions may be referred to Mr. Kincaid (ext. 37356) and Mr. Nelson (ext. 38132) 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 and reliability risks; Mr. Trines, OBP (ext. 35639) 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

INTERNATIONAL MONETARY FUND

2012 Report on Risk Management

Prepared by the Advisory Committee on Risk Management

July 18, 2012

Contents Page

I. INTRODUCTION

1. **This report presents an overview of the principal risks facing the Fund as assessed by the Advisory Committee on Risk Management (ACRM).**[1] This report is based primarily on the risk management framework established in 2006 and subsequently modified (see Box 1). However, two enhancements to recent Reports have been made. One, a departmental risk survey was reinstituted to identify major risks facing the Fund. Two, utilizing the survey plus incident reports, the ACRM narrowed the focus of this Report to four key risks rather than continuing the previous more comprehensive approach. Both of these changes are consistent with the views expressed by Executive Directors at the Board meeting on the 2011 Report on Risk Management and the External Panel's Report.

2. **The previous annual report (SM/11/101) was discussed by the Executive Board in June 2011 (BUFF/11/87)**. 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. As regards core operational risks, Directors agreed that the main program-related risks were credit and reputation and noted the importance of effective design and monitoring of the Fund's lending instruments and individual country programs. They also broadly agreed that the balance of financial risks had shifted toward credit risk, while liquidity and income risks had receded. Focus was placed on the importance of strengthening network security and addressing the increase in HR-related risks. Directors anticipated the completion of the External Panel's review of the Fund's risk management framework and the prospect of a Board discussion of its report. Many Directors called for an enhancement of the Board's engagement in risk management. A number of Directors called for better prioritization of the key risks facing the Fund in the context of future annual risk management reports.

3. **In November 2011, the External Panel submitted its Report to the Managing Director who in turn immediately shared it with Executive Directors** (FO/DIS/11/232). An informal Board session was arranged in January 2012 to allow Executive Directors the opportunity to discuss with Panel members their findings and recommendations. In March 2012 to take the next steps to further strengthen the Fund's risk management, the Managing Director announced the launch of a Working Group on the Fund's Risk Management Framework. This work would be overseen by Messrs. Lipton and Zhu (FO/DIS/12/29). The Working Group (WG) is composed of staff serving in their personal capacities. Under its terms of reference, the WG is to make concrete proposals to address key recommendations of

---

[1] The ACRM is chaired by Mr. Min Zhu, Deputy Managing Director, and consists of senior staff representatives from: OBP, ICD, WHD, FIN, SPR, EXR, and HRD. OIA serves as the Committee's Secretariat.

the External Panel and to examine the potential role of quantitative analysis in the Fund's management of financial risks, drawing notably on the experience of the private sector. An informal briefing on risk management developments by the ACRM and WG chair was conducted on June 21, 2012.

4. **The ACRM has also followed 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 recently posted on its website its report on risk management by the European Central Bank (ECB). The annual IFI operational risk management forum took place on May 30–31, 2012. It was organized by the Asian Development Bank and attended by nine IFIs, mainly multilateral development banks. Topics included: recent Basel initiatives, IFI insurance practices, maximizing key risk indicators, causal mapping of incidents, risk and control assessment methodologies, and model validation.

5. **This report is organized as follows**. Section II presents the main conclusions drawn from an analysis of incident reports and the main results of the 2012 Departmental Risk Survey. (An appendix provides fuller detail on the survey results.) This risk survey allowed the ACRM to identify the four principal risks identified as facing the Fund and to ask for further drill down by relevant departments. The four identified risks are related to: (i) Fund–supported programs in Europe; (ii) governance and legitimacy; (iii) IT security and reliability risks; and (iv) risks arising from human resource and budget constraints. Each risk is examined in turn in a separate section. The final section presents some issues for discussion.

II. Incident Reports and Department Risk Survey

A. Incident Reporting

6. **Incident reporting is an important risk assessment tool**. The reporting, cataloguing, and analysis of incidents serve several key functions. One, it provides a snapshot of past problems (a lagging indicator). Over time, the cataloguing and subsequent analysis of incidents allows 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—root cause analysis; and the implementation of procedures to reduce the likelihood of future incidents. Two, incident reporting sensitizes staff to the importance of a rapid and tailored response according to the severity of an incident. Three, it de-stigmatizes the reporting of incidents thus enhancing the risk management culture. Finally, a sharing of experiences across organizational units breaks down silos and improves preventive actions. At the same time, any additional benefit of more formalized incident reporting requirements needs to be weighed against the costs, including the potential that it will become a routine exercise and

lose the ability to pick up evolving risks. A low-cost system with some form of flexibility is thus desirable.

Box 1. 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. **Non-core 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).

- **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.

Box 1. The Fund's Risk Management Framework (continued)

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

[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.

[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), *and 2011 Report on Risk Management* (SM/11/101); BUFF/11/87).

7. **The Fund's incident reporting system has been enhanced during the last year.** (Box 2 contains a summary of the Fund's incident reporting methodology.) One, reporting coverage is now more comprehensive, including all departments and offices. Field offices (i.e., resident representative offices, Regional Technical Assistance Centers, and overseas training centers) are reported by the relevant area department or ICD. Two, guidelines have been clarified to encourage reporting only of major incidents. (For example, TGS reduced its reporting of low-severity incidents deemed minor, such as complaints of odor or noise.)

This new guidance combined with expanded coverage has made comparisons of the number and nature of reported incidents from earlier periods more difficult. Looking forward, comparability should improve with greater stability in coverage and reporting thresholds. Nonetheless, serious incidents are the most clearly defined and are the most consistent and well recorded; hence they are considered the most reliable. Serious incidents are typically also reported to the Executive Board. Three, a SharePoint application for incident reporting was developed and distributed to departments by the ACRM secretariat. In addition, training was made available. Four, to increase departmental awareness of incident reporting and its uses, the ACRM chair circulated in July 2011 a short note to all department heads. The most recent incident report has been also distributed to heads of departments and offices following its discussion by the ACRM.

Box 2. Incident Reporting Methodology and Departmental Practices

The incident reporting survey covers all departments and offices, in order to obtain a comprehensive view of incidents at the Fund level, including for overseas offices. Area departments were asked to include in their incident reports relevant occurrences in their resident representative offices and Regional Technical Assistance Centers (RTACs), and the Institute was asked to report incidents of the overseas training centers. Reporting guidelines were clarified to encourage departments and offices not to report minor incidents focusing instead on major operational risks, including their involvement in remediation, if any. The ACRM has defined tentatively what constitutes an "incident" and three 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. Near misses are events characterized by pre-emptive action that averted what would, or could otherwise have been, a serious or less serious incident.

These reporting practices are consistent with the advice of the External Panel for the Review of the Fund's Risk Management Framework. The Panel commented in its November 2011 report that "vis-à-vis risk assessment, the goal should be to employ a parsimonious list of tools that are both effective and contribute to an institution-wide appreciation of the benefits of risk management. Three tools of choice, at varying stages of development in the Fund, stand out…The third is incident reporting systems, which are gaining traction in many institutions. The Fund's system is in its early stages, and experience should be reviewed to design any needed changes."

Departmental practices for incident collection and classification remain varied. Incident collection practices remain comparable to those observed during the previous reporting period. Certain departments surveyed do not appear to maintain and document incident logs on a periodic basis. EXR, FIN, HRD, MCM, OBP, OIA, SEC, TGS, TGS-IT maintain incident logs on an ongoing basis, either web-based, Word templates, or on Excel spreadsheets or databases. SPR does not formally log incidents, but monitors incidents during the twice-weekly meetings of the front office and division chiefs. OMD set up a SharePoint log in February 2011. Other reporting departments (AFR, APD, EUR, FAD, LEG, MCD, OTM, RES, and WHD) do not maintain ongoing logs and report on an ad hoc basis via email. The now-merged INS/OTM departments mentioned that they will look to combine their respective reporting mechanism into one common system.

Differences in incident classification noted during the previous reporting periods remain applicable. For example, FIN and HRD employ three tiers of severity categories (i.e., serious, less serious, and near miss) as developed by the ACRM, while TGS and TGS-IT utilize specific criteria, such as the length of disruption to building operations, closure of overseas offices and impact on missions, or the length of outages. Some departments do not report any classification criteria. The disparity of reporting methods, incident classification, and the lack of a centralized incident reporting database still make the counting and classification of incidents a manual, time consuming process. On the other hand, a consistent six-month reporting period has been adopted by the ACRM, starting with this cycle. Serious incidents are the most clearly defined and recorded and hence are the most reliable.

8. **During the 12-month period ending in March 2012, reported serious incidents averaged less than two per month with a lower incident pace during the second six-month reporting period.** Such incidents involved threats to the physical security of staff, information leaks, IT problems including a major breach, and process errors (e.g., transfer to investment account, inaccurate IFS data). Less-serious incidents are far more numerous than serious incidents—averaging over 25 items per month and also were less frequent during the second six-month reporting period. Less-serious incidents typically pertain to building-service problems (e.g., elevator), particularly in HQ1, minor business outages, and overseas security problems.

9. **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 2011—285—doubled over those received in 2010, in part reflecting outreach by the Ethics Office. Categories of reports included the following: Requests for Information, email scams, substantive allegations, and other miscellaneous reports. The Hotline received 19 substantive allegations during 2011—a significant increase over the six substantive allegations recorded in 2010. These 19 allegations covered a wide range of issues. However, 17 allegations were closed due to insufficient information, informal resolution, no finding of ethical misconduct, or referral to another office. Only two allegations merited investigation by the Ethics Office.

10. **Looking forward, the ACRM has a modest agenda with respect to the further development of risk management tools, which is viewed as the purview of the Working Group on the Fund's Risk Management Framework**. With respect to incident reporting, efforts will center on improving the definitions employed for various incident categories to ensure a more consistent Fund-wide application including a suitable minimum threshold. As regards the latter, several IFIs employ a minimum threshold of US$ 5,000 or € 5,000. It might be useful to have more explicit department tolerances, which could vary depending upon the type of business activity. Turning to key risk indicators (KRIs), no progress was made by the ACRM in their further development since the 2011 risk management report, owing primarily to the fact that efforts were focused on incident reporting and supporting the External Panel. Nearly all IFIs reported in the 2012 benchmarking exercise that they utilized KRIs as a risk management tool.

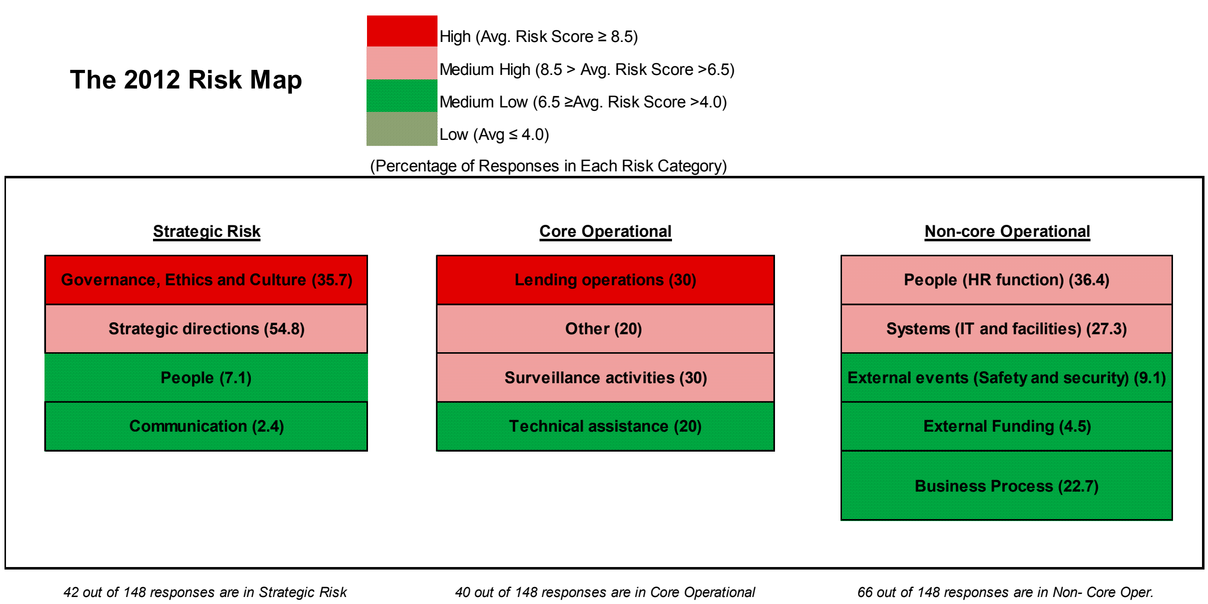
B. The 2012 Departmental Risk Survey

11. **After having been suspended since 2009, the ACRM conducted a streamlined departmental risk survey in early 2012**. 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 a more open-ended manner than previous surveys, but sought to focus more sharply on the most important risks. 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. Each self-identified risk was assigned a rating using a four-point rating scale for degree of impact severity and the likelihood of occurrence, taking account of any mitigating actions that had been implemented. A four-point scale was employed in previous surveys, avoiding excessive use of the middle rating associated with three and five point scales. A four-by-four matrix results from this process as well as an ordinal ranking 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.

12. **The survey responses from 21 departments and offices identified 148 individual risks.** Given the open-ended format, some responses while not identical clearly overlapped. As regards their distribution, strategic and core operational risks had roughly the same number (42 and 40, respectively); non-core operational risks totaled 66 entries. In terms of risk intensity (Figure 1), six risks stood out: those relating to lending (with risk intensity of 9.3), Fund governance (8.7) and concerns about the Fund's strategic direction (7.9). Concerns about "strategic direction" related principally to the consequences of the Fund's involvement in Europe for the Fund's reputation and credibility, its financial position, its overall effectiveness, and its even-handedness. Three other risks also received significant attention: concerns about effectiveness in surveillance (notably, the potential for an excessive focus on European issues to result in missing other risks elsewhere or inadequate surveillance in other regions) (7.3), and two non-core operational risks—people (or human resource issues) (6.9), and a possible breach of the Fund's IT system (6.8).

Figure 1. 2012 Risk Map



13. **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 most likely (2.7). The other two risks perceived with potentially high to serious impact (3.3)—specifically, concerns about **governance** and **strategic directions**—were seen as marginally less likely than the risks associated with lending, but still close to likely (2.5). As can be seen from the figure, the other three concerns noted above—HR, IT, and surveillance—preoccupied respondents, but with significantly lower perceptions of potential severity—(somewhere between medium-low and medium-high impact)—or potential likelihood (somewhere between "unlikely but possible" and "likely").

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

Strategic risks

- The risk that governance reforms (and the 14th General Review of Quotas) might not be enacted by the 2012 Annual Meetings was frequently cited along with lack of progress on a new quota formula.

- Departments also expressed concern that too much attention was paid to European issues, that program design for European members might not achieve their objectives, and that implementation fatigue might set in. Concerns were expressed about insufficient engagement outside of Europe and that the Fund might not therefore meet the expectations of its entire membership, possibly missing emerging vulnerabilities elsewhere. Some also worried that surveillance reform was not having a sufficient impact.

Core operational risks

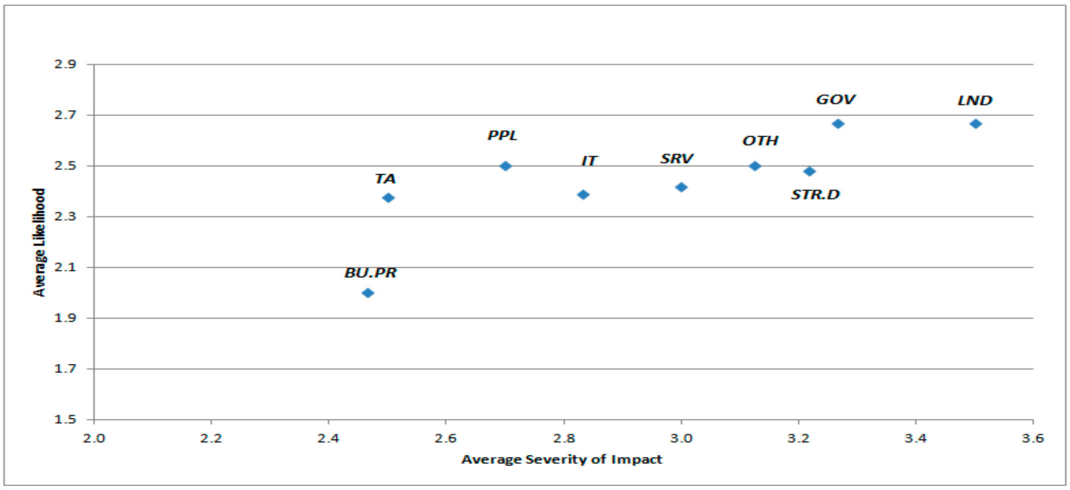
- **Problems could arise from Fund-supported programs with euro area members.** In particular, their various program targets might not be achieved within the specific time period and other euro area members may need financial assistance. These developments were seen as giving rise to risks to the Fund's overall credibility, to the global economy, and to the Fund's finances.

- **The possibility of surveillance missing tail risks** (e.g., the risk of failure to identify the precise timing of a possible hard landing in China and organize a timely response to such an event, other emerging crises) or key developments in other regions.

- **Other surveillance-related concerns** related to the pressure to reform bilateral financial surveillance, the potential for the Fund to give poor advice because of heavy workloads and time pressures, and a concern that the proliferation of multilateral surveillance products might muddy key policy messages.

Distilling these various concerns, two principal risks dominate, namely, those relating to governance and legitimacy and the range of risks that are the potential consequence of the Fund's intense involvement with euro-area members. The latter affects both the financial risks to which the Fund is exposed (credit and liquidity risks), and ultimately its reputation (to the extent that the Fund's bilateral and multilateral surveillance suffers) as well as its capacity to meet expectations in other regions in surveillance, program design, and program implementation.

Figure 2. Perceptions of Severity of Impact and Likelihood



BU. PR	Business Process	STR. D	Strategic directions
SRV	Surveillance activities	GOV	Governance, Ethics and Culture
IT	Systems (IT and facilities)	LND	Lending operations
TA	Technical assistance	OTH	Other
PPL	People (HR Function)		

Non core-operational risks

- **IT concerns** principally reflected the risk of a security breach leading to a loss of sensitive material, reputational risk, or an inability of IT systems to handle the Fund's operational workload, particularly that associated with financial transactions.

- Departmental concerns with regard to **business processes** ultimately seem to have their root cause in constraints posed by human resources and budget pressures. On the human resource side, a heavy focus emerged on the adverse implications of quality, skill mix, and work pressures. Budgetary concerns were also seen as having potential impact on the Fund's technical assistance activities; some departmental respondents noted the consequences that could arise if external donors fail to renew their funding of the Fund's TA program or impose constraining conditionality on the use of TA resources.

- **Human resource risks,** when elaborated, ultimately, centered on two risk areas: concerns about **staffing pressures** included staff being drawn away to work on euro-area issues, poor morale, poor promotion prospects, inadequate salary levels, inability to compete for the best staff, failure to deliver on promised output, and excessive work pressures giving rise to errors. The salary pressures could have ramifications on the ability of the Fund to compete in the market for high quality staff. Mention was also made of an **outdated employment framework** itself risking the loss of experienced staff (e.g., the four-year limit on contractual staff), the lack of new staff positions, the loss of qualified experts, and the poor prospects for promotion.

III. EUROPE-RELATED RISKS[2]

15. **Risks related to Fund-supported programs are heavily concentrated in Europe, as are risks to global growth**. A few large programs with euro area members, in particular, present elevated operational, credit, and reputational risks. The primary tools for managing these risks are the Fund's policies on access, program design and conditionality. The Fund has 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 space allows, and streamlined conditionality to secure greater ownership.

Concentration of risks

16. **Risk concentration remains a concern, given the substantial increase in lending to euro area members**. Total credit outstanding and total commitments have both reached new highs: credit outstanding has risen from SDR 65.5 billion at end-April 2011 to SDR 94.2 billion at end-April 2012, while undrawn GRA commitments also increased from SDR 116 billion on May 1, 2011 to SDR 121 billion on May 1, 2012, reflecting the approval of new programs that are expected to be drawn. This credit exposure is highly concentrated, with commitments under current programs with European members accounting for 64 percent of current Fund arrangements and 75 percent of total GRA credit outstanding as of end-May 2012 under current arrangements (up from 61 percent and 65 percent, respectively, as at the same time last year). These levels of concentration on Europe are higher than the share of outstanding credit to Asia during the Asian crisis and Latin America during its debt crisis.

17. **Risks from euro area programs arise from different factors, and require policy response both from program countries and the euro area as a whole**. There are risks from reform fatigue and political ownership, employment and inflation dynamics, divergence in competitiveness, and lack of independent monetary and exchange rate policy. In the absence of fiscal and banking unions, the burden of adjustment is on the individual members rather than being shared with the union as a whole. The Fund's engagement in Europe carries

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

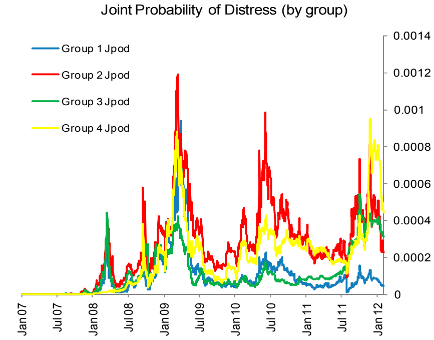
significant reputational risks that would materialize if these programs encounter difficulties or prove unsustainable. While the easing of funding tail risks, owing to ECB liquidity operations, and progress toward fiscal and structural reforms helped stabilize market conditions briefly, markets remain volatile due to political uncertainties, including about the ability of European policymakers to bring about a durable resolution to the euro area crisis, even after the recent Greek elections. The Fund, in the context of the euro area consultations, has discussed policies aimed at limiting these risks, emphasizing the importance for financial support from European partners, as well as progress toward a fiscal and banking union. More generally, going forward, program design for members of currency unions will need to take a case-by-case approach that reflects the architecture of the currency union.

18. **The modification of the second exceptional access criterion in 2010, in the context of the program for Greece, has increased the potential for credit risk.** This modification—which was already discussed in last year's report on Risk Management—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. Arrangements have also been approved on the basis of this policy modification for Ireland and Portugal. But this change has resulted in an increased risk that these Fund arrangements will not engineer a sufficient improvement in the balance of payments to allow these members to regain viability over the program periods. It has also highlighted the difficulty the Fund faces in anticipating and quantifying the likely extent of contagion. This should become a focus of ongoing risk management efforts. Finally, it should be underscored that members' capacity for timely repayment of the Fund will hinge critically on their ability to regain access to international capital markets, the prospects for which remain uncertain, as well as continued support from European partners.

Correlation of risks and potential spillovers

19. **Risk concentration increases the risks from contagion and/or common shocks, a concern particularly relevant for members of a currency union**. Studies suggest that deterioration in Europe's periphery, driven by funding strains and possibly accompanied by deposit runs, could cause additional write-downs on sovereign bonds and other credit losses, leading to higher solvency risks of systemically important financial institutions (SIFIs) in core European economies, with consequent impacts on Fund members elsewhere in Europe and beyond. Indeed, the spillovers from contagion are likely to be bigger since the stress in the periphery seems to be migrating to the euro area core.

Joint Probability of Distress (by group)



Note: Group 1: U.S. LCFIs; Group 2: European LCFIs; Group 3: Asian LCFIs; Group 4: European LCFIs with significant exposures to Eastern Europe.
Source: Fund staff estimates.

20. **An intensification of the European crisis would likely have implications for the Fund as well as individual members**. A deterioration of European conditions would likely result in additional demand for Fund-supported programs, in Europe and beyond, propagated through both real sector and financial channels, including deleveraging by European banks. In many low-income countries (LICs) a deteriorating situation in Europe, coupled with more limited policy space, would contribute to a more severe overall economic impact. Falling exports, remittances, and foreign direct investment would result in significant external financing needs of LICs, which could result in additional calls on Fund resources. For the Fund itself, risks would relate to the need for program redesign in existing arrangements, possible need for augmenting existing arrangements, and the adequacy of the Fund's liquidity (i.e., lending capacity) and precautionary balances. Difficulties may also arise in raising additional financing for the Fund's concessional financing lending to LICs, as aid budgets in the more advanced countries come under greater pressure.

Management of program-related risks

21. **Program risks are being monitored closely**. Given the potential risks associated with slippages of Fund-supported programs, both in terms of the Fund's credit risk, and in terms of spillovers to other members, all Fund-supported programs, particularly those presenting heightened risks, are subject to reviews. In the case of European programs, the Fund has also made adjustments in the face of ever-changing events, to strengthen the chance of ultimate success. The lengthening of maturity under the new Greece program is one example. In addition to individual program reviews, reviews of developments across all programs have been undertaken regularly. The Crisis Program Review (FO/DIS/12/106) allowed the Board a more focused look at the way Fund programs have been designed and implemented during the current crisis. The Review of Conditionality (SM/12/148) assesses the effectiveness of recent reforms of conditionality, as well as analyze program design and outcomes across countries. The Board will also be given many opportunities to follow progress in the context of surveillance, and informally through regular briefings by staff, as noted in the Work Program.

Management of credit and liquidity risks

22. **The Fund employs a multi-layered framework for managing credit risks.** The role of the Executive Board in monitoring and managing the Fund's financial risks is summarized in Box 3. The primary tool is the strength of Fund policies on program design and conditionality (including for Flexible Credit Line (FCL) and Precautionary and Liquidity Line (PLL) arrangements where ex ante conditionality through qualification plays a bigger role), 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. These policies include assessments of members' capacity to implement adjustment policies and repay the Fund, and the exceptional access framework for the Fund's largest exposures. The

framework also includes the structure of charges and maturities, safeguards assessments, requirements for adequate junior co-financing from other official lenders, the burden-sharing mechanism, precautionary balances, and the Fund's preferred creditor status.

Box 3. The Executive Board's Role in Monitoring and Managing Financial Risk in the Fund

The Executive Board is closely involved in the monitoring and management of the Fund's exposure to financial risks. The Fund faces a range of financial risks, notably liquidity, credit, market (on the investment portfolio), and income risks.

Liquidity risk

Papers on the Fund's Liquidity—Review and Outlook are issued semi-annually, and more frequently if warranted.

Proposals by the Managing Director for the establishment of an activation period under the New Arrangements to Borrow (which are subject to the approval of both Participants holding 85 percent of credit arrangements eligible to vote, and the Executive Board) must include, inter alia, information on the overall size of possible Fund arrangements on which discussions are well advanced, and additional financing needs that, in the opinion of the Managing Director, may arise during the proposed activation period.

All requests for arrangements with exceptional access are accompanied by an analysis of the impact on the Fund's liquidity, as well as the broader assessment of program risks.

In January 2012, the Board discussed a paper on the adequacy of the Fund's resources, and has recently discussed a paper on the modalities for additional bilateral borrowing and approved a modification of the Borrowing Guidelines. The Fund has recently received commitments for new bilateral loans totaling $456 billion from 37 members.

Credit risk

All Fund arrangements and reviews of such arrangements must be approved by the Board. Similarly, all waivers and modifications of performance criteria, and augmentation and changes to the phasing of arrangements require the approval of the Board.

The Board conducts regular reviews of program conditionality that focus, inter alia, on the success of Fund arrangements in promoting balance of payments adjustment. The next such review is tentatively scheduled to be considered in July 2012.

The Board conducts regular reviews of the adequacy of the Fund's precautionary balances. In 2010 the Board adopted a new framework for setting precautionary balances. In the most recent review in April 2012, most Directors agreed to raise the medium-term indicative target from SDR 15 billion to SDR 20 billion, compared to the end-April 2012 level of about SDR 9.6 billion.

Box 3. The Executive Board's Role in Monitoring and Managing Financial Risk in the Fund (continued)

Market risks

The Fund does not face significant market (exchange and interest rate) risks in its lending and funding operations with members. Market risks related to the Fund's investment portfolios are currently relatively limited given the narrow investment strategy. The Board has been closely involved with the expansion of the Fund's investment mandate in connection with the new Gold Endowment.

Income risks

The Board conducts an annual review of the Fund's income position and receives regular updates of income and budgetary expenditures.

23. **Precautionary balances are being increased in response to the elevated credit risks. At the last review of the adequacy of precautionary balances in April 2012, most Directors agreed to raise the medium-term indicative target from SDR 15 billion to SDR 20 billion, compared to the end-April 2012 level of about SDR 9.6 billion**. This took into account the sharp increase in commitments and 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 are now projected to reach the SDR 10 billion floor during FY 2013. On current projections, the proposed SDR 20 billion target would be reached in FY 2018.

24. **However, a further intensification of the European crisis would add to financial risks for the Fund.** The Fund could be called upon to provide additional financial support for euro area members, or for other member countries affected by negative spillovers from the crisis. In this regard, the Fund's capacity to respond to the needs of all its members has been greatly enhanced by the recent pledges of $456 billion in new bilateral resource commitments from 37 countries, thereby significantly reducing near-term liquidity risks. At the same time, an intensification of the crisis would add to credit risks, as 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. In these circumstances, the capacity of the Fund's existing financial mechanisms for addressing an arrears situation could 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.

Diversion of staff resources away from other areas

25. **Responding to the crisis required a rethinking of restructuring plans**. When the crisis hit in late 2008, the Fund was embarking on a major restructuring targeted to deliver, over three years, a budget reduction of $100 million in real terms and a decrease in staff of 380. Efforts were put in place to redirect resources toward EUR and other departments at the forefront of the crisis (initially MCM and SPR). A number of measures were adopted:

- **Activities were reprioritized,** including the streamlining of support and governance activities, and subsequently also of multilateral surveillance products. Over FY 2008 to FY 2012 support and governance spending declined from 40 percent of total to 29 percent in FY 2012, while lending/crisis-related spending increased from 10 percent to 15 percent, and global surveillance and oversight rose from 18 percent to 22 percent. Since FY 2009, close to $30 million in crisis resources have been provided to EUR alone. This redirection of resources is ongoing with further resources shifted to EUR in the FY 2013 budget.
- **Recruitment was stepped up**, in a partial reversal of the downsizing, through a combination of a larger EP cohort (from 15-20 pre-crisis to 45 in 2009) and hiring of mid-careers.
- **Volunteers for separation packages were deferred**, to retain key skills and help bridge the recruitment of new staff/mitigate the effect of transfers to crisis cases, and stayed on for a period of 1-2 years.

26. **Notwithstanding these steps, work pressures have led to an increase in overtime (see also Section VI)**. Measured as percent of total worked hours, overtime in crisis departments (EUR, MCM, SPR, FAD, LEG, and EXR) has increased from 11 percent in FY 2008 to almost 19 percent in FY 2012.

IV. GOVERNANCE AND LEGITIMACY RISKS[3]

27. **In December 2010, the Board of Governors approved a package of far-reaching reforms of the Fund's quotas and governance**. These reforms aim to strengthen the Fund's legitimacy and effectiveness through an unprecedented doubling of quotas, a major realignment of quota shares—a shift of more than six percent from over-represented to under-represented members, a shift of more than six percent to dynamic emerging market and developing countries, and the BRIC economies among the top ten shareholders—and protecting the quota shares and voting power of the poorest members. The Board of Governors also supported an amendment to the Articles of Agreement that would facilitate a

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

move to a more representative, all-elected Executive Board. They committed to best efforts to implement the package by the 2012 Annual Meetings.

28. **Delays in implementation could adversely impact the Fund's perceived legitimacy.**

- For the reforms to come into effect, (i) the proposed amendment to the Articles of Agreement on reform of the Executive Board needs to be accepted by at least three-fifths of IMF members representing 85 percent of the total voting power, and (ii) members representing at least 70 percent of the total quotas on November 5, 2010 must consent in writing to their quota increases. Many members need the approval of domestic legislatures to accept the proposed amendment to the Articles of Agreement.
- However, progress has been slow, in particular on acceptance of the proposed amendment. As of June 4, 2012, only 79 members (of the 113 needed) having 54 percent of the total voting power (of the 85 percent needed) had accepted the proposed Board Reform Amendment, while members having 66 percent of quotas (70 percent needed) had consented to their proposed quota increases.[4]
- If the reforms are not fully implemented by the 2012 Annual Meetings, this could also delay the voluntary re-composition of the Executive Board, which is to follow the implementation of the reforms. It entails a reduction by two of the number of Executive Directors representing advanced European members in favor of emerging market and developing countries.

29. **Risks to the Fund's legitimacy rise if the 2010 reforms are delayed.** Delay in completing the Fourteenth General Review of Quotas will postpone the rebalancing of quota and borrowed resources, thereby increasing financial risks for the Fund (quota resources ultimately back the Fund's capacity to repay its borrowing). Risks to legitimacy could also rise should the Fund have to draw more heavily on borrowed resources to make large program loans to economies facing correlated shocks. Without timely action, there is a risk that the 2012 election of EDs would take place based upon the pre-2010 voting power and that the five largest members would therefore continue to appoint their EDs. To mitigate these risks, the Board is updated on a monthly basis as to the status of acceptances, and both management and staff are actively engaging with country authorities.

30. **Delays in completing the quota formula review could also affect the Fund's legitimacy**. As part of the 2010 package, the Board of Governors called for a comprehensive review of the quota formula to be completed by January 2013. The Executive Board had an initial discussion in March 2012, and further discussions are planned. A dedicated work

[4] 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.

stream of the IMFC Deputies is also engaging on the issue. Any such a delay could also impact the next quota review, which is to be completed by January 2014.

31. **Surveillance of member countries' policies is central to the IMF's mandate, and several changes have been implemented recently to enhance its effectiveness**. In this context, there is a risk that surveillance will lose legitimacy unless it is evenhanded both in practice and perception. Insufficient progress on governance reforms could hamper the effectiveness of surveillance and hurt the reputation of the Fund. In October 2011, the Triennial Surveillance Review (TSR) was completed. The review highlighted progress since the beginning of the global financial crisis but also remaining gaps. In particular, surveillance was seen as too fragmented, with risk assessments lacking depth, and an insufficient focus on interconnections and shock transmission. Surveillance was also found to have less traction with larger members. The recommended actions focused on improvements in interconnectedness, risk assessments, external stability, financial stability, traction and the legal framework. In addition, work has begun on a new external sector report (ESR), which would examine what is driving imbalances and some of the associated risks to external stability. The ESR is also intended to bolster evenhandedness. The spillover reports, Data Gaps Initiative, the work on an Integrated Surveillance Decision and work program, and MD's Action Plan aim to address these risks.

V. Risks to IT Security and Reliablility[5]

32. **The Fund was subject to a major IT security breach by so-called "Advanced and Persistent Threat" (APT) actors**. The breach, which was detected on May 31, 2011, resulted in unauthorized access to and theft of sensitive information and in reputational damage resulting from negative media attention. In response, TGS engaged the services of a specialized IT cybersecurity company (Mandiant) to assist with the forensic analysis and the development of risk mitigation efforts. These security experts helped identify the leaked information, which was information stored on shared network drives (there was no evidence of other IT systems being accessed, including email, HR and financial systems). The information leaked was subsequently analyzed by a Working Group lead by SPR to assess the Business Impact, with IT performing an IT impact assessment and HRD performing a HR/privacy assessment. Sensitive information included details of the (i) Fund business (such as strategic issues, crisis response, surveillance, and policy work); (ii) Fund's internal operations (such as data on the IT environment and security controls); (iii) member countries and relations with third parties (such as TA reports, safeguards assessments, sensitive country cases, and confidential BTOs); and (iv) staff personal and private data (such as passport information, and bank account information if copies were stored on network drives). The assessment of SPR and departmental representatives was that most information had a relatively short critical lifespan, and thus the risk levels would drop off quickly. There has

[5] This section was prepared by TGS.

been no evidence of any of the leaked information being abused. In terms of risk mitigation, only one recommendation has not been implemented. The unimplemented one pertains to the blocking of access to uncategorized sites, which cannot be undertaken yet for technical reasons given the extensive use of Skype at the Fund.

33. **In addition to the immediate response to the breach, TGS proposed and Management agreed (a) to create a Working Group on Selected IT Security Controls that identified several controls to further mitigate risks; (b) to launch an IT security awareness campaign; and (c) to commission a comprehensive IT security risk assessment**. The implementation of controls identified by the Working Group (WG) remains in progress through the deployment of a variety of technologies: (i) technology to prevent non Fund computers or computers that are non compliant from accessing the Fund's internal network (using Network Access Control technology); (ii) technology that only allows approved applications to run (using Bit9's Application White Listing technology); (iii) technology that will scan all web and email traffic for APT malicious code (using FireEye's APT scanning tools); and (iv) technology that allows TGS to enforce stricter controls on mobile devices (using Mobile Iron's Mobile Device Management tool). The Fund-wide security awareness campaign was launched on a voluntary basis to equip staff with the knowledge and tools to identify information security threats and respond accordingly. As of May 2012, only 75 percent of Fund staff have completed the security training despite successive attempts to push for 100 percent participation. Management is considering the pros and cons of options to make online information security training mandatory, given the voluntary approach has not achieved full participation to date. As part of the WG efforts, a comparison of the Fund's IT security practices with other IFIs and agencies, including some central banks, was performed. Not surprisingly, other organizations that have experienced similar APT attacks, such as the World Bank and OECD have also moved more aggressively towards implementing security controls similar to those implemented at the Fund.

34. **The comprehensive IT security risk assessment was awarded to PricewaterhouseCoopers (PwC)** following a competitive bidding process, and PwC completed its assessment in May 2012. PwC has concluded that the Fund's current information security program and capabilities are insufficient to protect against current and future threats, exposing the Fund to possible information losses and reputational risks. Specifically, PwC feels that there is a high likelihood of another costly breach which may affect the Fund's ability to execute its mission and, most importantly, to protect its reputation. The PwC assessment, based on evaluating the design of the Fund's security controls in relation to best practices and testing a number of selective controls, found that the Fund had an unexpectedly high number of vulnerabilities. In terms of root causes, PwC's analysis identified three main areas: (i) IT security governance; (ii) people; and (iii) processes. On the other hand, PwC noted that the Fund's commitment to IT security, an established Information Security Group, and investments in key IT security technologies implemented or being piloted post last year's data breaches represented a solid foundation on which to build

upon. The PwC report identified three main areas of improvement and recommendations: (i) implement a stronger governance structure with a centralized Information Security team reporting to the CIO; (ii) start work immediately on 14 "Priority 1" projects (in particular start fixing the identified vulnerabilities immediately) with another seven to follow; and (iii) hire additional IT security staff with relevant information security skills. A presentation was made to the ACRM by PwC and the finalized report has been distributed to Management in late June. PwC's recommendations will be considered in the broader context of the Fund's IT strategy that will integrate various factors such as security, reliability, stability, and efficiency of IT systems.

35. **More generally, TGS has seen evidence that the risk of disruptive and targeted attacks on the Fund's IT systems and users indeed continues to increase**. In early 2011, the "cyber activist" group called "Anonymous" issued a call to members to disrupt the business of the U.S. Federal Reserve and other institutions such as the World Bank and the IMF. "Anonymous" has the capacity to be disruptive—mainly through large scale "denial of service" attacks that might disrupt the Fund's policy evolution or its credibility. TGS had previously contracted with a specialist firm to provide enhanced protection, leveraging their 84,000 servers worldwide to detect and block rogue traffic closer to the source. The service successfully defended against the attack. The Fund continued to come under targeted "spear phishing" attacks that were considered near misses as TGS were able to clean infected machines. For example, over the last six months, the Fund experienced attacks similar to the APT attacks that led to the IT security breach in 2012, resulting in about 40 PCs being removed and wiped. Typically, these attacks start with a well crafted, socially engineered, email that a user clicks on, resulting in malicious code being placed onto a Fund PC. TGS' new defenses are alerting the Fund to these attacks a lot faster than previously, so it has been able to contain them more effectively. Nevertheless, as PwC also warned, these attacks are becoming ever more sophisticated and today's defenses are not guarding against future attacks.

36. **Other serious incidents included unauthorized disclosure of un-cleared and sensitive information**. These include a sensitive member country document made available on an Internet file sharing website due to poor business processes used by contracted translators and disclosure of Strictly Confidential and Personal information (pay slips) via the Fund's email systems due to a malfunction of the archiving system. Reacting to the highly publicized breach at RSA that provides SecurID tokens to Fund staff for remote access, TGS re-issued new tokens to all users. Finally, the Fund had a few instances of unencrypted laptops and iPads with sensitive information lost or stolen from mission staff.

37. **Finally, in terms of reliability, there has been a lot of focus on addressing the performance and stability problems on PCs**. Fund PCs have not been performing as well as they should, and many staff are experiencing slow boot times, slowness, and crashes. The problem has been quite widespread and there has been a lot of variability. This issue is being

given the highest priority, with increased resources working on the "desktop" and several external experts having been engaged to help TGS pinpoint the principal problems. Most importantly, there has been improved measurement of performance at the individual PC level. In addition to looking at the software on PCs, there has also been focus on the performance of back-end components such as storage systems, servers and networks as these also have an impact. While significant progress has been made, especially to improve slow boot times, further improvements are needed and additional measures are in the works. In addition, while TGS has been focusing on the PC performance issues in the current environment, work is also progressing on the PC refresh, which will start with the laptop replacements late this calendar year. The PC refresh effort will be used as an opportunity to deploy a leaner, faster, and more stable configuration on faster machines.

38. **From a risk perspective, the IT security and reliability risks have a direct impact on the work pressures and reputational risks**. Staff are increasingly being asked to work more, including producing more, remotely. This has led to large productivity increases, but failure or delays in IT systems inevitably cause greater disruption. Similarly, efforts to reduce IT security risks need to be weighed against added costs in terms of budgetary resources and potential impact on overall staff productivity.

VI. Human Resource and Budget Risks[6]

39. As noted above, human resources risks and budget constraints were cited by several, although not all, departments as an important risk. Overall, the severity measure of risk perceptions (see Figure 2 and the appendix for further details) was greater than the severity measure for IT security but below that of governance and financial risks. To better understand the nature of these perceptions reported in the survey, 15 departments were asked to elaborate further on their survey responses. Based upon this additional information, it appears that workload pressures and low morale were the main drivers. Specific departmental concerns were also elaborated (e.g., excessive turnover in one department and uncertainties about external financing in another).

Workload pressures

40. **About half of the departments cited risks associated with workload pressures**. Most linked these risks to resource constraints in an environment that is imposing additional demands on the institution, including as a result of the continued global economic uncertainty, especially in Europe, associated efforts to intensify surveillance, and stakeholder demands for engagement by the Fund in areas outside its core business. Most departments suggested that, in the case of a further deterioration in the economic environment or additional demands, this could lead to errors by staff or lower quality of work, as well as

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

pressures limiting the delivery of some key outputs (e.g., general research). Some departments expressed concern about the difficulty of retaining experienced staff, particularly in highly specialized technical assistance areas, with potential consequences for the Fund's reputation. Several departments also considered that continued workload pressures could affect staff morale (see below). As noted in the paper on the FY 2013-FY 2015 Medium-Term Budget (EBAP/12/32, 03/30/12, Box 2), workload pressure indicators have indeed remained elevated, especially in departments most affected by the crisis.

41. **To mitigate these risks, a number of departments are working to more flexibly allocate resources within the department, better prioritize work programs and streamline products, while related policies are under review.** Other strategies include collaborating with external partners to help with the delivery of outputs that lie outside the IMF's core areas of expertise; enhancing supervisory oversight to minimize errors; and seeking additional mission support from other departments. At the Fund-level, the FY 2013 budget included reallocation of resources across departments made possible by streamlining and refocusing of targeted products (e.g., the vulnerability exercise, the fiscal monitor, REOs) and other savings, to provide additional resources for some crisis related activities. It also allowed for a net addition of about 30 staff, which should help alleviate some of the pressures. The work underway on work force planning (a paper is under preparation by HRD with OBP, and is expected to be discussed at the Board by the end of the year) will provide a holistic basis for further addressing these work pressure risks. The upcoming employment framework review could also be a useful tool in addressing concerns about potential mismatches of skills and positions. Furthermore, OBP and SPR are continuing to explore scope for further streamlining that may free up resources. However, should overtime levels remain elevated, and work pressures remain high, more rigorous choices will have to be made about what will have to be streamlined. This could lead to increased operational or reputational risks if there are not enough staff resources to provide adequate coverage of evolving risks.

Low morale

42. **Some departments noted concerns for morale arising from perceptions of continued erosion of salaries, benefits, and work practices, partly related to the lack of a structural increase in salaries for FY 2013, and others flagged the possible negative impact of workload pressures on staff.** Some noted that this could lead to difficulties in retaining and attracting high-quality staff. The recent staff survey and anecdotal evidence suggest that the overall diversity strategy, and specifically the efforts needed to achieve the benchmarks, may also be affecting morale. Some staff not from underrepresented groups are concerned about diminishing career opportunities, while some staff from underrepresented groups point to increasing discomfort with assumptions about unfair advantages and access to opportunity resulting from the diversity agenda.

43. **Several of the concerns raised by departments in the survey were reflected in the results of the 2010 staff survey.** A comprehensive plan to address these concerns has been put in motion, including the department-level action plans and use of flexible work arrangements. Furthermore, with the help of nine working groups, Management has adopted a range of measures that are being and will be implemented Fund wide. These include the adoption of an accountability framework for department Directors, measures to enhance internal and external mobility opportunities, the development of a leadership development program for managers at all levels, changes to the management performance system to help staff grow to their potential and deal more effectively with weak performers, more communication and education on diversity, and the planned adoption of a statement on workplace values. A second phase of measures will be prepared after implementation of this set of actions. Concurrently, to ensure deeper involvement and understanding of policy changes, HRD is actively engaging with the broader HR community to foster a corporate view of HR, including on ongoing employee survey action plans, to be able to respond more quickly to concerns and issues that need to be addressed.

VII. Issues for Discussion

Executive Directors' views are sought on the following issues:

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

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

Appendix: 2012 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. In describing the results of the survey, 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: Mino**r: 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; and 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

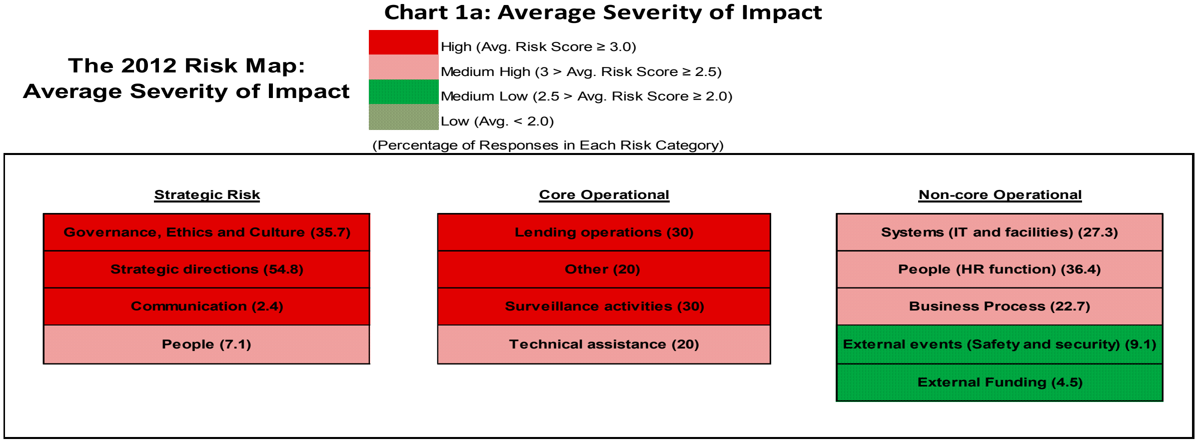
3. As noted above in the text of the report (and as shown in Appendix Table 1), respondents were cautious in their assessment on the likelihood of occurrence of a risk, with less than six percent of responses suggesting that a risk would occur with a very high likelihood or certainty. Equally, few risks (less than 8 percent) were seen as very unlikely either—most responses were evenly divided in their characterization as either "unlikely but possible" or "likely." Also of interest, the few risks characterized either as highly unlikely or highly likely were predominantly among the non-core operational risks to which the Fund is exposed. Of risks seen as likely, IT and people-related risks were most often the principal concerns.

In contrast, departments were less cautious in expressing concern that the occurrence of a risky event might have a serious impact: more than 20 percent of responses were viewed in this way, and more than two thirds of responses characterized the impact of such risk occurrences as at least of medium-high impact or as entailing a potentially serious impact. Risks at these levels of potential severity were relatively evenly distributed among the three principal risk categories (with a slightly higher share among non-core operational risks).

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 six subcategories suggest an average severity at least of medium-high impact, four carry particular weight in terms of the frequency of responses: governance, strategic directions, lending operations, and surveillance activities (with only one respondent expressing concern about communications), and these were all among strategic or core operational risks. One other core operational risk—"other risks"—also received a high severity score—but this proves to be a catch-all category. The written characterizations of this risk primarily relate to human-resource challenges in staffing or budget constraints limiting a department's ability to deliver core, or expanded outputs: as such, they primarily refer to non-core operational risks.

Chart 1a: Average Severity of Impact



Although many respondents also identified the three non-core operational risks of IT, the HR function, and business processes as a concern in terms of impact, these were all rated as falling between a medium-low and medium-low impact on average.

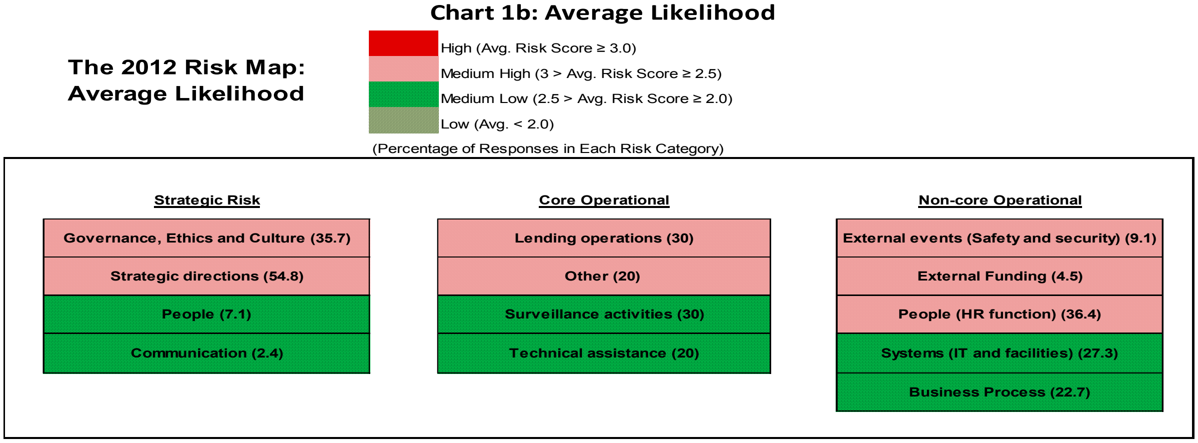
Table 1. Summary by risk categories, severity of impact and likelihood

Severity \ Likelihood	1 -Very unlikely but not negligible	2 - Unlikely but possible	3 - Likely	4 - Very likely/Almost certain	Subtotal
A. Minor Impact	**1**	**-**	**-**	**-**	**1**
Non Core Operational	*1*				*1*
Business Process	1				1
B. Medium-Low Impact	**2**	**19**	**20**	**2**	**43**
Strategic Risks		*3*	*2*		*5*
Governance, Ethics and Culture		1	1		2
People		1			1
Strategic directions		1	1		2
Core Operational Risks		*4*	*6*		*10*
Other			2		2
Surveillance activities		2	1		3
Technical assistance		2	3		5
Non Core Operational Risks	*2*	*12*	*12*	*2*	*28*
Business Process	1	4	2		7
External events (Safety and security)			3	1	4
External Funding		1	1		2
People (HR function)		6	2	1	9
Systems (IT and facilities)	1	1	4		6
C : Medium-High Impact	**8**	**27**	**33**	**4**	**72**
Strategic Risks		*10*	*13*	*1*	*24*
Communication		1			1
Governance, Ethics and Culture		2	4	1	7
People		1	1		2
Strategic directions		6	8		14
Core Operational Risks		*9*	*7*	*1*	*17*
Lending operations		2	4		6
Other		1	2		3
Surveillance activities		4	1	1	6
Technical assistance		2			2
Non Core Operational Risks	*8*	*8*	*13*	*2*	*31*
Business Process	3	2	1		6
External events (Safety and security)		2			2
External Funding			1		1
People (HR function)	1	3	8	1	13
Systems (IT and facilities)	4	1	3	1	9
D: Serious Impact	**-**	**19**	**11**	**2**	**32**
Strategic Risks		*8*	*5*		*13*
Governance, Ethics and Culture		3	3		6
Strategic directions		5	2		7
Core Operational Risks		*8*	*5*		*13*
Lending operations		2	4		6
Other		3			3
Surveillance activities		2	1		3
Technical assistance		1			1
Non Core Operational Risks		*3*	*1*	*2*	*6*
Business Process				1	1
People (HR function)		2			2
Systems (IT and facilities)		1	1	1	3
Subtotal	**11**	**65**	**64**	**8**	**148**

B. Average Likelihood of Occurrence

5. Chart 1b illustrates that none of the subcategories of risk are perceived, on average by respondents, as at least "likely" or more so. On average, all are seen as less likely, viz., between "likely but possible" or "likely" by the sample of respondents. But again, with a few exceptions, the risks seen as most likely are those which match those seen as having at least a medium-high impact in terms of importance—governance, strategic directions, lending, HR functions (and "other core operational," which, as noted, largely relates to people and budgets). The only exceptions relate to the possibility of adverse external events influencing safety and security and sources of external funding. Surveillance also has an average likelihood rating of 2.4, almost on the border of "possible but still not likely."

Chart 1b: Average Likelihood



C. Average Risk Intensity

6. Drawing on these results to estimate average risk intensity (the product of likelihood and severity, as seen in Figure 2 in the text), respondents suggest that the key risks facing the Fund can be distilled to three risks among core operational and strategic risks: those relating to lending (with risk intensity of 9.3), Fund governance (8.7) and the Fund's strategic direction (7.9). Three other risks also stand out, though to a lesser degree: concerns about the Fund's effectiveness in surveillance (7.3), and two non-core operational risks—people (or human resource issues), with a risk intensity of 6.9, and concerns about a breach of the Fund's IT system (6.8).

7. There was a significant drop off in terms of the risks perceived by other risk subcategories, both in terms of the number of departmental respondents identifying them and in terms of risk intensity. Technical assistance, identified by only five percent of respondents, had a risk intensity of only 5.8, with most seeing this risk as only "unlikely but possible" and of medium to low impact. While external events posing safety and security risks were seen as likely, most departments saw these as risks of medium to low impact. While 10 percent of respondents expressed concern about "business processes"—the identified risk intensity was only 5.1, reflecting a preponderance of views that these risks were either very unlikely or

"unlikely but possible," and with substantial variance in perceptions as to the severity of impact of these risks.

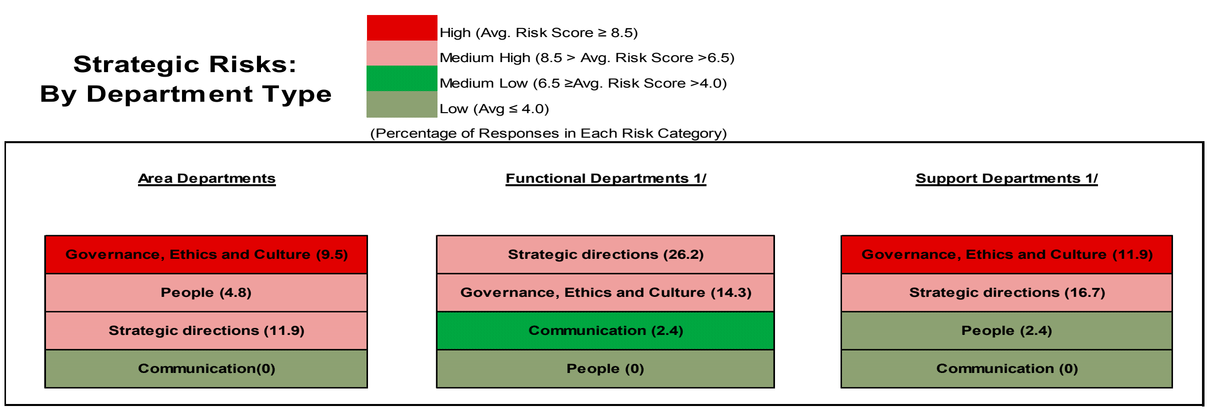
D. Perspectives on Risk across Department Types

8. Among **strategic** risks, there was a strong commonality of views on the high risk associated with governance, with area and support departments ascribing the highest risk intensity (8.7 – 9.4) and functional departments slightly lower at (8.0) (Chart 2.1). Departments were also largely in agreement on the risks associated with the Fund's strategic direction, with functional and support departments perceiving these risks with somewhat higher risk intensity (7.9 – 8.2) than area departments (7.4).

9. Among **core operational risks,** there was again substantial convergence on the high risks associated with the Fund's lending programs (see Chart 2.2), with area departments somewhat less concerned (risk intensity of 8.5) than functional and support departments (9.6-10.0). There was a significant commonality in perspective on the risks associated with surveillance (with risk intensity of about 7.3). Risks associated with the viability of technical assistance were seen as significantly lower, with risk intensity seen as much higher by functional and support departments (5.6 – 7) relative to area departments (4.0).

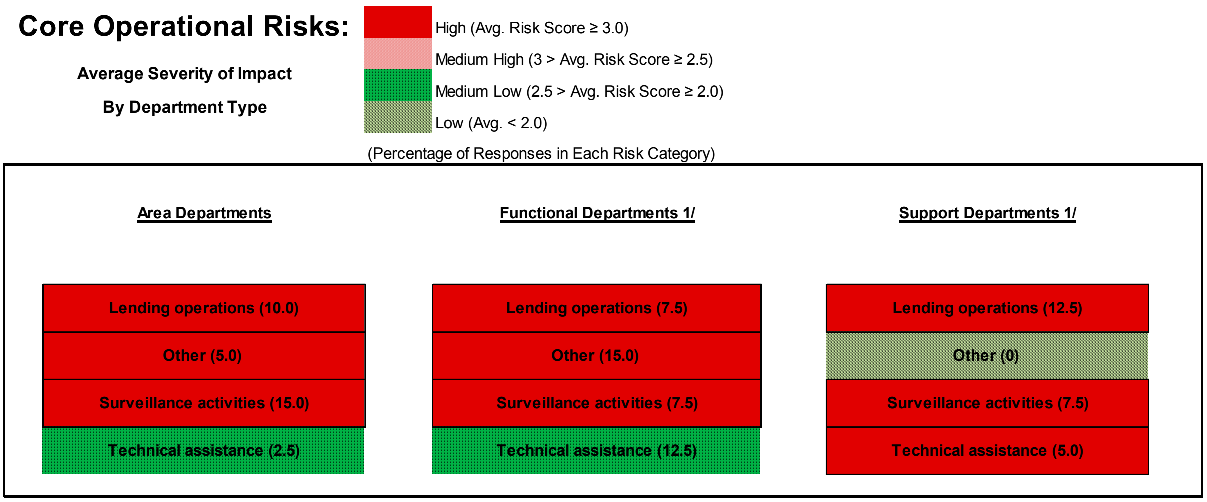
10. Since departments were asked to identify those **non-core operational risks** that bore principally on their *own* departmental functioning, a greater variance in perspectives would not be surprising (see Chart 2.3). This is particularly the case concerning **IT system** risks, where a high risk intensity of 10.5 was expressed, but by only two of the area departments. In contrast, functional and support departments attached considerably lower risk intensity—6.4-6.8—to this risk. A similarly high variance was associated with **business processes** in the Fund, with functional departments perceiving a high risk intensity to their operations (at 8.3), with only two area departments even identifying this as a risk (with risk intensity of only 6), and most support departments identifying this as a risk but with low risk intensity. Human resource issues appear as a generally shared and identifiable risk, though of only moderate risk intensity (ranging from 6 to 7.3).

Chart 2.1: Strategic Risks by Department Type



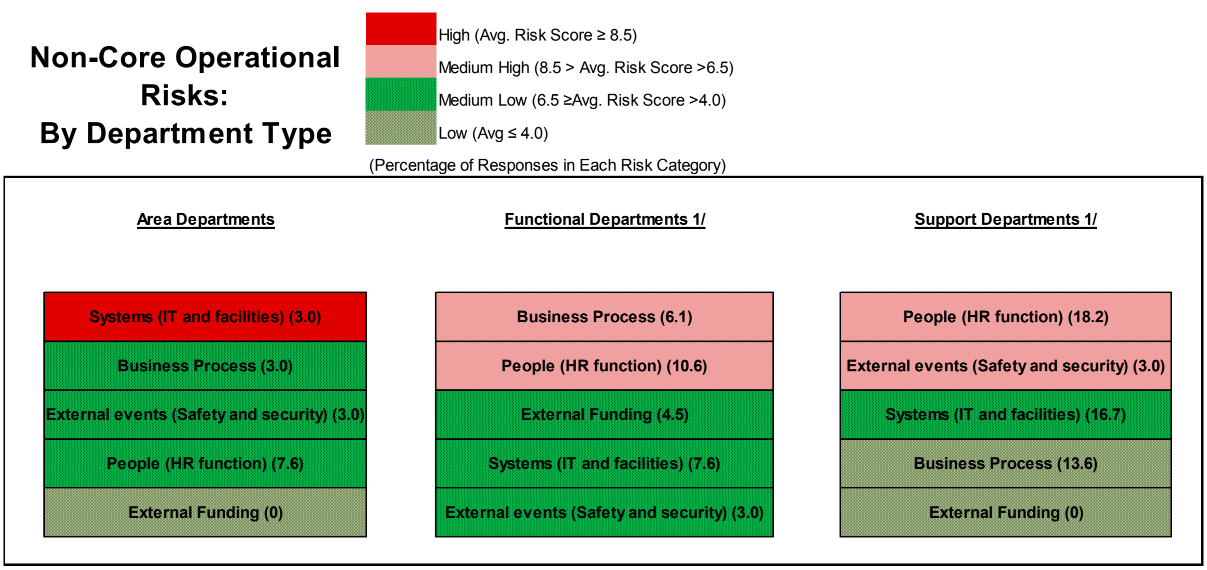
1/ Support departments include EUO, OBP, OIA, SEC, and TGS ; Functional departments include EXR, FAD, FIN, INS/OTM, LEG, MCM, RES, and SPR.

Chart 2.2a: Core Operational Risks - Average Severity of Impact by Department Type



1/ Support Departments include EUO, OBP, OIA and SEC; Functional departments include EXR, FAD, FIN, INS/OTM, LEG, MCM and STA.

Chart 2.3: Non-core Operational Risks by Department Type



1/ Support Departments include EUO, HRD, INV, OBP, OIA, SEC, and TGS; Functional departments include EXR, FAD, FIN, INS/OTM, LEG, MCM, RES, and STA.

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

11. This section elaborates on the discussion of perceived risks identified by departments in the survey and briefly summarized earlier in the text. What will be striking is the extent to which these risks overlap in obvious dimensions, such that a clear delineation is not possible. The characterizations also highlight the extent to which the above statistical measures display "noise" to the extent that the written descriptions of risk associated with specific sub-risk categories suggest that the intended risks could have been classified under other sub-risk

subcategories. As an example, the characterization of other core operational risks could have been as easily identified as human resource risks under non-core operational risks. Similarly, the overlap between the effects of business processes and human resource risks is also notable.

Strategic risks

- **The risk that governance reforms (and the 14th General Review of Quotas) might not be enacted by the 2012 Annual Meetings was expressed often and was perceived by departments as having the highest risk intensity among strategic risks**, contributing to a loss in the Fund's legitimacy and undermining the Fund's long-term effectiveness. This issue was cited five times with serious impact under strategic risk and six times with a medium-high impact.

- **Uneven responsiveness to shareholders**: Departments expressed concern that too much attention was being paid to European members, reflecting their current voting power; that program design might be "softened" as a consequence of that pressure from European members, with uneven treatment between European and non-European members; that there was insufficient engagement by the Fund outside of Europe, with too much Fund resources being utilized for Europe and a weakening of the Fund's work outside (e.g., in low-income countries, Arab Spring) and with a possible ignoring of the needs of emerging markets, and that these factors would be contributing to a loss in the Fund's legitimacy. Loans to Europe were mentioned under strategic risk six times with serious impact and eight times with medium-high impact, and this does not include the references under core operational risks (see below).

- **Not meeting the expectations of its members**: Departments expressed concern that the Fund was not sufficiently dealing with global issues and that a weakened global economy would itself reinforce this problem and weaken the Fund's leadership. Some worried that surveillance reform was not having a sufficient impact. Concern was expressed that if the Fund proves ineffective in Europe, this would have ripple effects on the Fund's perceived effectiveness and weaken the Fund's overall credibility. This latter concern echoes concerns expressed by departments on the Fund's core operational risks in lending, viz., that the program design in European countries might not work or the risk of a possible default in Europe.

  Both of the latter two risks appear to emanate from the same source, namely, the heavy focus by the Fund on the challenges faced in the Eurozone.

Core operational risks:

- **Problems that could arise from the Fund's loans to Europe** dominate the characterization of risks associated with the lending subcategory, and obviously overlap with concerns in the strategic risks area. Failure in Europe was seen as giving rise to a risk to the Fund's overall credibility, to an adverse impact on the global economy, and to risks to the Fund's finances. Lending to Europe was cited eight times as entailing serious risk among the core operational risks, and six times as of medium-high impact.

- **The possibility of surveillance missing tail risks:** principally expressed in the sub risk category of surveillance are expressions of concern that because of the Fund's involvement in Europe, the Fund could miss key developments in other regions (e.g., the risk of failure to identify the precise timing of a possible hard landing in China and organize a timely response to such an event, the possibility of crises in emerging market countries), inadequate policy traction in surplus countries and prove unable to address these risks or to identify emerging crises.

- **Other surveillance-related concerns** related to the pressure to perform bilateral financial surveillance, the potential for the Fund to give the wrong advice because of the pressures under which it is operating, and a concern that there are too many multilateral surveillance products. Though categorized among "other" core operational risks, concern was expressed of the risk of competitive devaluations and increased protectionism.

Distilling these concerns, one can observe that two principal risks dominate, namely, those relating to governance and legitimacy and the range of risks that are the potential consequence of the Fund's intense focus on Europe. The latter affects both the financial risks to which the Fund is exposed (credit and liquidity risks), and ultimately its reputation (to the extent that the Fund's bilateral and multilateral surveillance suffers as well as its capacity to meet expectations in other regions in both surveillance, program design, and program implementation.

Other operational risks

- **IT concerns** reflected principally the fear of a breach of security, leading to a loss of sensitive material, reputational risk, and/or an incapacity of IT systems to handle the operational workload, particularly that associated with financial transactions. This issue was cited six times among non-core operational risks with impact ratings of serious and medium-high.

- **Human resource challenges surfaced as a key concern, both as a core and noncore operational risk,** affecting the capacity of the Fund to do its work and the intense pressure to perform**. Concerns were expressed** of staff being drawn away to work on EU issues, poor morale, poor promotion prospects, inadequate salary levels, inability to compete for the best staff, and failure to deliver on promised output, excessive work pressures giving rise to errors.

- **Employment framework risks** to some extent reflect the pressure of budget on salaries, with ramifications on the ability of the Fund to compete in the market for high quality staff. But mention was also made of an outdated employment framework itself risking the loss of experienced staff (e.g., the four-year limit on contractual staff), the lack of new staff positions, the loss of experts, and the poor prospects for promotion.

- Departmental concerns with regard to **business processes**, as noted above, ultimately proved to be concerns about the effect of tight budgets on the ability of the Fund to carry out its responsibilities, with a heavy focus on the implications for the quality and quantity of available staff resources.

- **Although technical assistance was identified** as a core operational risk, these concerns appear more to derive from their human resource and budgetary risks. Departments expressed concern about the effects of external donors not renewing their funding of the Fund's TA program; external funding also surfaced as another risk to the extent that donor conditionality on the use of TA resources could adversely influence both the Fund's TA priorities and its effectiveness in implementation.