Review of Internal IDA Controls

Independent Evaluation by IEG

Approach Paper

July 10, 2006

Background

1. This Approach Paper (AP) is submitted for the review of the Committee on Development Effectiveness (CODE) and the Audit Committee (AC). It describes the work to be done by IEG[1] to evaluate the work by Management and the Internal Audit Department (IAD) on the ongoing review of IDA's Internal Controls (described overall as "the Review"). This AP updates the draft that was sent to CODE and AC on November 23, 2005, as a background document to the AC/CODE meeting on November 28, 2005 that discussed Management's initial work plan for the Review. The present version of the AP incorporates the clarifications that were made by Management during the AC/CODE meeting, including that the Review will focus only on IDA, and it also reflects more recent detailed definitions and modifications by Management of the scope of work, the approach to be taken for the Review, and the planned reporting.

2. In the IDA14 Replenishment Report[2] Bank Management "has committed to carry out an independent comprehensive assessment of its control framework including internal controls over IDA operations and compliance with its charter and policies" (paragraph 39 of that document), while Annex Table 3 of the document stipulated that this assessment should be undertaken by IEG (the former OED). This document has been approved by the Executive Directors.

3. This Review of IDA's controls was discussed briefly at a Board meeting in May 2005.[3] At that time, Management reiterated that - consistent with the Bank's COSO-based control framework - there should first be a self-assessment with a role for IAD leading up to the IEG evaluation. IEG confirmed that it was prepared to take on the requested evaluation if the Board should so wish. As this was not in the IEG work program, there would need to be a non-fungible addition to the IEG budget for this purpose.

4. Management has since confirmed that the different parts of the Review will be conducted in three phases: first Management will conduct an assessment of the internal controls over IDA's operations and compliance with laws and regulations; second, IAD will examine this assessment and provide a review of Management's assessment; and third, IEG will undertake an independent evaluation of both the assessment and the review.

---

[1] The Independent Evaluation Group (IEG) is since the fall of 2005 the name for the Bank's independent evaluation function. IEG comprises the independent evaluation entities in the Bank, IFC, and MIGA. All the evaluation work to be done under this draft Approach Paper will be done through IEG-WB - the former Operations Evaluation Department (OED).

[2] See "Report from the Executive Directors of the International Development Association to the Board of Governors, Additions to the IDA Resources: Fourteenth Replenishment, Working Together to Achieve the Millennium Development Goals" (approved by the Executive Directors of IDA on March 10, 2005).

[3] At the May 12 2005 discussion of IEG-WB's FY06-08 work program and FY06 budget.

The Management Assessment and the IAD Review
The Management Assessment

5. ***Overview, Scope and Standards:*** In defining the approach, scope and method to its assessment, Management has stated its intention to view IDA's internal controls in the context of the COSO internal control framework[4] and to use audit standards associated with that framework (see below). Management also stated that there would be certain limitations and phasing in its Work Plan, basically taking a two-stage approach to assessing the extent to which COSO objectives were being achieved in IDA. COSO is the framework which provides to senior management, the Board or other stakeholders a basis by which to judge and confirm that IDA's internal controls provide reasonable assurance that it has achieved:

i. Reliability in its financial reporting;
ii. Compliance with its charter and internal policies and procedures.
iii. Efficiency and effectiveness in its operations;

6. Recounting the fact that the Bank and IDA are already conforming to COSO standards in their reporting on financial matters, Management has stated that its assessment will, therefore, be concerned with the second and third of these COSO objectives, namely with issues of *compliance with IDA's charter and relevant internal policies and procedures,* and with *effectiveness and efficiency in operations.* Further, for practical reasons, Management intends to conduct the assessment in two parts, Part I to deal mainly with *compliance issues,* Part II with *effectiveness and efficiency* issues.

7. Management has clarified the definitions it will use regarding compliance (see ***Attachment 1)***: this will be judged against IDA's charter (those sections dealing with specific development goals, and those dealing with IDA's fiduciary requirements) together with IDA's internal policies and procedures (which are taken to be expressed in the Bank's published OPs, BPs, Operational Memos, and in the provisions of the Integrated Risk Management Framework).

8. The audit standards to be used define the degree of rigor in controls assessment and testing. Management has stated that it will use a set of standards based on concepts which are contained in the Audit Standard 2 (AS2) criteria. These standards are as directed by the Sarbanes-Oxley legislation (SOX), which were designed to strengthen financial reporting under the COSO framework. These standards needed to be defined because this is the first time the Bank has been required to provide assurances of its compliance and operations, so the issue arises whether it is appropriate to use the same standards as those used in its financial reporting. These proposed AS2 standards are more rigorous than the standards currently in use in the Bank and IDA for financial reporting, but the Bank is now preparing to adopt new standards which will bring it very close to conformity with AS2. There is agreement between Management, IAD and IEG that all will use the same audit standards, a description of which is contained in ***Attachment 2***. Since the adoption of standards for compliance reporting is new ground for IDA, IEG conducted a considerable amount of research, which contributed to the agreement reached. The aim was to find standards which were parallel to experience in other organizations, consistent with COSO, and also close to IDA's financial reporting standards.

[4] COSO: Committee of Sponsoring Organizations of the Treadway Commission, 1992. For a discussion of COSO standards, and a description of COSO principles, see Attachment 2 and 3 to the present AP. See also: World Bank, Office of the Controller, *Controls Guide: Implementing a Control Program in Your Unit* (2003), and IBRD and IDA FY05 COSO Year end Report (sent to the Audit Committee on October 19, 2005).

9. In summary, therefore, in the current scope of work defined by Management, the broad content of Part I and Part II, respectively, are described as being the following:

i. Part I: Processes and controls applicable to the fiduciary aspects of IDA operations (*The Compliance Assessment)*: including linkage of strategy to CAS, allocation of IDA funds, project cycle, financial management, procurement and safeguard activities, and use of budgetary resources. This Part I will focus mainly on two critical and specific COSO components: *risk assessment* and *control activities* as related to defined processes in IDA operations. It will not directly address the three other COSO components (*control environment*, *monitoring and learning*, and *information and communications*).

ii. Part II: Overarching control framework for IDA *(The Efficiency and Effectiveness Assessment)*: including all aspects of corporate governance and entity level control. By this stage, the focus of the review will be on efficiency and effectiveness of IDA operations; it will encompass all five of the COSO components; and will also cover areas not covered in Part I, such as site visits to field offices, and IT management issues.

10. As mentioned above, it is intended that for each of Part I and Part II, there will be three phases, with Management conducting an *assessment*, IAD providing a *review* and an *opinion*, and IEG completing an *evaluation* of both.

11. ***Management's Assessment Method:*** In emphasizing, for Part I, the fiduciary aspects of IDA controls, and while keeping within the COSO framework, Management decided to approach its assessment by focusing on the business processes that IDA performs on a daily basis in the execution of its operations. Management has defined 30 such Business Process Modules (BPMs) in nine business function areas as being in its view sufficient to capture the bulk of what governs IDA in its operations. Within each BPM Management has identified one, two or several *Key Controls* (110 in all), defined as mandatory, stop-go gateways through which a given transaction has to pass in order to be processed to conclusion. Management will both assess the design of these *key controls* and then test the effectiveness with which they operate. This will generate a basic data set from which to judge the effectiveness of the identified internal controls – individually and severally. Management will report weaknesses that are revealed, will make a judgment on their seriousness, and will recommend a remedial action plan as follow-up, where necessary. While this will be an essentially "bottom-up" approach to controls testing, Management intends also to link the 30 BPMs to their associated published policies and procedures, to the key units involved in their operation, and, where relevant, to the respective COSO components that they serve.

The IAD Review and Opinion

12. IAD has stated that its objective is to review the basis of Management's assessment and express an opinion on whether the assessment of internal controls over IDA operations, relating to their compliance with the IDA charter and its internal polices and procedures, has been fairly stated, based on the criteria established in the COSO framework.

13. ***Audit Scope:*** IAD takes Management's description of what will be examined in Part I (paragraph 10) as defining the scope of the first part of Management's assessment, and that this describes the scope of the review to be conducted by IAD. This will include criteria for the selection/exclusion of the BPMs; the mapping and documentation of the BPMs; the testing methods applied by Management; methods of assessing both design and operating effectiveness of key controls; adequacy of fraud detection; the identification of deficiencies; and Management's overall assessment. IAD will also perform, where needed, additional testing of key controls, partly by using its own ongoing related normal audit work being undertaken as part of its FY07 work program.

14. IAD also takes note of areas that will not be covered in Part I of Management's assessment. These include: the overarching control framework, corporate governance and entity level controls; efficiency and effectiveness of operations; 14 specific business process modules that have been explicitly excluded from being assessed under Part I and certain significant systems applications not already selected for review under the separate assessment on internal controls over financial reporting.

15. ***Audit Method:*** IAD states that its main focus will be on conducting additional testing and "walkthroughs" of all of the BPMs being assessed by Management, to review and form an opinion on each of Management's two key assessment levels: (a) *Testing design effectiveness of key control*s, basically by conducting additional walkthroughs to establish whether key risks have been matched by appropriate controls; and (b) *Testing operating effectiveness of the same controls,* by reviewing Management sampling methods for its testing of the key controls, and by conducting additional tests where necessary. IAD will use those audit standards agreed to also by Management and IEG, as described in ***Attachment 2.***

The IEG Evaluation

16. ***Overview, Scope, Standards:*** IEG will complete an evaluation of both the Management and the IAD studies, both separately and taken together, in such a way as to offer an independent conclusion to the Board as to:

> ***the degree of assurance with which the assessment and opinion presented respectively in the final reports by Management and IAD can be taken to be fairly stated, in terms of their giving reasonable assurance (or other conclusion) that IDA's controls over compliance with its charter and relevant policies and procedures are effective.***

17. IEG will take the COSO framework, and the audit standards consistent with that framework, as the starting point for its evaluation. It will assume that the judgments regarding the effectiveness of the internal IDA controls over compliance and operations will have to be made against criteria contained in the COSO framework as a whole. At the same time, IEG recognizes that Management has taken an approach in Part I that has certain scope limitations, and that relates only partially to the COSO framework. It will assume that whatever scope limitations that have been made – for whatever practical reasons – to the scope of the Management and IAD reviews in Part I, may have a bearing on the quality of assertions that can be made to the management and Board of IDA, and may themselves dictate certain imperatives about the scope and timing of the completion of Part II. IEG concurs with IAD that the key scope limitations in Part I are those described above, namely: the postponement to Part II of issues relating to entity-level controls; consideration of only two out of the five COSO

components;[5] the treatment of *compliance* only, and not *efficiency and effectiveness of operations;* and the postponement to Part II of the treatment of decentralized locations and IT systems. IEG will evaluate the implications of these postponements in making its judgments on the overall quality of the Management assessment and the ensuing statements of assurance and IAD opinion.

18. IEG's audit standards are the same as those to be used by both CTR and IAD, and which are explained in *Attachment 2.*

19. *IEG Evaluation Method:* In making its evaluation, IEG will apply four principal methods:

i. It will critically review the final reports from Management and IAD, as presented;
ii. It will conduct an independent analysis of the raw data generated by the test results from Management's assessment. (*This analysis will speak to the quality and effectiveness of the underlying internal controls);*
iii. It will generate its own data stream on the quality of both Management and IAD approaches, by applying evaluation tools designed for the purpose of rating each step in the assessment and review processes, in terms of definition, rigor, robustness of result and quality of conclusions and recommendations. (*These data will therefore speak to the quality of the Management assessment and the IAD review);*
iv. IEG may also conduct its own tests of the design and/or operating effectiveness of selected key controls, as a means of obtaining verification independent from the results obtained by Management.[6]

20. In summary, IEG will be providing its evaluative judgment using a combination of the four methods described above in order to provide an overall view of the quality of Management's assessment and the IAD review and opinion in all its key elements. The purpose of the evaluation will be to judge the quality of the two previous studies, and to evaluate the degree of assurance that can be attributed to their assessment and opinion on IDA's internal controls over compliance. How these three tiers of assessment, review and evaluation will fit together has been summarized in the Table 1 below.

[5] In Management's approach the focus will be mainly on *Risk Management* and *Control Activities*, which are COSO components; but there will be no direct focus on the other three components (*Control Environment, Monitoring and* Learning and Information and Communications) until Part II.

[6] IEG may consider commissioning its own testing, if and when:

(i) A general random selected testing of controls seems warranted;
(ii) Certain controls were found not to have been tested; and
(iii) Testing that was done may be deemed inadequate, for example because of sampling deficiencies or other flaws in approach.

TABLE 1: A SUMMARY DEPICTION OF THE KEY ELEMENTS IN THE PART I ASSESSMENT, REVIEW AND EVALUATION		
KEY STEPS IN THE METHOD AND APPROACH		
Management Assessment	***IAD Review and Opinion***	***IEG Evaluation***
Definition of Approach, Method Identification of Business Processes Documentation of Business Processes, Key Controls Assessing Design Effectiveness Testing Operation Effectiveness Assessing Results Drawing Conclusions Making Recommendations	Criteria for Inclusion/Exclusion Review process Test Methodology Review Management process for documenting test results Assess process to detect fraud Review Deficiencies, criteria Review Overall Assessment	Evaluate Impact of Scope Limitations: Evaluate Overall Cluster for conformity to COSO Evaluate each Module: Rank Strategic Significance Provide Quality Ratings for : Documentation and Mapping Assessment of Design Effectiveness Testing of Key Control Compliance Linkage to COSO Framework Conduct Independent Analysis of Management exceptions data Evaluate Quality of Management, IAD Conclusions
Statement of Assurance	**Unqualified Opinion or Modified Report**	**Overall Evaluation, Recommendations**

21. IEG will be delivering a final evaluation report backed up by the results it will have generated from its own analysis.

22. As is now normal for many of IEG's major evaluations, a senior ***Advisory Panel*** will be invited to review and comment on the IEG evaluation report and will be requested to share its comments also with CODE/AC. The members of the panel for this evaluation are all former Auditor-Generals, from India, Norway, and Australia, respectively.

Duration

23. ***Timetables***: Management has set out its revised timetables for the overall work in its revised work plan. Under this schedule, the Management assessment (for Part I) is now to be divided into two parts: Part IA will identify key business processes and controls and assess the design effectiveness of the identified key controls, while Part IB will assess the operating effectiveness of the identified key controls through testing for compliance with the identified procedures, and Part II will be the efficiency and effectiveness assessment. Management suggests the following timetables (it is assumed that the Management and IAD reports will only be distributed to CODE/AC with the respective IEG reports for each part of the exercise):

Management Report		**IAD Report**	**IEG Report**
I A	July 31, 2006	Within 4 weeks of receipt of Management's report	Within 6 weeks of receipt of IAD's report
I B	December 2006	Within 4 weeks of receipt of Management's report	Within 6 weeks of receipt of receipt of IAD's report
II	September 2007	November 2007	January 2008

24. IEG will make its best efforts to deliver its reports within the above timetables, which at this stage must however be kept contingent on there being no delays on the part of Management and/or IAD. The timing of the IEG reports will also always be subject to the overall consideration that IEG needs to take the time required to deliver a fully evaluated report, without having time constraints compromise quality.

25. ***Interim Report:*** IEG expects that its report on Part IA could contain a qualified evaluation of the Part IA assessment completed by Management and – if available – also on the concomitant report issued by IAD. Under the timetables described in the table above, - and on condition that IEG receives the Management and IAD reports on the indicated dates - IEG would be able to present its first (interim) report on Part IA by mid October. This would permit a CODE/AC discussion of the report, following which the report could be made available to the IDA Deputies in time for their next meeting planned for end November.[7] If delays occur in this timetable which would result, e.g., in IAD not being able to deliver its report to IEG in the stated time, IEG might then have to issue at that stage an evaluation of Management's assessment only, perhaps – time permitting – with only a cursory and highly qualified evaluation of IAD's report. The IEG evaluation will likely be substantially qualified, in addition, because of the approach taken by IEG to its overall evaluation. This has been designed within the COSO framework as a whole, and it may therefore be difficult to draw any final conclusions even on selected individual elements of the controls system, before the overall framework has been assessed.

Attachment 1: **A Note on the Definition of IDA's Internal Policies and Procedures**
Attachment 2**: A Note on the Standards Agreed by Management, IAD and IEG to be used in the Evaluation**
Attachment 3: **The Framework, General Approach and Tools that will be used in the IEG Evaluation.**

[7] IEG understands that Management would like for a report to be available in time for the meeting of the IDA Deputies (after appropriate discussion at CODE/AC). However, the scope of this evaluation report will depend on the timely delivery of the management and IAD reports.

Attachment 1

A NOTE ON THE DEFINITION OF IDA's INTERNAL POLICIES AND PROCEDURES

1. **Introduction**: In the main text of this Approach Paper it is stated that Part I of this review is to be focused on an assessment, review and evaluation of IDA's compliance with its *Charter and its internal policies and procedures*. While in the case of compliance with the Charter, this may seem clear and unambiguous, this may be less so in the case of the "*internal policies and procedures*". Therefore, it is necessary to have a clear definition of what is to be meant by these policies and procedures.

2. IEG takes note of the definition provided by Management in some of the background materials which have been supplied to IEG, and to the Board Committees, and hereby records its understanding of what those definitions comprise, both for the Charter and the policies, namely:

i. Provisions of the Articles, as interpreted from time to time by IDA's Executive Directors, relating to the management of the fiduciary aspects of lending operations. In this sense Management uses the term "fiduciary" to imply all those control processes which govern and ensure the allocation, disbursement and utilization of IDA funds for the purposes intended; also, with due regard to the debt sustainability of countries borrowing IDA resources, as provided for in the Articles;

ii. Internal policies and procedures relating to the management of the fiduciary aspects of lending operations, such policies to be contained in the Bank's published documentation (Operations Policies; Bank Procedures), and/or in other recognized sources of guidelines and practices in operational matters, to include reference to the allocation and country use of IDA funds for the purposes intended.

3. **Internal Policies and Procedures:** These may be taken to include the full range of policies embodied in IDA's activities: the mobilization of its resources, and the ensuing dialogue with its donor members; dialogue with its recipient member countries, including surrounding the IDA's project activities. In all cases, the policy frameworks for these initiatives and programs will provide the context within which the Association will pursue its activities to actually deliver development services using the following four distinct product lines:

i. Financial products (credits, grants and other transfers)
ii. Knowledge products (AAA – Analytical and Advisory Activities)
iii. Aid Coordination Services
iv. Information Management and transfer

4. *Internal Policies and Procedures* may also be extended to include internal management processes within the Association, among which:

i. Clear and consistent corporate and country strategies
ii. Transparent and effective management processes
iii. Empowerment of the staff, balanced with accountability

iv. Transparent and effective Governance and effective Board relations
v. Controlling Corruption
vi. Cohesiveness and Effectiveness of Trust Fund and other Partnership arrangements

5. Since this review and evaluation will not be examining issues relating to the soundness of IDA's financial reporting (the first COSO objective), it is the extent to which IDA's control systems serve to attain these less tangible elements of policy and procedure that will permit the evaluation to conclude (or otherwise) that compliance with the second COSO objective has been achieved. However, it is also understood that, in the phasing of the task that has been agreed, these non-tangible aspects will be tackled more directly during Part II of the evaluation, than in Part I which is the prime subject of this Approach Paper.

Attachment 2

Standards Agreed by Management, IAD and IEG to be Used in Assessing Deficiencies, Significant Deficiencies and Material Weaknesses

1. The Bank is currently performing its assessment of internal controls over external financial reporting using existing auditing standards on attestation of internal controls over financial reporting as prescribed by generally accepted auditing standards. In performing its review of compliance with IDA's charter and applicable internal policies and procedures, Management plans to use, as much as possible, the same concepts as those defined in the Auditing Standard No. 2 (AS2) *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, issued by the U.S. Public Company Accounting Oversight Board (PCAOB) in response to the provisions of Section 404 of the SOX legislation.

2. Management believes that applying the concepts that have been defined by audit standard setters for assessing internal controls over financial reporting will provide the level of comprehensiveness, rigor and consistency required in its self-assessment of internal controls and compliance with IDA's charter and applicable internal policies and procedures.

3. During our work it is anticipated that Management will discover items that represent deficiencies and which may or may not require remediation. A *control deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect noncompliance on a timely basis.

i. A deficiency in *design* exists when (a) a control necessary to meet the control objective is missing, or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not always met.

ii. A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

4. Control deficiencies are classified as one of the following: (i) an internal control deficiency; (ii) a significant deficiency[8]; or (iii) a material weakness[9]. The classification of the deficiency is based upon the likelihood of occurrence/noncompliance and/or the significance of noncompliance.

---

[8] AS2 defines a *significant deficiency* as a control deficiency, or a combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

[9] AS2 defines a *material weakness* as a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.

5. Conclusions about what constitutes a material weakness over compliance or operations are judgmental, more so than in the case of material weaknesses in financial reporting. Therefore, the definition of material weakness needs to be adapted from the context of the financial reporting definition, with its reliance on materiality in relation to the financial statements, to one using more judgment as to whether the operations and compliance objectives of internal control are met. To guide financial auditors in making these judgments, AS2 identifies examples of attributes the auditor should consider in evaluating identified internal control deficiencies to determine whether the deficiencies, individually or in combination, are significant deficiencies or material weaknesses. Management, IAD and IEG have agreed that clearly defined measures be established for judging operational materiality. These measures will be used as guides by each of the three groups in determining whether identified internal control deficiencies in compliance constitute significant deficiencies or material weaknesses. Identified deficiencies could be significant deficiencies or material weaknesses where the control deficiencies have attributes that could:

i. impair the achievement of IDA's objectives,

ii. violate requirements of IDA's charters or other contractual agreements,

iii. significantly weaken safeguards against waste, loss, or unauthorized use of funds, property, or assets,

iv. involve conflicts of interest,

v. involve systemic problems in country assistance, partnerships and project lending, and

vi. require the attention of Senior Management, the Board as well as the awareness of external stakeholders.

6. All deficiencies identified during Management's assessment will be placed on a summary deficiency schedule. The deficiency schedule will outline Management's assessment of the deficiency (type of deficiency), any mitigating controls over the deficiency, the potential financial impact, if any, the impact from a non-financial perspective, and management's determination of how to address the deficiency, i.e. corrective action (remediation). A control deficiency or combination of control deficiencies that, in management's judgment, represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives is a "Significant Deficiency". A significant deficiency or a combination of significant deficiencies that Management determines to be significant enough to be reported outside IDA shall be considered a "Material Weakness".

7. CTRVP and OPCVP will prepare a report assessing the overall deficiencies and make a determination on the impact the deficiencies have individually and in total on the internal controls over IDA's compliance with its charter and applicable internal policies and procedures. This report which will include: (i) Management's assessment of IDA's compliance with its charter and applicable internal policies and procedures; and (ii) a description of any significant deficiencies or material weaknesses identified through its assessment, together with their respective remediation plan.

Attachment 3

THE FRAMEWORK, GENERAL APPROACH AND TOOLS THAT WILL BE USED IN THE IEG EVALUATION

General

1. It has been agreed that the review of IDA internal controls will be conducted within the COSO framework. Equally, as described in the main text of the Approach Paper, IEG recognizes that Management has phased its approach, and will not be fully addressing all COSO-related issues in Part I of the review. Also, IEG recognizes that Management's approach in Part I will be based on its mapping, assessment of design and then testing of the working of some 30 business process modules, embodying over 100 control points. Each of these processes is, in effect, a micro unit in IDA's overall controls system, reaching through many levels of IDA's hierarchy, and also connecting in some cases to the macro framework of the five COSO components.

2. In making its evaluation IEG in essence faces a triple-tier task: it will have to evaluate the CTR *Assessment* and the IAD *Review*, and, in addition, it will need to come to its own judgment on the effectiveness of the underlying internal controls, independent of the findings of the other two studies. It intends to achieve these objectives through the application of the following four methods:

i. It will critically review the two final reports from Management and IAD, as presented;
ii. It will conduct an independent analysis of the raw data generated by the test results from Management's assessment; (*this analysis will speak to the quality and effectiveness of the underlying internal controls);*
iii. It will generate its own data stream on the quality of both Management and IAD approaches, by applying evaluation tools (template questionnaires or Protocols) designed for the purpose of rating each step in the assessment and review processes, in terms of definition, rigor, robustness of result, quality of conclusions and recommendations. (*These data will therefore speak to the quality of the CTR assessment and the IAD review)*
iv. IEG may also conduct its own tests of the design and or operating effectiveness of selected key controls, as a means of obtaining verification independent from the results obtained by Management.[10]

3. What follows is a brief account of the principal tools that IEG will use in applying these methods, specifically the two Evaluation Protocols. Management (and as corroborated by IAD) will be bringing forth its evidence in the form of 30 business process modules (BPMs), identified, mapped, documented, marked as to the *Key Controls* in each module, assessed for *design* effectiveness, and tested for effectiveness in *operation*. In order to evaluate each of these

[10] IEG may consider commissioning its own testing, if and when:
(i) A general random selected testing of controls seems warranted
(ii) Certain controls were found not to have been tested
(iii) Testing that was done may be deemed inadequate, for example because of sampling deficiencies or other flaws in approach.

steps in each of the 30 BPMs, in a transparent and standardized manner, IEG decided it would need a common template of questions to apply to each of the 30 modules. It therefore designed a *Business Process Protocol* for this purpose. In addition, since it will also be necessary to evaluate the overall cluster of modules, taken as a whole – in particular as seen from the perspective of the over-arching COSO framework – IEG designed a *COSO Protocol* for this second purpose. Both will be needed to make the overall evaluation.

The Business Process Protocol

4. The *Business Process Protocol* is designed to achieve three objectives: (i) to rank each BPM in terms of its overall significance – strategic importance, weight and centrality as a management tool, frequency of occurrence, potential financial magnitude; (ii) to apply quality ratings on Management's assessment (and IAD's review) of each step in identifying, documenting, mapping, assessing control design and testing control operation, and to rate the quality of Management's conclusions derived from its results. (iii) To evaluate the degree to which these assessments and reviews of the identified BPMs have been linked to specific components of the COSO framework. The protocol has over 50 questions, aimed at throwing light on the Management and IAD approaches and methods, which taken overall will speak to the principle question: *with what degree of assurance has it been shown by Management and IAD that their respective assurance and opinion have been fairly stated, from the perspective of providing reasonable assurance about the effectiveness of IDA's internal controls over compliance with its charter and internal policies and procedures?*

5. Broadly stated, the content of the *Protocol* in terms of the questions it contains, will allow coverage of at least the following types of issues:

i. Whether the scope of the assessments have been correctly defined; evaluate the implications of any deficiencies observed
ii. The quality of work performed to identify and relate risks to process maps
iii. The quality of the process testing; scope for alternatives
iv. Can a historical perspective be established, which will signal progress in strengthening control processes?
v. The quality of the work performed to assess the design of control activities to deal with identified risks and the subsequent testing of controls to verify they are working as intended
vi. The extent of adherence to the COSO Integrated Framework; possible observations regarding the adequacy of the Bank's adaptation of the framework to its control processes

The COSO Protocol: Linking to the COSO Framework

6. The principal function of the *COSO Protocol* is to establish the extent to which the effectiveness of the COSO framework can be tested by examining the cluster of BPMs, taken as a whole. Management's essentially bottom-up approach may have limitations because it has deferred the examination of entity-level controls. For this reason, the *COSO Protocol* has been designed to focus on the cluster of BPMs as a whole, and to ask questions (again, over 50 in all) which explore the linkages between the revealed features of the cluster and the 5 COSO components.

7. For the purposes of this Approach Paper the key elements of the COSO framework that have been highlighted in the IEG evaluation approach are listed below:

i. The three COSO ***Objectives*** are:
Reliable Financial Reporting;
Operational Effectiveness and Efficiency
Compliance with Charter and Internal Policies

ii. The 5 key ***Components*** of COSO are*:*
The Control Environment
Risk Assessment
Control Activities
Monitoring and Learning
Information and Communications

8. With regard to establishing ***Risk Focal Points***, the Bank Group has used the COSO framework to analyze and categorize risk into four major aspects:

Effectiveness of Strategy
Operational Efficiency
Financial Soundness
Stakeholder Support

9. As a comprehensive control framework, COSO therefore provides a set of cohesive criteria, against which to judge the extent to which IDA is achieving financial reliability, effectiveness and efficiency in its operations and compliance with its charter and internal policies and procedures.