

**AIC decision on appeal #2**

**CASE NUMBER AI0262  
IBRD/IDA INTEGRATED RISK MONITORING REPORT**

**(Decision dated October 19, 2010)**

1. On September 8, 2010, the Secretariat to the Access to Information Committee (the “Secretariat”) received the attached application (the “Application”) appealing the Bank’s decision to deny access to the report titled “IBRD/IDA Integrated Risk Monitoring Report AC2009-0131”, dated November 13, 2009 (the “Report”). The Bank had denied access to the Report based on the “Deliberative Information” exception under the Bank’s Access to Information Policy (the “Policy”).

2. The Application indicates two grounds for the appeal, namely “violation of Policy” and “public interest”. It states:

“The World Bank Group has initiated several reform processes that involve a potential redistribution of risk management and monitoring functions within the Bank and between the Bank and its clients. These reforms represent potential changes to core components of the Bank’s business model & safeguard policy applicability. The public is entitled to be as informed about the scenarios for risk monitoring in the context of Bank operations and Bank management in general in light of the fundamental importance of these reforms. Therefore, we feel that the benefits of disclosing the report, “IBRD/IDA Integrated Risk Monitoring Report AC2009-0131 (Nov. 13, 2009)”, outweigh any cost.”

***Findings and Decision of the Access to Information Committee***

3. The Access to Information Committee (the “AIC”) considered the Application on both grounds.

***“Violation of Policy”***

4. Pursuant to the Policy, a requester who is denied access to information by the Bank may file an appeal if the requester is able to establish a *prima facie* case that the Bank has violated the Policy by improperly or unreasonably restricting access to information that it would normally disclose under the Policy (*see* paragraph 36 (a) of the Policy). In reviewing the Application in accordance with the Policy, the AIC found that the Report:

(a) is a deliberative document covered by the “Deliberative Information” exception under the Policy and includes matters such as financial projections, corporate considerations, security and business continuity issues. These matters are covered by the “Security and Safety”, “Corporate Administrative Matters”, and “Financial Information” exceptions under the Policy (*see* paragraphs 12, 15, and 17 of the Policy). In view of the exceptions that apply, the Report is restricted from public access and would not normally be disclosed under the Policy; and

(b) is a Board Committee paper classified as “Confidential”. For the purposes of the Policy, Board papers are defined to include Board Committee papers (*see* footnote 17 of the Policy). The Policy states that Board papers classified as “Confidential” may only be eligible for declassification 20 years after the date on the document (*see* paragraph 33 of the Policy). As the Report dates November 13, 2009, the earliest the Report might become eligible for declassification is November 13, 2029. However, in accordance with the Policy, deliberative documents may be declassified after a passage of time only if it does not contain or relate to information that is not eligible for declassification (i.e., Personal Information; Communications of Executive Directors’ Offices; Ethics Committee; Attorney-Client Privilege; Security and Safety; Information Restricted Under Separate Disclosure Regimes and Other Investigative Information; Information Provided by Member Countries or Third Parties in Confidence; Corporate Administrative Matters; and banking or billing information of World Bank Group entities, member countries, clients, donors, recipients, or vendors, including consultants) (*see* paragraphs 32, 33 of the Policy). Because the Report is a deliberative document that contains and relates to information covered under the “Security and Safety” and “Corporate Administrative Matters” exceptions, which are not eligible for declassification, the Report is not a document that would be eligible for declassification under the Policy even after 20 years.

5. Based on the above findings, the AIC decided that the Bank properly and reasonably denied access to the Report and, therefore, did not violate the Policy. For this reason, in response to the appeal asserting a violation of the Policy, the AIC decided to uphold the Bank’s decision to deny public access to the Report.

6. Under the Policy, if the AIC upholds the initial decision to deny access to information in appeals alleging “violation of Policy”, the requester can appeal to the Access to Information Appeals Board (the “AI Appeals Board”) as the second and final stage of appeals (*see* paragraph 38 of the Policy). If you wish to file an appeal to the AI Appeals Board, click [here](#).

[URL provided in original decision sent to the requester.]

#### ***“Public Interest” case***

7. Pursuant to the Policy, a requester may file an appeal on a “public interest” basis if the requester is able to make a public interest case to override certain Policy exceptions that restrict the information requested. Public interest appeals are limited to information restricted under the Corporate Administrative Matters, Deliberative Information, and Financial Information (other than banking and billing information) exceptions (*see* paragraph 36 (b) of the Policy). The AIC:

(a) found that the “Security and Safety” exception applies to the Report which the AIC has no authority to override; and

(b) did not find compelling public interest reasons to override the “Deliberative Information” exception of the Policy (on which the Bank initially denied access to the Report), or the

“Corporate Administrative Matters” and “Financial Information” exceptions, which the AIC also found to apply to the Report.

8. For these reasons, in response to the public interest appeal, the AIC decided to uphold the Bank’s decision to deny public access to the Report.

9. Under the Policy, the decision of the AIC is final for appeals that assert a public interest case to override a Policy exception (*see* paragraph 37 of the Policy).