WORLD BANK GROUP INTEGRITY COMPLIANCE GUIDELINES

Revised November 24, 2025

WORLD BANK GROUP

PURPOSE AND APPLICATION

1. These Guidelines provide practical guidance to entities sanctioned through the World Bank Group's (WBG) sanctions system whose release from WBG sanction (e.g., debarment with conditional release, conditional non-debarment) is conditioned on the sanctioned entity developing, adopting, and implementing integrity compliance measures (e.g., an integrity compliance program) acceptable to the WBG, as determined by the WBG Integrity Compliance Officer. These Guidelines may also be consulted when reviewing an entity's integrity compliance measures before a sanction is imposed, or outside the sanctioning context by entities seeking to learn more about integrity compliance principles and measures.

2. These Guidelines outline the key principles comprising an integrity compliance program (Program). In the WBG context, a Program should, at a minimum, be designed to prevent, detect, investigate, and remediate the WBG's five sanctionable practices (i.e., fraudulent, corrupt, collusive, coercive, and obstructive practices). An effective Program also should incorporate the entirety of an entity's integrity compliance efforts and should function as an integral part of the entity's business operations.

3. These Guidelines apply to IBRD, IDA, IFC, MIGA, and relevant entities sanctioned under the WBG sanctions system.

DEFINITIONS

As used in these Guidelines, capitalized terms have the meanings set out: (i) in the applicable WBG sanctions procedures; or (ii) below. If a definition in these Guidelines conflicts or is inconsistent with a definition in the relevant WBG sanctions procedures, the definition in these Guidelines shall prevail.

1. **Business Partners**: external parties working with an entity, including but not limited to agents, representatives, consultants, law firms, financiers and bankers, investors, brokers, intermediaries, distributors, suppliers, vendors, contractors, subcontractors, subconsultants, consortium partners, joint venture partners, and other third parties.

2. **Collective Action**: collaborative initiatives with other persons, companies, or organizations regarding integrity compliance and business ethics.

3. **G&E**: gifts, hospitality, and entertainment, whether offered or received by an entity.

4. **Misconduct**: (i) fraudulent, corrupt, collusive, coercive, and obstructive practices, as defined in the applicable WBG documents and guidelines; and (ii) any other type of misconduct that an entity deems relevant under its Program, depending on the circumstances.

5. **Politically Exposed Persons**: individuals who are or have been entrusted with a prominent public or political function, as well as their immediate family members and close associates.

6. **Program**: an entity's integrity compliance program.

7. **Public Officials**: individuals who serve in government, political parties, state-owned enterprises, public international organizations, or other public functions.

8. **Risk-Based**: an approach in which more attention and resources are dedicated to the more critical risks.

9. **WBG:** the World Bank Group.

SCOPE

A. INTRODUCTION

As part of the WBG's effort to improve its sanctions regime, the sanction of debarment with conditional release became the baseline sanction for cases initiated under the applicable WBG sanctions procedures in September 2010. The development (or enhancement) and implementation of a Program satisfactory to the WBG also became the standard condition for release from debarment (or conditional non-debarment). The WBG Integrity Compliance Office monitors integrity compliance by sanctioned entities and the WBG Integrity Compliance Officer determines whether such entities have satisfied the integrity compliance conditions and/or any other conditions imposed by the WBG as part of a sanction.

Although these Guidelines are intended primarily for entities sanctioned under the WBG sanctions system, other entities are encouraged to consider them as well. These Guidelines are designed to be adaptable to entities of all types and sizes in various environments, including small and medium-sized enterprises, state-owned enterprises, and multinational corporations.

These Guidelines are not meant to be exhaustive, exclusive, or wholly prescriptive; rather, an entity's use of these Guidelines should be determined based on that entity's own circumstances. While each entity's Program should be tailored to its specific circumstances and integrity risk profile, essential elements – such as those outlined below – should be incorporated into the Program through adequate and proportionate policies and procedures.

In addition to addressing the entity's own circumstances and integrity risk profile, an entity's Program should: (i) be designed to effectively prevent, detect, investigate, and remediate Misconduct; (ii) be dynamic; and (iii) comply with all applicable laws and regulations. The mere adoption of policies that reflect the principles in these Guidelines is not enough; an entity must also implement its Program consistently and in good faith, periodically assess the adequacy and effectiveness of the Program, and update it as needed to ensure that it works in practice.

The Program should be applicable to members of the entity's governance body, the entity's employees (at all levels and of all types, including management, and at all locations, including regional or overseas locations), and the entity's (directly or indirectly) controlled affiliates. The entity should seek to apply relevant aspects of the Program to: (i) the entity's and its controlled affiliates' Business Partners and supply chains; and (ii) joint ventures and consortia in which the entity or a controlled affiliate participate.

B. CORE PRINCIPLES

An effective Program should be founded on key principles, such as those outlined below, to address the risk of Misconduct. Entities should develop accessible and easy-to-understand policies and documents that clearly and in reasonable detail articulate the entity's values, integrity expectations, and processes and procedures for preventing and addressing Misconduct. Such policies and documents should be regularly reviewed and updated to reflect any new risks or changes in the entity's integrity risk profile.

1. Integrity Risk Assessments

The Program should be based on an initial (or updated) comprehensive integrity risk assessment of the entity's business and operations, which takes into account its size, business sector(s), location(s) of operations, regulatory landscape, and other circumstances particular to the entity. Such integrity risk assessment should evaluate the risk of Misconduct across the entity's entire workforce and business operations, including controlled affiliates, transactions, partnerships (e.g., joint ventures and consortia), and technologies in use. The Program should establish policies and procedures intended to address and minimize the risks identified during such risk assessment.

The risk assessment should be repeated regularly (ideally at least annually) to capture any changes to the entity's operations, legal obligations, and integrity risk profile. Such updated risk assessments also should consider lessons learned from the entity's own experiences and from entities in similar circumstances. After each review, the Program should be revised and adjusted as necessary to address any new risks or different levels of risk.

Integrity risk assessments can be conducted internally or by outside experts depending on the circumstances. In either case, relevant persons should be actively involved, including the entity's senior leadership, the integrity compliance team, and those responsible for the design, implementation, and oversight of the Program.

2. Prohibition of Misconduct

The entity's primary Program document (e.g., code of conduct or similar document) should explicitly and visibly prohibit Misconduct – including fraudulent, corrupt, collusive, coercive, and obstructive practices – in all forms and at all times, whether direct or indirect. Policies should be updated, as appropriate, to address new and emerging forms of Misconduct relevant to the entity's business.

3. Management Roles

Senior management and the entity's governance body should provide strong, visible, and continuous support for the Program and its full implementation, in both letter and spirit. Senior management should: (i) be responsible for developing and maintaining the Program and fostering a culture of integrity, with oversight from the governance body; and (ii) regularly communicate integrity-related standards to employees, while also leading by example. Managers at all levels (including middle management) should, in turn, reinforce integrity standards and encourage employees to abide by them. Senior management and the governance body should ensure that sufficient resources are provided for the effective development and implementation of the Program.

4. Individual Responsibility

Compliance with the Program should be mandatory and the responsibility of individuals at all levels of the entity and its controlled affiliates. These individuals should include employees, senior management, members of the governance body, and, where possible, relevant individuals at joint ventures and consortia in which the entity or its controlled affiliates participate.

5. Integrity Compliance Function

A senior officer with adequate independence, authority, autonomy, and stature – as well as the necessary resources and expertise – should oversee and manage the Program. The reporting lines of that officer should allow for direct communication with top-level management and the governance body, including any audit committee. Other members of the entity's integrity compliance function should similarly be empowered to perform their responsibilities with sufficient independence and autonomy. The entity should establish rules and processes to address potential and actual conflicts of interest involving the members of the integrity compliance function, especially any part-time members.

Persons responsible for the Program should: (i) receive proper training to perform their roles effectively; and (ii) have sufficient access to relevant sources of data to allow for timely and effective monitoring and testing of procedures and controls, as relevant.

6. Decision-Making Process

The entity should establish a sound decision-making process and designate appropriate decision-makers, including senior management and the integrity compliance function where appropriate, taking into account the value, complexity, and perceived integrity risk of each transaction. Decisions should be recorded appropriately, indicating that pertinent risks were considered.

7. Training and Communication

The entity should periodically communicate the Program and provide effective training tailored to relevant needs, circumstances, roles, and responsibilities. Such training and communication should be provided to all levels of the entity and its controlled affiliates (including for members of the governance body) and, where appropriate, to Business Partners. Targeted training should also be provided for specific functions, such as employees in sensitive and high-risk roles or areas. The entity's senior management should publicly communicate details of the Program – whether through annual reports or other channels – and ensure that the Program and related policies and procedures are easily accessible to employees and Business Partners as relevant, including in multiple languages if appropriate.

Entities should periodically assess the impact of their training and communication efforts on employee behavior and overall integrity culture. Entities also should seek feedback about the Program, and explore ways of receiving such feedback, including by using exit interviews and surveys where appropriate.

8. Advice and Guidance

Entities should adopt effective, confidential mechanisms for providing timely advice and guidance to employees, senior management, members of the governance body, and Business Partners on complying with the Program, including when they need to contact relevant individuals for urgent advice on difficult situations in overseas jurisdictions. The entity should publicize such mechanisms, including how they can be accessed and used by relevant persons, and make them available in multiple languages as needed.

Entities that use technology systems (e.g., chatbots) to provide advice and guidance under the Program should ensure that: (i) information provided by such systems is accurate and consistent with the Program; (ii) consultations with such systems remain confidential and only accessible by authorized persons in accordance with Program requirements; and (iii) such systems remind users of their reporting obligations under the Program and their options for submitting such reports, whether through whistleblowing channels or directly to relevant individuals.

9. Duty To Report

Employees and members of the governance body should be required to report integrity concerns – including any known or suspected Misconduct as well as other relevant suspected breaches of the Program – through designated channels, in compliance with applicable laws and regulations. In situations where mandatory reporting is not permitted by applicable laws or regulations, such persons should be strongly encouraged to report. External parties, including Business Partners, should similarly be required or encouraged, as appropriate, to report such concerns and breaches. Retaliation against persons who report in good faith should be prohibited and subject to appropriate disciplinary action.

10. Whistleblowing/Reporting Channels

Entities should provide secure, confidential, and appropriately scaled mechanisms for employees, members of the governance body, and external parties to report any integrity concerns, including any known or suspected breaches of the Program. Options for anonymous reporting should be available, to the extent possible under applicable laws and regulations. The entity should establish procedures to protect whistleblowers and reporters (including Business Partners and other third parties) from retaliation. The entity also should periodically assess employees' awareness of the whistleblowing/reporting mechanisms and their comfort level in using them.

11. Investigation Procedures

Entities should develop and implement protocols for investigating suspected Misconduct and other alleged violations of the Program (whether encountered, reported, or discovered) and should assign responsibility for such investigations to appropriate persons. The entity should prohibit retaliation against persons (including Business Partners and other third parties) who support or assist an investigation or audit. The entity should establish clear protocols for responding to external investigations and audits in a timely and legal manner, as directed by the entity's leadership with input from the integrity compliance function where relevant.

12. Remediation and Disciplinary Mechanisms

When Misconduct is identified, the entity should take reasonable steps to respond with appropriate remedial action and prevent further Misconduct. Such steps should, where appropriate, include disciplinary measures (up to and including termination) to address violations of the Program at all levels of the entity and its controlled affiliates. The entity should designate suitable individuals or committees to determine the appropriate disciplinary action or other remedial measures and implement or oversee them.

13. Collective Action

Entities should participate in appropriate integrity and Collective Action initiatives – for example, with businesses as well as trade, professional, and civil society groups – to promote integrity and encourage other entities to put in place effective integrity compliance measures.

C. INTERNAL CONTROLS

Internal controls, such as those detailed below, are essential for building a robust Program that prevents, promptly detects, investigates, and appropriately remediates Misconduct.

14. Employee Due Diligence

Prospective employees and prospective members of the governance body should undergo integrity vetting before employment – to the extent permissible under applicable laws and regulations – to identify any history of Misconduct, behavior inconsistent with an effective Program, or potential or actual conflicts of interest. Such vetting may include background and reference checks, searches of public data, and other measures. While all candidates should be subject to some degree of vetting, high-risk individuals or positions should receive more scrutiny. The entity should consider the findings of the integrity vetting process when making hiring decisions. The entity also should consider vetting existing employees and members of the governance body, using a Risk-Based approach, especially before promotion or reassignment to sensitive positions.

15. Employee Contractual Obligations

Employment contracts should include integrity-related obligations, including requiring employees to abide by the Program, act in good faith, and disclose any potential or actual conflicts of interest. The contracts also should state that the entity may impose remedies and/or penalties for Misconduct (including possible termination of employment, where appropriate). Similar obligations should apply to other relevant persons such as members of the governance body, as appropriate.

16. Periodic Certification

To the extent permitted under applicable laws and regulations, employees, especially those with decision-making authority or in a position to influence business outcomes, should periodically (at least annually) certify, in writing, that they have: (i) reviewed and understand their obligations under the Program; (ii) complied and will continue to comply with the Program and applicable laws; and (iii) reported and will report any known or suspected Misconduct through the appropriate channels. Similar obligations should apply to other relevant persons such as members of the governance body, as appropriate.

17. Relationships with Current and Former Public Officials and Politically Exposed Persons

The entity should impose appropriately tailored restrictions on remunerative arrangements and other commercial arrangements with current and former Public Officials, Politically Exposed Persons, and entities associated with such persons, particularly when such arrangements relate to positions or functions that such persons hold, have held, or could materially influence. Clear protocols should be in place to prevent undue influence or the appearance of impropriety if such persons are engaged by the entity, regardless of whether their roles are full-time, part-time, or unpaid.

18. Gifts, Hospitality, Entertainment, Travel, and Expenses

The Program should establish controls and procedures to ensure that gifts, hospitality, and entertainment (G&E), whether offered or received: (i) are reasonable and comply with the entity's guidelines; (ii) do not violate applicable laws and regulations; and (iii) do not improperly influence, or create an appearance of improperly influencing, the outcome of any process or transaction, or otherwise result in an improper advantage. Such controls should include, to the extent necessary, limits on the type and monetary value of G&E, reporting requirements, and requirements for pre-approval by the integrity compliance function or other high-ranking persons in high-risk situations. Similar controls and procedures should be established for travel and other business expenses.

19. Political Contributions

The entity should only make contributions to organized political parties, candidates for elections, or other political entities in accordance with applicable laws and regulations. The entity also should take appropriate steps to publicly disclose all such contributions (unless secrecy or confidentiality is legally required). To reduce the risk of Misconduct, entities may implement controls such as conducting due diligence, requiring senior management approval before such contributions are made, or having the integrity compliance function review such contributions for integrity risks.

20. Charitable Donations and Sponsorships

An effective Program should include safeguards to prevent donations and sponsorships from being used as a subterfuge for Misconduct. In this regard, donations and sponsorships should be free from conflicts of interest, should be publicly disclosed as far as possible, and should not confer improper advantages or create an appearance of impropriety. The entity also should conduct Risk-Based due diligence on proposed recipients of its donations and sponsorships to ensure that they are reputable and that no improper purpose is intended. Donations and sponsorships should take into account the findings of such due diligence and, where appropriate, should be formalized through written agreements that outline integrity-related expectations and rights.

21. Facilitation Payments

The entity should prohibit facilitation payments, as well as require prompt reporting to the integrity compliance function and proper recording in the entity's books and records if such payments are requested or exceptionally made (e.g., in case of duress). To the extent necessary, the entity should establish clear protocols for avoiding, as far as possible, and responding to requests for facilitation payments, and conduct training on how to handle such situations.

22. Recordkeeping

Appropriate records should be maintained regarding all aspects of the Program. The records should be kept in an auditable format and be accessible to relevant persons, including for purposes of inspections, audits, and investigations. The entity's policies should assign responsibility for creating, accessing, and maintaining different types of records under the Program.

23. Business Development

Particular safeguards and procedures should be adopted to prevent and address Misconduct in the entity's business development efforts. In this context, the entity should seek to ensure that all bidding and other business development activities are based on accurate and complete disclosures and representations (which should be reviewed and verified for their accuracy and completeness), comply with applicable laws and rules, and do not otherwise involve Misconduct. The entity should consider segregating sales or business development functions from those responsible for preparing, reviewing, or approving bid submissions and business proposals, where appropriate.

24. Merger and Acquisition

Other companies or organizations that come under the entity's control through a merger or acquisition should be subject to the Program and undergo an integrity risk assessment as a basis for their integration into the Program. The integrity compliance function, with input from the risk assessment and due diligence findings, should guide the Program integration process, including decisions on adding resources to the integrity compliance function, training and communications, updating policies or procedures, and amending contracts where necessary. The entity also may consider reserving the right to exit or cancel the transaction if material integrity compliance problems are discovered.

25. Business Partners

The entity should take steps to mitigate integrity risks in its engagements with Business Partners. In this respect, the entity should:

i) conduct Risk-Based integrity due diligence on Business Partners prior to engagement, and update such due diligence periodically during any period of engagement, to assess potential integrity risks associated with the Business Partner (e.g., if they have engaged in Misconduct or have potential or actual conflicts of interest), with the understanding that different types of Business Partners should undergo due diligence tailored to their specific risk profiles; the entity should avoid dealing with Business Partners known or reasonably suspected to be engaging in Misconduct, except where appropriate mitigating measures are put in place;

ii) inform Business Partners of its integrity-related expectations and make it clear that the entity expects all activities carried out on its behalf to comply with the Program;

iii) use its best efforts to require or encourage, as appropriate, all Business Partners to adopt an equivalent commitment to prevent, detect, investigate, and remediate Misconduct;

iv) include in its Business Partner contracts: (i) appropriate contractual obligations outlining integrity-related expectations (e.g., audit rights, obligations to disclose conflicts of interest and not engage in Misconduct); and (ii) remedies and/or penalties in relation to Misconduct, including a plan to exit the arrangement if necessary (e.g., a contractual right of termination if the Business Partner engages in Misconduct, is reasonably thought to have engaged in Misconduct, or has behaved in a manner inconsistent with the Program);

v) conduct Risk-Based monitoring of Business Partners on an ongoing basis to ensure, as far as is reasonable, that there is no Misconduct in the business engagement; and

vi) document fully and accurately its relationships with Business Partners.

26. Appropriate Remuneration and Payment

Third party remuneration should be justifiable for legitimate services to be rendered or goods to be provided. Likewise, payments to Business Partners and other third parties should be for legitimate services rendered or goods provided, paid through *bona fide* channels, and duly recorded in the entity's books and records. Payments and expenses incurred by the entity should also be supported by proper documentation and receipts, and any reward-based remuneration to be offered to Business Partners (e.g., commissions, incentives) should be evaluated for potential integrity concerns. Business Partner contracts should: (i) clearly describe the services to be performed and/or the goods to be delivered; and (ii) specify payment terms.

27. Financial Controls and Audits

Entities should establish and maintain effective internal controls over their financial, accounting, and recordkeeping practices, and other business processes, in compliance with applicable laws and regulations. The internal control systems, including financial and accounting controls as well as other aspects of the Program, should be subjected to regular, independent, internal and external audits and testing to provide assurance on their design, implementation, and effectiveness. Appropriate persons within the entity should review relevant audit findings with a view to implementing any recommendations and addressing any identified issues or gaps, as appropriate.

28. Incentives

Entities should promote compliance with the Program by adopting and implementing suitable incentives for employees, management, and members of the governance body. They also should seek ways to encourage ethical behavior and compliance with the Program by their Business Partners, to the extent appropriate.

To learn more about the ICO, please visit our website: https://www.worldbank.org/en/about/unit/integrity-vice-presidency/sanctions-compliance.

For additional resources on integrity compliance, we invite you to explore the WBG Integrity Compliance Knowledge Sharing Platform: https://www.integritycomplianceknowledgehub.org/.