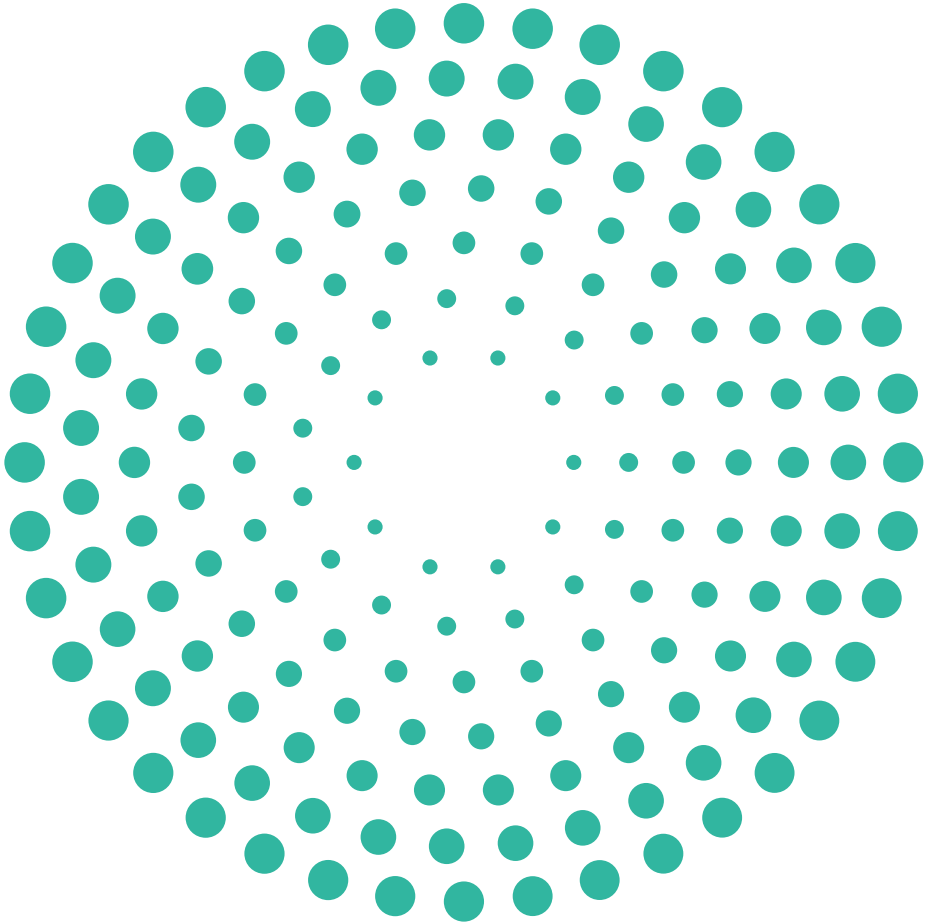


Integrity Compliance Programs for SMEs

Practical Guidance and Resources



Integrity Compliance Programs for SMEs

Practical Guidance and Resources



THE WORLD BANK
IBRD • IDA



Ministry of Justice

Some rights reserved

This work is a co-publication of the Ministry of Justice, Republic of Korea (MOJ), and The World Bank.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent, or those of the Ministry of Justice, Republic of Korea. The World Bank and MOJ do not guarantee the accuracy, completeness, or currency of the data included in this work and do not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank or MOJ concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Rights and Permissions



This work is available under the Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO) <http://creativecommons.org/licenses/by/3.0/igo>. Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:

Attribution Please cite the work as follows: Ministry of Justice, Republic of Korea, and The World Bank. 2024. Integrity Compliance Programs for SMEs: Practical Guidance and Resources. License: Creative Commons Attribution CC BY 3.0 IGO

Translations If you create a translation of this work, please add the following disclaimer along with the attribution: This translation was not created by the Ministry of Justice, Republic of Korea, or The World Bank and should not be considered an official translation. The Ministry of Justice, Republic of Korea, and The World Bank shall not be liable for any content or error in this translation.

Adaptations If you create an adaptation of this work, please add the following disclaimer along with the attribution: This is an adaptation of an original work by the Ministry of Justice, Republic of Korea, and The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by the Ministry of Justice, Republic of Korea and The World Bank.

Third-party content The Ministry of Justice, Republic of Korea, and The World Bank do not necessarily own each component of the content contained within the work. The Ministry of Justice, Republic of Korea, and The World Bank therefore do not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to re-use a component of the work, it is your responsibility to determine whether permission is needed for that re-use and to obtain permission from the copyright owner. Examples of components can include, but are not limited to, tables, figures, or images.

All queries on rights and licenses should be addressed to the Ministry of Justice, Republic of Korea Ministry of Justice(International Legal Advisory Division), 47 Gwanmunro Gwacheon-si, Gyeonggi-do, 13809, Republic of Korea, E-mail: mohjd@korea.kr.

Foreword by the Deputy Minister for Legal Affairs, Ministry of Justice, R.O.K.

In recent times, the management of ESG (Environmental, Social, Governance), which has become a global agenda, is firmly establishing itself as an essential consideration for both large corporations and small to medium-sized enterprises (SMEs), serving as a crucial factor for the development of 'sustainable businesses.' Moreover, as climate change, energy crises, and corruption prevention gaining global significance, ESG is increasingly utilized to evaluate and regulate companies on international scale.

To ensure that companies venturing abroad do not encounter difficulties amid rapidly changing global regulations and policies, the Korean Ministry of Justice established the International Legal Affairs Department in 2023, which actively engaged in providing legal consultations for small and medium-sized export enterprises, monitoring overseas regulations, and organizing tailored legal briefing sessions through the International Legal Advisory Division. The publication of the *Integrity Compliance Programs for SMEs: Practical Guidance and Resources* is the culmination of approximately four years of collaboration and research in partnership with the World Bank.

This book serves as a practical guide based on the experience of the Integrity Compliance Office within the World Bank's Integrity Vice Presidency (INT), responsible for integrity compliance and corruption prevention for about 15 years. It is based on the insights gained through global communication with companies, issue analysis, and the formulation of compliance improvement measures. Specifically, with the aim of preventing governance risk for SMEs--the core drivers of global economic development and trade--the guidebook provides tailored risk prevention and management guidelines aligned with the 'Global Standard,' business models, budgets, and risk factors. Amidst your busy schedules, I extend my gratitude to all individuals involved in this publication project, including Lisa Miller, Director Shin, Donghwan, and all personnel from the World Bank's Integrity Vice Presidency and International Legal Advisory Division. I hope that this publication serves as a valuable reference for the implementation of integrity compliance measures for small and medium-sized enterprises in various countries, including Korea.

Seoul, Republic of Korea
January 30, 2024

Koo, Sang-Yeop
Deputy Minister for Legal Affairs, Republic of Korea

Foreword by the World Bank's Integrity Vice President

The World Bank has a critical mission: to support countries in eliminating poverty and boosting shared economic prosperity. It does this through the provision of global knowledge and financing for development projects. In pursuing these World Bank-financed projects, it is often necessary to draw on the skills and expertise of private sector companies, who are contracted to support the implementation of the project's objectives. Ultimately, a project's success may not only rely on the capabilities of these companies, but also the integrity with which they operate their businesses.

The World Bank's Integrity Vice Presidency (INT) works to ensure that companies and individuals who work on World Bank projects do so in accordance with the highest standards. INT vigorously promotes the adoption of compliance best practices in the private sector because doing so is a key element of the Bank's overall strategy for combating fraud and corruption. In addition to pursuing sanctions against bad actors and advising project teams on risk mitigation, INT—through the Integrity Compliance Office—works with hundreds of companies around the world and engages in outreach efforts to advance the spread of best practices in the integrity compliance field. This publication is the latest step in that ongoing effort.

This publication seeks to incorporate not only well-established best practices in the integrity compliance area, but also the accumulated experience of the Integrity Compliance Office over nearly 15 years of continued engagement with Small- and Medium-Sized Enterprises (SMEs) and other types of companies around the world. We hope that SMEs will continue to be drivers of not only sustainable economic growth, but also the creation of a business climate across sectors and geographies in which fraud and corruption are not tolerated. By raising awareness and understanding of integrity compliance best practice and fostering greater engagement by SMEs on this important topic, we can support better business practices and help advance impactful development around the world.

Mouhamadou Diagne
World Bank Integrity Vice President

Acknowledgments

This Guide is a collaborative work between the World Bank Integrity Vice Presidency (INT) and the Ministry of Justice, Republic of Korea (MOJ).

The World Bank team, led by Lisa Miller (Head, World Bank Integrity Compliance Office (ICO)), includes Joseph Mauro (Senior Counsel-Integrity Compliance Specialist, ICO), Jihoon Cho (Integrity Compliance Analyst, ICO), Vedran Aladrovic (Project and Learning Tools Development Coordinator, ICO), Yeawon Choi (Intern, ICO), James David Fielder (former Senior Counsel, ICO), Howard Dean (former Senior Investigator, INT), Gordon De Villiers (Forensic Accountant, INT), Jin Ho Kim (former Senior Litigator, INT), Bernardo Becker Fontana (former Investigator, INT), Eunwoo Lee (former Consultant, ICO), and Tiange Chen (former Intern, ICO). The team is especially grateful for the support of Mouhamadou Diagne (Vice President, INT) and Alan Bacarese (Director of Investigations, Strategy and Operations, INT).

The Guide benefitted from peer review by several World Bank colleagues, including Ceri Wyn Lawley (Chief Compliance Officer, Office of the IFC Chief Compliance Officer, International Finance Corporation (IFC)), Jamieson Smith (Chief Suspension and Debarment Officer, World Bank Office of Suspension and Debarment), Roberta Berzero (Senior Investigator, INT), Daniel Nikolits (External Affairs Officer, World Bank External and Corporate Relations), and Yannick Stephant (former Senior Risk Officer, IFC Business Risk, IFC).

The team expresses its appreciation to Mayya Revzina (Senior Publishing Officer, World Bank Information and Technology Solutions, Knowledge and Information Services) for her expert guidance and editorial inputs.

The team also wishes to thank ICO colleagues, Christine Walsh (Integrity Compliance Analyst, ICO), Thilda Outhuok (Integrity Compliance Analyst, ICO), and Gwendoline Plumley (Integrity Compliance Assistant, ICO) for their assistance.

The Guide benefitted from review by MOJ team within the International Legal Advisory Division, including Donghwan Shin (Director-Senior Prosecutor), Sunggic Lee (Vice Director-Public Prosecutor), Dahye Park (Deputy Director), Sangha Lee (Deputy Officer), Yunseong Kang (Public Service Advocate). The team also expresses its appreciation to Inhye Sim (Deputy Director), Hyunjoon Hwang (Deputy Director), Eunju Yun (Deputy Officer), Seungmin Shin (Public Service Advocate), Youngmi Noh (English Translator), and Sooyoung Ahn (English Translator, International Legal Policy Division) for editorial inputs.

The MOJ team is especially grateful for the support of Woojung Shim (Acting Minister of Justice, MOJ) and Sangyeop Koo (Deputy Minister for Legal Affairs, MOJ).

The MOJ team is especially grateful for the support of Woo Jung Shim (Acting Minister of Justice, MOJ) and Sang-yeop Koo (Deputy Minister of Justice, MOJ).

The team apologizes to any individuals or organizations inadvertently omitted from this list and expresses its gratitude to all who contributed to this Guide, including those whose names may not appear here.

Contents

Acknowledgments	005
Introduction	008
Core Principles	011
<i>Risk Assessment</i>	013
<i>Prohibition of Misconduct</i>	016
<i>Ongoing Leadership from Management</i>	020
<i>Integrity Function</i>	023
<i>Decision-making Processes</i>	025
<i>Access to the ICP</i>	026
<i>Advice and Guidance</i>	027
<i>Duty to Report</i>	029
<i>Whistleblowing Channels</i>	031
<i>Investigation and Remediation Procedures</i>	032
<i>Training, Communication, and Collective Action</i>	035
<i>Integrity Compliance Training</i>	036
<i>Communication</i>	039
<i>Collective Action</i>	041

Internal Controls	043
<i>Seeking and Obtaining Business</i>	044
<i>Employee Due Diligence</i>	046
<i>Employment Contracts and Integrity Certifications</i>	048
<i>Conflicts of Interest</i>	051
<i>Business Partnerships and Combinations</i>	053
<i>Financial Controls</i>	061
<i>Audits</i>	063
<i>Gifts, Entertainment, Travel, and Hospitality</i>	065
<i>Political and Charitable Donations, and Sponsorships</i>	067
<i>Facilitation Payments</i>	069
<i>Incentives</i>	070
<i>Disciplinary Mechanisms</i>	072
<i>Recordkeeping</i>	074
Conclusion	076

Introduction

Small and medium-sized enterprises, or “SMEs,” play a major role in global economic development. For example, SMEs account for a significant number of employment opportunities and a large portion of economic activity in many low-income and lower-middle-income countries. Yet, compared to larger companies, SMEs can be particularly exposed to increased risks of corrupt activity, such as bribery, fraud, and collusion. (This Guide refers to all such unlawful practices as “misconduct.”) A great deal has been written about how companies can guard against misconduct by adopting integrity compliance programs or “ICPs.” However, much of that guidance focuses on large companies that have the resources to deploy high-priced safeguards and automated tools. This Guide seeks to provide SMEs with a useful framework for developing effective ICPs that fit their own business models, budgets, and risk profiles.

It should be stressed at the outset that having in place an effective ICP should be viewed as a competitive advantage regardless of a company’s size. A strong ICP not only should help to reduce the risk of misconduct, but also can make companies stand out among competitors. For example, an ICP may increase an SME’s chances of winning contracts from multinational companies or procurement agencies looking for ethical partners. An ICP can also:

- enhance a company’s attractiveness to investors,
- improve a company’s ability to attract competitive financing,
- enhance a company’s attractiveness to ethics-minded business partners,
- attract ethics-minded employment candidates,
- increase opportunities for long-term relationships with business partners,
- enhance control and oversight of business decisions and finances, and
- protect against financial penalties and other costs associated with misconduct, such as litigation, blacklisting, and reputational harm.

This Guide is intended to serve as a distillation of prevailing best practices and guidelines, as set out by leading national and international institutions. Numerous SMEs around the world have worked with the World Bank Integrity Compliance Office, or “ICO,” to develop creative strategies for devising and implementing ICPs intended to combat the risk of misconduct in their operations and, even more broadly, among their business networks. Some of these strategies are described in this Guide.

This Guide is intended for informational purposes only; it does not constitute legal advice and should not be relied upon as such. Neither the World Bank nor any authors bear any responsibility for actions undertaken in connection with this Guide. In addition, the Guide neither establishes nor confers any rights. Every company should analyze its own risks and legal obligations when designing and implementing an ICP as appropriate in its unique circumstances. This Guide does not contain a complete collection of every issue that an ICP should address in all situations. Detailed guidelines, templates, and legal directives on the topics discussed in this Guide can be found in numerous publications, including, among others, the World Bank's [Integrity Compliance Guidelines](#), the [MDB General Principles for Business Integrity Programmes](#), and other resources like those available via the [Integrity Compliance Knowledge Sharing Platform](#) funded by the Korea-World Bank Partnership Facility. It is hoped that this Guide—which explains certain core principles, internal controls, and essential elements of ICPs—will be of real, practical value for SMEs seeking to build a culture of integrity in their businesses and communities.

Terms and Abbreviations Used in this Guide

Term or Abbreviation	Definition
Business partners	External parties working with a company, such as agents, representatives, consultants, financiers and bankers, investors, brokers, intermediaries, distributors, suppliers, vendors, subcontractors, subconsultants, consortium partners, joint venture partners, and acquisition targets.
CCO	Chief Compliance Officer. (As used in this Guide, “CCO” denotes the person with overall responsibility for a company’s ICP, regardless of the person’s actual title.)
Collective action	Collaborative initiatives with other companies or organizations regarding integrity compliance.
G&E	Gifts, entertainment, travel expenses, and other hospitality.
General manager	As used in this Guide, “general manager” denotes the top official within a company, regardless of the person’s actual title.
Guide	Integrity Compliance Programs for SMEs: Practical Guidance and Resources.
ICO	World Bank Integrity Compliance Office.
ICP	Integrity Compliance Program.
INT	World Bank Integrity Vice Presidency.
Integrity function	The CCO and additional employees who are assigned responsibility for specific ICP tasks within a company.
Misconduct	Unlawful practices related to business integrity and corruption, such as bribery, fraud, collusion, and others.
Public officials	Individuals who serve in government, political parties, state-owned enterprises, international financial institutions, or other public functions.
Risk-based	An approach in which more attention and resources are dedicated to the more critical risks.
SMEs	Small and medium-sized enterprises.

Core Principles

The primary goal of an ICP is to identify a company's integrity risks and effectively address them. In that regard, an ICP and related controls should be designed to:

- prevent misconduct from occurring,
- detect any misconduct that does occur,
- fully investigate allegations of misconduct, and
- properly remediate any misconduct that is found to have occurred.

Types of misconduct include bribery, corruption, fraud, collusion, coercion, money laundering, bid rigging, and a variety of other unlawful practices. The degree to which each type of misconduct poses a risk varies by company. Yet, regardless of a company's particular circumstances, certain core principles should serve as the foundation of every ICP. These include:

- the preparation of a thorough risk assessment to inform ICP development,
- the prohibition of relevant misconduct,
- ongoing leadership from company management, including not only setting an appropriate so-called "tone from the top" and "tone from the middle" (with both words and actions), but also taking steps to incentivize compliance with the ICP and a corporate culture of integrity,
- the establishment of an integrity function, with adequate levels of independence, autonomy, and authority, as well as appropriate reporting lines and sufficient resources,
- the establishment of appropriate decision-making processes for important transactions,
- ready access to the documents comprising the ICP for company employees and business partners as relevant,
- the establishment of channels for providing ICP-related advice and guidance,
- appropriate requirements to report suspected misconduct,
- the establishment of channels to report suspected misconduct confidentially or anonymously as allowed under applicable law, and without fear of retaliation,
- the implementation of protocols for investigating misconduct and taking remedial actions if misconduct is found to have occurred, and
- training, communication, and collective action activities.

These principles, and how SMEs can seek to effectively incorporate them into an ICP, are detailed in this section of the Guide.



Risk Assessment

Risk assessment is the foundational element of an ICP. Before developing or updating an ICP, a company should thoroughly evaluate the integrity risks it faces in its operations (e.g., areas most susceptible to misconduct). That way, ICP protocols and controls can be designed to address the most critical risk areas and threats. Indeed, ICP development and implementation should be informed by the risks that have been identified and should be tailored accordingly. Importantly, senior company leaders, including any board of directors, should provide resources and support for the risk assessment process. Risk assessments should:

Have a broad scope

Risk assessments should cover all company operations, including any subsidiaries or controlled affiliates. All transactions and partnerships (e.g., joint ventures, material supplier relationships) should be considered as well.

Include the right personnel

Risk assessments can be conducted internally or by outside experts depending on the circumstances. In either case, company leaders should be closely involved, including:

- the top official within the company (referred to in this Guide as the “general manager”),
- the person who will have overall responsibility for the ICP (referred to in this Guide as the Chief Compliance Officer or “CCO”; other titles often used for this position include Chief Ethics Officer, Ethics & Compliance Officer, Chief Integrity Officer, and others), and
- other senior company leaders, as well as the individuals who will be responsible for designing, implementing, and overseeing the ICP.

In that regard, it is important to include personnel from all relevant functions in the risk review process (e.g., compliance, legal, risk management, finance, internal audit, human resources, procurement, sales, business development).

Identify all relevant risks

A broad scope of risks should be considered. In addition, companies may find it useful to consult with organizations, such as local chambers of commerce, trade unions, or industry associations to learn about the prevailing risks in their regions of operation and industries.

Examples of risk categories

- **Geographical and contextual risk.** Each jurisdiction poses different risks based on its business environment, laws and regulations, degree of enforcement, cultural norms, and business practices.
- **Business sector risk.** Certain industries and sectors pose greater risks. For example, bribery risks may be higher where there are frequent interactions with officials in government, political parties, state-owned enterprises, or other public functions (e.g., employees of international financial institutions). (These officials are collectively called “public officials” in this Guide.) For instance, transactions, such as permitting, licensing, and customs clearance may carry added risk. Similarly, fraud risks may be increased in bidding for public contracts, and collusion risks may be elevated where there are a limited number of companies in a particular industry or where employees interact autonomously with public officials.
- **Transactional risk.** Different transactions pose different risks. Factors to consider include the nature of the transaction, the counterparties, the subject matter, and how important the transaction is to any of the parties involved.
- **Business partnership risk.** Integrity risks also may be posed by external parties involved in the company’s business, such as business partners. Engagements with agents, brokers, and distributors may create particularly acute risks.
- **Business opportunity risk.** Certain opportunities pose greater risks than others, particularly those with higher monetary value or complexity.

Prioritize the key risks

Once the company has identified the relevant threats, it is important to prioritize them based on their likelihood and potential impact. The ICP should be designed to follow a “risk-based” approach – i.e., more resources and attention are devoted to the more critical risks. Companies should pay special attention to any prior allegations of misconduct or conflicts of interest.

Recur periodically

The risk assessment process should be repeated regularly (ideally at least annually) to capture any changes to the company’s operations or legal obligations. After each review, the ICP should be updated accordingly to reflect any new risks or different levels of risk.

Examples of Transactions that may Carry Elevated Risks

- *High monetary value.*
- *Use of agents.*
- *Interactions with public officials (e.g., public procurement, permitting and licensing, inspections, customs clearance, employee work permits and visas).*
- *Development of new products.*
- *Launch of new business lines.*
- *Entry into new markets.*
- *Work in high-risk jurisdictions.*
- *Emergency circumstances that may require rapid changes to business processes.*
- *Participation in transactions (e.g., making or receiving payment) without knowing the counterparty's beneficial owners where necessary.*

Prohibition of Misconduct

Companies should adopt clear rules prohibiting all relevant types of misconduct. Typically, such rules are published in a code of conduct that is distributed to all employees and made available to the public. Even if an SME generally uses informal business processes, it should establish a written policy prohibiting misconduct and clarifying the company's integrity compliance rules. Having in place such a written policy helps to ensure that business partners, managers, and employees at all levels (including any board members or senior executives) know what is expected of them. Questions to consider in this area include:

Are all relevant types of misconduct prohibited?

Companies should consider all laws and regulations that apply to their businesses. This includes the laws in all jurisdictions where business is conducted, as well as rules that may only apply to certain projects or tenders, such as the frameworks applicable to companies working with World Bank entities or receiving World Bank funds (e.g., <https://www.worldbank.org/en/projects-operations/products-and-services/procurement-projects-programs>). In addition, companies may identify other types of misconduct that they wish to prohibit.

Is it clear which behaviors are prohibited?

Individuals subject to the ICP must understand exactly what they can and cannot do, as well as the potential consequences of violations.

Is the prohibition of misconduct being communicated clearly?

Rules on misconduct should be communicated simply, universally, and unequivocally. They should clearly apply to everyone who works for or represents the company, as well as business partners to the extent appropriate.

Sample Types of Misconduct

From the World Bank Guidelines on Preventing and Combating Fraud and Corruption in Projects Financed by IBRD [International Bank for Reconstruction and Development] Loans and IDA [International Development Association] Credits and Grants (revised as of July 1, 2016):

- a) *A “corrupt practice” is the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.*
- b) *A “fraudulent practice” is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation.*
- c) *A “collusive practice” is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party.*
- d) *A “coercive practice” is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.*
- e) *An “obstructive practice” is (i) deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a [World] Bank investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or (ii) acts intended to materially impede the exercise of the [World] Bank’s contractual rights of audit or access to information.*

From the Republic of Korea Improper Solicitation and Graft Act (revised as of December 7, 2021):

Article 5 (Prohibition of Improper Solicitations)

(1) No person shall make any of the following improper solicitations to any public servant, etc. performing his or her duties, directly or through a third party:

1. *Soliciting to process, in violation of statutes, such tasks as authorization, permission, license, patent, approval, inspection, qualification, test, certification, or verification, for which statutes (including Ordinances and Rules; hereinafter the same shall apply) prescribe requirements and which should be processed upon application by a duty-related party;*

2. *Soliciting to mitigate or remit administrative dispositions or punishments, such as cancellation of authorization or permission, and imposition of taxes, charges, administrative fines, penalty surcharges, charges for compelling compliance, penalties, or disciplinary actions, in violation of statutes;*
3. *Soliciting to intervene in or exert influence on the recruitment, selection, employment, promotion, assignment or reassignment of a public servant, etc., or any other personnel matter relating thereto, in violation of statutes or regulations;*
4. *Soliciting to select or reject a person, in violation of statutes, for a position which intervenes in the decision-making of a public institution, such as a member of various deliberation, decision-making, and arbitration committees, and a member of a committee for a test or screening administered by a public institution;*
5. *Soliciting to select or reject a specific individual, organization, or juridical person to be issued an award, prize, or to be chosen as an outstanding institution, person, or scholarship recipient, all of which activities are conducted under the auspice of a public institution, in violation of statutes or regulations;*
6. *Soliciting to disclose, in violation of statutes, duty-related confidential information on tender, auction, development, examination, patent, military affairs, taxation, etc.;*
7. *Soliciting to select or reject a specific individual, organization, or juridical person as a party to a contract, in violation of statutes governing contracts;*
8. *Soliciting to intervene or exert influence so that subsidies, incentives, contributions, investments, grants, funds, etc., are assigned to, provided to, invested in, deposited in, lent to, contributed to, or financed to a specific individual, organization, or juridical person, in violation of statutes;*
9. *Soliciting to allow a specific individual, organization, or juridical person to buy, exchange, use, benefit from, or possess goods and services that are produced, supplied, or managed by public institutions, at prices different from what is prescribed by statutes, or against normal transaction practices;*
10. *Soliciting to handle or manipulate the affairs of schools of each level, such as admission, grades, performance tests, thesis review, or conferment of degrees, in violation of statutes or regulations;*
11. *Soliciting to process affairs related to military service, such as physical examination for military service, assignment to a military unit, or appointment to a position, in violation of statutes;*
12. *Soliciting to perform various affairs of public institutions in relation to assessment, judgment, or acknowledgment in violation of statutes or regulations, or to manipulate the results thereof;*

13. *Soliciting to make a specific individual, organization, or juridical person subject to or exempt from administrative guidance, enforcement activities, audit, or investigation; to manipulate the outcome thereof; or to ignore any illegality, in violation of statutes;*
14. *Soliciting to handle investigation of a case, trial, adjudication, decision, mediation, arbitration, reconciliation, execution of punishment, the guidance on treatment and safe custody of inmates, or other equivalent affairs, in violation of statutes or regulations;*
15. *Soliciting a public servant, etc. to act beyond the limits of his or her position and authority granted by statutes, or to take any action for which he or she lacks legitimate authority, regarding any and all affairs that may be the subject matter of improper solicitation as prescribed by subparagraphs 1 through 14.*

** The Improper Solicitation and Graft Act applies to all public institutions and employees (constitutional institutions, central administrative agencies, local governments), as well as municipal or provincial offices of education, and public service-related organizations and employees (private and public schools of various levels, educational corporations under the Private School Act, and media companies under Article 2.12 of the Act on Press Arbitration and Remedies, etc.).*

Ongoing Leadership from Management

Senior managers and any board of directors should demonstrate strong, explicit, visible, and active support for the ICP, in both letter and spirit. They should widely circulate messages to reinforce the company's commitment to ethical conduct and integrity, such as by email reminders, statements at company events, and periodic talks with groups of employees or business partners. The company should also consider including a statement of support, signed by the company's senior manager(s), at the front of core ICP documents like a code of conduct.

Mid-level managers (i.e., middle management) should make similar demonstrations of support. Mid-level managers play a key role in spreading the integrity compliance message throughout a company with both their words and their actions.

The following principles should be considered:

Daily interactions and dialogue.

In the SME context, managers often are more visible to employees on a day-to-day basis than in large companies, so their actions and words may carry added weight. SME managers may be able to speak directly with all employees about the need for ethical behavior and explain how any prior acts of misconduct were handled. Open and transparent dialogue should be encouraged. Also, managers should be empowered and educated to communicate directly with clients and business partners about the company's values and integrity compliance rules.

Personal involvement.

SME managers often need to be more personally involved than their counterparts at large companies in designing internal controls and issuing approvals. It is particularly important to involve managers at all levels during the ICP design phase. This helps ensure that internal controls are consistent with existing good practices within the company and can be integrated into the company's existing policies, procedures, and day-to-day business operations. Regarding approvals, for example, an SME may examine the misconduct risks associated with company donations and decide that any such donation requires advance approval from the general manager or board of directors, with prior input from the CCO. Additionally, management personnel should ensure that appropriate remedial measures, including disciplinary actions as relevant, are undertaken in cases of substantiated ICP violations.

Regular engagement with and involvement of the CCO.

The CCO should be involved in, or at least should be regularly kept apprised of, corporate matters that may impact the ICP, such as changes in corporate structure, key employees, or reporting lines.

Regular updates from the CCO.

Senior company leaders, and any board of directors, should receive regular updates about the ICP from the CCO (e.g., quarterly reports and ad hoc reports if material matters arise in the interim). Updates about the ICP should be communicated to downstream managers as well for their attention and follow-up as needed. Updates should address matters such as:

- changes in the company's risk profile (e.g., development of new products, launch of new business lines, entry into new markets, corporate reorganizations),
- changes in laws and regulations affecting the ICP,
- revisions to ICP documents or rules to address, for example, lessons learned following misconduct investigations or system weaknesses identified through audits,
- progress implementing ICP protocols throughout the business, as well as any challenges that have arisen,
- an analysis of questions being asked by employees that may reveal trends or patterns suggesting systemic issues, or areas that are unclear and may warrant clarification or further instructions, and
- reports of suspected misconduct and how they are handled.

Sample High-level Management Support Statement

[Company] is committed to doing business in an ethical manner, with business integrity, and in accordance with all applicable laws and regulations, and to act with integrity in all business dealings. We expect all company personnel and business partners to share that commitment, to abide by the rules and principles set out in the company's integrity compliance program, and to work together to promote a culture of integrity.

Personnel and business partners should seek guidance from the company's compliance team if they are unsure of the proper action to be taken. In addition, they should speak up if they suspect that misconduct has occurred. They can report their concerns confidentially, anonymously, and without fear of retaliation through various means, including [provide contact details]. The company will review and address all reports, including by conducting investigations and taking remedial measures when appropriate.

The entire Board of Directors and management team, including me personally, are committed to ensuring that the integrity compliance program is followed and that company business is conducted with integrity. We appreciate your support and commitment as well.

[Signature]

Integrity Function

Companies should carefully consider who will have primary responsibility for ongoing ICP development and implementation. The CCO should be selected based on factors such as experience, trustworthiness, leadership skills, independence, and personal commitment to ethics and integrity. Furthermore, all but the smallest companies should assign additional employees, on a part-time basis if appropriate, to carry out specific ICP tasks such as due diligence of vendors and other parties, risk assessment, and training. Such employees should be ready to step in if the CCO is unavailable (e.g., on leave). The CCO and these additional employees are collectively called the “integrity function.” SMEs should consider the following principles when establishing integrity functions to fit their operations and risk profiles:

Seniority, independence, and authority.

The CCO should be empowered to make decisions without pressure from internal or external parties. The CCO should have sufficient seniority and authority to command respect within the company, including from senior managers. In addition, the CCO should have independent access, and direct reporting lines, to the company’s general manager and any board of directors (especially any independent directors or committees, like an audit committee), and the CCO should not be subject to discipline or replacement without their consent. Even in SMEs that are governed by a single individual or a small group of owners, steps can be taken to insulate the CCO from business pressure. For example, clearly defining the CCO’s authority in written terms of reference and ensuring direct access to independent advisors such as external counsel may help to avoid undue influence.



Autonomy.

Just as the CCO should be able to act independently, other members of the integrity function should be empowered to carry out their ICP responsibilities without external pressure. Written policies and terms of reference should establish that they report directly to the CCO on ICP matters and will not be subject to retaliation for faithfully executing their compliance duties.

Part-time employees and conflicts of interest.

While it is a best practice to appoint full-time staff to the integrity function, SMEs with limited resources may need to rely on part-time assistance from existing personnel. In such cases, companies should carefully consider potential conflicts of interest. For example, companies may choose to appoint an existing General Counsel or Chief Financial Officer to serve as CCO on a part-time basis. This may be a good choice based on the individual's expertise, seniority, and degree of independence from the business. However, conflicts can arise between the CCO's ICP role and legal or financial roles—for example, if an allegation of misconduct arises against a member of the legal or finance teams. Accordingly, companies should adopt written protocols for avoiding and managing such conflicts, to avoid even an appearance of impropriety. In the example noted above, it may be appropriate to inform employees that they can report suspected misconduct to someone other than the CCO if a member of the CCO's team is implicated. Appropriate recusal mechanisms can be adopted so that someone other than the CCO takes responsibility for addressing such allegations.

Additionally, certain employees may have inherent conflicts of interest that prevent them from serving in the integrity function. For example, it is typically not advisable to appoint sales and business development staff to part-time integrity roles, because it may be difficult for them to be completely objective in vetting their own transactions. As such, companies often select employees in areas such as legal, finance, internal audit, or human resources to serve in the integrity function.

Training.

It is critical for the CCO and other members of the integrity function to complete advanced integrity training suitable for their roles. Such training should be completed not only at the time of taking the position, but also on an ongoing basis thereafter. This is especially important for SMEs that do not have the resources to hire established compliance experts. Trainings on how to conduct due diligence, investigations, and risk assessments are commonly appropriate, among other topics.

Decision-making Processes

Decisions within a company should be made by individuals who have an appropriate degree of authority and expertise in consideration of the value, complexity, and risk of each transaction. While SMEs may have simpler decision-making frameworks than larger companies, they still should adopt written decision protocols, as well as process workflows, for important transactions such as those described in this Guide. To that end, principles such as the following should be incorporated in ICP documents to ensure that the right individuals are involved in each transaction:

- experienced managers should be responsible for decisions that require more judgment, are of higher value, or otherwise carry greater risks,
- as appropriate, decision protocols should incorporate tools such as risk score calculations, decision trees, escalation rules, delegations of authority, limits on individuals' discretion, limits of authority as to monetary thresholds, and dual-signature requirements above certain monetary or risk thresholds,
- the CCO and integrity function should be involved in decision-making processes to the extent needed, and
- decision-makers should properly record each decision to the extent appropriate under the circumstances, including in documents that show how the company considered pertinent risk factors, any mitigating measures to be put in place, and the justification for approvals given.

Sample Considerations for Limits of Authority and Approval Matrices

- *Nature of activity.*
- *Activity risk rating.*
- *Monetary value of transaction.*
- *Nature of counterparties.*
- *Responsible person.*
- *Reviewer (e.g., for comment or validation).*
- *Approver/decision-maker.*
- *Others who should be consulted or who must concur.*
- *Others who should be informed.*

Access to the ICP

Core ICP policies and documents should be readily available to all employees, and ancillary (or supporting) documents should be similarly available to the employees who need them. In that regard, companies that have shared intranet portals or internal webpages should make ICP documents available there. Companies should also provide ICP documents directly to employees, together with training and advice on how to apply them. Employees without computer access may be given hard copies as needed, and posters may be displayed in public areas of company facilities. Companies also frequently post their codes of conduct and other core ICP documents on public-facing websites, to inform customers and business partners about their values and expectations.

The content of the documents should be accessible as well. Legal jargon should be minimized, and instructions should be understandable and practical. It may be particularly helpful to include real-world scenarios that are relatable to employees. This is especially important for companies whose employees may have less formal education or training. Graphics and pictorial descriptions may be helpful as well. Documents should be translated as necessary for employees to understand the rules that apply to them.

Sample ICP Accessibility Strategies

Location

- *Copies provided to employees.*
- *Hard copies in common areas.*
- *Posted on company intranet.*
- *Summary posters in company offices and project sites.*
- *Posted on company website.*

Content

- *Simple and clear language.*
- *Workflow charts and process diagrams.*
- *Pictorial descriptions.*

Advice and Guidance

Companies should be able to provide timely advice and guidance about the ICP to employees, and to external parties where relevant. For example, employees may need advice when they do not know whether they have witnessed misconduct, or when they are unsure how to respond to an inappropriate demand from an external party (or from their own supervisors). Secure and confidential channels for seeking guidance should be accessible to all employees, and others as relevant, including on an urgent basis and in multiple languages as needed. It should be made clear to employees that they should seek advice whenever they are unsure of how to proceed or of the best course of action. Companies also should provide the option to seek guidance anonymously to the extent permissible under applicable law.

While large companies often install dedicated ICP telephone lines, email addresses, and webform communication tools, fewer channels may be required in the SME context, especially if all employees work in the same office or time zone. SMEs often simply share the CCO's telephone number and email address (or a separate email address that is routed to the CCO, such as "integrity@company.com") and inform all employees, and others as relevant, that they can contact the CCO at any time with questions or concerns. Placing confidential inquiry boxes in offices, warehouses, and other company facilities also may be used for this purpose.

Note

If anything is unclear, employees should know to ask before they act!

Companies should track requests for advice and look for any trends or patterns that might suggest systemic issues, or areas that are unclear and may warrant clarification in relevant ICP documents or additional training. If any such matters are identified, the company should seek to address them and mitigate any associated risks.

Example Situation: Monitoring and Revising an ICP in Practice

One company's compliance team decided to track requests for guidance by categories (e.g., bidding, gifts and entertainment, business partners) and automated collection of the data for review on a weekly basis. After a few months of data review, the company identified several similar questions that had been submitted from the same region pertaining to gifts and entertainment. In particular, employees in that region had asked repeatedly about the allowability of purchasing a cup of coffee or tea for business counterparts, sometimes including government officials, following business meetings, which was understood to be a custom in the region. The responses consistently advised that such expenses, regardless of value, needed to be submitted for approval by the appropriate compliance team member pursuant to company rules in effect at the time.

The compliance team then looked into approval requests received for gift- and entertainment-related expenses in the region during the same time period. It found that the number of such requests had dropped significantly without explanation. The compliance team then reached out again to some of the advice seekers to ask whether the practice of offering coffee or tea following a business meeting had stopped. The compliance team learned that was not the case but, rather, the employees had simply begun paying for the cups of coffee or tea personally, and not seeking reimbursement, as they found it to be too inefficient to seek approval in each instance.

The compliance team of course noted that such activity was in contravention of the ICP, leading to minor reprimands for relevant employees. However, the compliance team also recognized that the ICP was too restrictive in this area and could benefit from revision. As a result, the gift and entertainment policy was revised to set a low-value threshold below which certain types of expenses, such as a cup of coffee or tea attendant to a business meeting, would still need to be tracked but would not require submission for approval. The company also held an additional training session focused on gifts and entertainment for personnel in the region. In this way, by tracking and analyzing requests for advice, the company identified and corrected a weakness in its ICP and increased employees' compliance.

Duty to Report

Written policies, trainings, and communications should emphasize that every employee has a duty to promptly report integrity concerns, including known or suspected misconduct, to designated personnel. Companies should extend reporting obligations to agents, representatives, and other business partners as appropriate. The scope of the reporting obligation, and protocols for submitting reports, should be tailored to each company's circumstances and applicable laws. In locations where it may be legally impermissible to require that all misconduct be reported, companies should require such reporting to the extent possible and otherwise strongly encourage it. Clear instructions and periodic reminders should address topics such as:

- the duty to report,
- available channels for reporting and how to use them,
- the ability to report anonymously, to the extent legally permissible,
- disciplinary action that may result from failing to report when required,
- protocols in place to protect the confidentiality of whistleblowers and their reports,
- the company's strict prohibition of retaliation against those who submit reports in good faith or cooperate in investigations or audits, and
- disciplinary action that may result if a person is found to have engaged in retaliatory acts.

Sample Employment Contract Clause

[Employee] understands and agrees that [employee] will report any suspected or actual violations of [company's] integrity compliance program to designated persons. Any failure to report will itself constitute a violation of the integrity compliance program subject to appropriate disciplinary action in accordance with company policies and applicable law.

SMEs may have advantages and disadvantages in this area. While smaller companies may lack the resources to install state-of-the-art electronic whistleblowing systems, they may have a greater degree of familiarity and personal interaction among employees and supervisors, which can facilitate direct reporting. However, any successful reporting system depends on maintaining an atmosphere of trust and accountability. Small companies may need to provide additional information to assure employees that their reports will remain confidential. Prompt feedback and support should be provided to employees who have raised concerns.

Sample Reporting Form

The below text is based on the online form for submitting reports to INT, available at www.worldbank.org/fraudandcorruption.

Thank you for your vigilance. We rely on people like you to ensure that company projects are executed with integrity and benefit the people they are designed to help. If you have a specific concern, please fill out this short form, which is important for investigators in the company's integrity function to properly evaluate your report.

*What is this report about? Name of the project, contract name/reference number (if applicable)
Please describe your concern.*

All information provided will be treated in the strictest confidence. The company will still review your report even if you wish to remain anonymous. The company will not disclose any information that may reveal your identity without your consent, unless required by law. If you agree to be identified, please provide us with your contact information. Please provide us with at least an email address so that we may contact you for additional information or clarification.

If you have any evidence to support your report, please attach files here.

Whistleblowing Channels

Companies should provide multiple channels through which allegations or concerns can be raised, on a named or anonymous basis to the extent permissible under applicable law. Employees should be able to submit reports at any time and in any language used by the company. Each company's reporting system should fit its operations, personnel, budget, and risk profile. Care should be taken to ensure confidentiality consistent with applicable laws, particularly when a company's smaller headcount may make it easier for employees to identify a whistleblower.

Sample Types of Reporting Channels

- *Directly to the employee's supervisor, to be forwarded onward to the integrity function.*
- *Directly to the CCO or other integrity function personnel.*
- *Email addresses routed to the CCO or integrity function, such as "integrity@company.com."*
- *Dedicated telephone lines answered by the CCO or other members of the integrity function.*
- *Dedicated fax numbers or physical mailing addresses for submitting reports to the CCO or integrity function.*
- *Smartphone apps through which reports can be submitted directly to the CCO or integrity function.*
- *Physical drop boxes in company offices, warehouses, and other facilities that are checked regularly by the CCO or members of the integrity function for any reports or questions about the ICP.*
- *Telephone or webform reporting hotlines managed by third-party firms, which provide an added layer of confidentiality before the reports are forwarded onward to the integrity function.*
- *Links on the company's external website or intranet portal through which reports can be submitted to the CCO or integrity function.*

Investigation and Remediation Procedures

No matter how robust a company's ICP may be, it is quite possible that a company will encounter a bad actor at some point. Whether suspected misconduct is internal or external to a company, company leaders must be promptly informed (e.g., by the CCO or integrity function) about any wrongdoing that may have occurred or may be about to occur in connection with company business. Accordingly, in addition to emphasizing employees' duty to report suspected misconduct and providing effective mechanisms for reporting, as discussed above, companies should establish suitable protocols for conducting internal investigations and taking remedial actions in connection with such reports, all in accordance with applicable law.

More specifically, companies should adopt written investigation protocols that fit their operations and risk profiles. Appropriate decision processes should be followed during investigations and after the discovery of any misconduct. To the extent possible, SMEs should develop investigation protocols that take advantage of their smaller size and closer proximity among staff. For example, the General Counsel or CCO may be able to conduct certain investigations without external counsel or auditors. Companies also should establish procedures for undertaking remedial measures if an investigation substantiates findings of misconduct. Factors such as the following should be incorporated in protocols for investigations and remedial actions, to the extent appropriate for each company:

Acts to be investigated.

The investigation protocol should provide examples of the types of behavior that may result in an investigation and a finding that disciplinary action is warranted.

Standards of proof.

The protocol should set out appropriate standards of proof to be used in investigations. Typically, a "preponderance of the evidence" or "more likely than not" standard is used.

Subjects of investigations.

The protocol should clarify who can be the subject of an investigation. Employees, business partners, and members of any board of directors or governing body should all be potential subjects of an investigation to the extent permissible under applicable law.

Responsibility for investigations.

The protocol should clarify who is responsible for initiating and conducting investigations, and the role of each individual in the process. Decisions about whether to investigate an allegation or suspicion should be based on proper criteria and made at a sufficiently high level within the company, including at the general manager or CCO level where appropriate. Depending on an SME's size and business needs, investigative teams may consist of internal personnel, external investigators, or a combination.

Documentation.

The investigation protocol should mandate detailed recordkeeping processes to ensure that investigations are thoroughly documented, from the initial report through follow-up on any remedial actions. The protocol should also clarify which records might be part of an investigative review and what access restrictions may apply (e.g., possible restrictions and/or consent requirements relating to personal data under applicable law). Appropriate recordkeeping allows companies to track and analyze investigations and to use the findings to identify patterns of misconduct or weaknesses in internal controls.

Timeliness.

The protocol should require investigations to be resolved in a timely manner so that remedial actions can be implemented as soon as possible.

Due process.

It is critical to ensure that investigations are conducted fairly and impartially. The investigation protocol should adequately describe the rights of those under investigation, consistent with applicable law.

Cooperation.

The protocol should reiterate the requirement for employees and business partners to cooperate with investigations into alleged misconduct, whether conducted by the company directly or by a third party, as directed by management. This requirement should be built into the ICP and possibly set out in employee and business partner contracts as well.

Remedial measures.

A thorough investigation should identify not only the underlying facts, but also any vulnerabilities in the company's operations or internal controls that contributed to the misconduct. The protocol should state that senior managers and the CCO will be involved in coordinating updates to

company processes or ICP protocols as necessary following the discovery of misconduct, and in imposing disciplinary or remedial action as appropriate.

Reporting to the Board of Directors.

Matters pertaining to reports of misconduct, outcomes of investigations, and remedial measures should be a standing topic in regular communications from the CCO to senior management and any board of directors, as well as in ad hoc communications when material issues arise.

Training, Communication, and Collective Action

An ICP is only as effective as the individuals implementing it. It is critical that employees not only understand the applicable rules, but also appreciate why following them is essential. Information should be disseminated through channels such as:

- integrity compliance trainings,
- communications about the ICP, and
- collaborative initiatives with other companies and organizations, often called “collective action,” to promote integrity compliance more broadly.

Such activities can create connections that help to build a culture of integrity and transparency in companies and communities. In this regard, SMEs often can take advantage of direct and personal interactions more readily than larger companies, especially if they have simpler organizational structures or are well integrated in their local business communities. These essential elements should be considered together but will be discussed in turn in the subsections that follow.

Integrity Compliance Training

Training and communication are the lynchpins of an effective ICP. Companies should seek to ensure that all employees not only understand their responsibilities under the ICP, but also believe in the company's commitment to ethical conduct and business integrity. To that end, integrity trainings should:

- credibly convey the company's values and dedication to compliance,
- clearly explain employees' obligations under the ICP, as well as the consequences of violations, and
- reasonably articulate the rationale behind ICP rules and processes.

Training on core ICP policies should be mandated for all employees as soon as they join the company and on a regular basis thereafter. Refresher training generally should be provided at least annually, and mini-trainings can be provided more frequently on discrete topics.

Examples of Training Approaches

- *Online training modules—more than just “click-through” pages.*
- *In-person training (e.g., presentations, interactive activities).*
- *Small-group discussions.*
- *Real-world case scenarios and role-playing exercises.*

In addition, specialized integrity training should be required for certain groups as necessary. For example, members of the integrity function typically should complete advanced training relevant to their roles. Management personnel also might be provided with more in-depth training on key areas of the ICP and with respect to setting the proper tone across the company and among their teams. It also may be necessary to require special training for employees who perform sensitive functions like procurement, business development, sales, human resources, and finance, to sensitize them to pertinent risks and reinforce applicable controls. Similarly, targeted training should be considered for persons involved in specific activities under the ICP, such as employee or business partner due diligence.

Companies also should consider providing training to business partners where appropriate. Such training may be particularly relevant for agents or other persons retained to act on the company's behalf.

Strategies such as the following may help to increase the effectiveness of training efforts while minimizing costs:

External modules and templates.

The global anti-corruption community offers a rich set of training modules and template documents, many of which are available online for no cost or for reduced fees based on company size. Sample training templates and modules, of course, should be tailored for use to each company's operations, personnel, and risk profile.

Train the trainer.

Especially in companies without in-house compliance expertise, it may be appropriate for the CCO to undertake advanced training from an external source and then become the designated trainer for other company personnel. The CCO also can train other individuals to become trainers, especially members of the integrity function or managers in other departments or locations.

Simple language.

Training programs and materials should use simple, clear wording, avoid "legalese," and be translated as necessary so that all employees can clearly understand their rights and obligations. As previously noted, graphics and pictorial descriptions may be helpful as well.

Meaningful updates.

Refresher trainings should not simply regurgitate the same information, but should include updates, in format and substance, to keep employees engaged and informed. Interactive activities and entertaining graphics can help boost interest and attention.

Case studies and examples.

It is important to include case studies on the types of real-world scenarios that employees may face with respect to potential misconduct. Actual events that have occurred at the company can be discussed as well, including as lessons learned, to the extent appropriate.

Knowledge testing.

It also is important to ensure that employees understand the material presented. In this respect, companies may use strategies such as brief quizzes or discussions to evaluate employees' comprehension.

Communication

Together with ICP training, effective communication is the bedrock upon which employee understanding and buy-in are built. ICP-related communications should explain all pertinent rules and processes, and should be delivered in a clear, timely, and credible fashion. Senior company leaders should publicly express their full support for the ICP and should stress that the company will not tolerate misconduct. It should be emphasized that senior leaders are subject to the same high standards as employees. Such statements can be directly communicated to employees and business partners and may be posted on the company's internal or external webpages as well. As with training, it is important to include case studies on the types of real-world scenarios that employees may face regarding potential misconduct, including actual events that occurred at the company to the extent appropriate.

Sample ICP Communication Strategies

- *Including introductory notes in a code of conduct or other ICP documents from top leaders such as the general manager or chairman, to emphasize that the company places the highest importance on ethics and integrity compliance.*
- *Posting video messages on compliance from company managers.*
- *Incorporating short compliance messages into meetings or workshops on other topics, such as periodic team meetings or project kick-off meetings.*
- *Incorporating reminders about the ICP into company communications on other subjects like holidays, company initiatives, or the rollout of new processes or tools.*
- *Issuing periodic company-wide emails discussing topical news or other developments related to integrity compliance, such as headlines regarding misconduct in the company's industry, or integrity-related events like International Anti-Corruption Day on December 9th each year.*
- *Incorporating information about the ICP and its implementation into published company reports, such as annual reports.*
- *Hosting integrity-related events, such as "Integrity Days" or "Integrity Weeks."*
- *Adding colorful logos or graphics on internal or external webpages to highlight the company's values and commitment to ethics and integrity compliance.*
- *Exhibiting posters, display screens, or banner stands at company facilities as a reminder about the company's values and ICP.*

- *Creating branded mobile apps with information and reminders about the ICP.*
- *Setting up periodic pop-up integrity messages that appear when employees log on to their computers.*
- *Including information about the ICP on employee business cards.*
- *Printing brief integrity compliance messages on company-branded promotional items, such as badges, stickers, mugs, calendars, pens, or magnets.*

Leading by example is an important means of integrity communication, especially in small companies with a high degree of interaction among managers and employees. Managers' actions and words should make it clear that the company does not advocate or condone obtaining business by any means necessary. For example:

- Walking away from an engagement due to integrity concerns shows that company management is committed to the ICP and doing business with integrity.
- Taking decisive disciplinary action against employees at any level, including management if warranted, further underscores that the company's leaders are committed to integrity and do not tolerate misconduct.
- Providing adequate resources and authority to the integrity function demonstrates a substantive commitment to the ICP.
- Upholding confidentiality and anti-retaliation protections for whistleblowers attests to the company's support for integrity and transparency.

Collective Action

Wherever possible, companies should collaborate with other organizations and businesses to promote integrity and encourage the development of effective ICPs. Alliances may be created with groups such as professional associations, civil society organizations, and governmental units. Examples include:

- similar companies coordinating with each other to develop a collective ICP or common set of business integrity principles under which to operate,
- extending integrity commitments and requirements throughout supply chains,
- arranging conferences to share experiences about ICP implementation,
- holding calls or meetings among interdisciplinary teams to develop best practices,
- issuing joint communications or publications on integrity topics,
- industry associations issuing common integrity principles to which their members are expected to subscribe,
- utilizing integrity pacts in which parties to a transaction agree to act with integrity in connection with the transaction, and
- jointly supporting or contributing to anti-corruption legislation or regulations.

As another example of collective action, the ICO has established a mentorship program in which it seeks to pair entities that were sanctioned by the World Bank and have met the integrity compliance conditions imposed for their release from such sanction with other entities—and SMEs in particular—that are currently sanctioned by the World Bank and are working to implement their own integrity compliance controls. The mentorship program is one way in which World Bank-sanctioned SMEs in emerging markets have been able to collaborate directly with similarly situated companies and multinational corporations in their regions.

Impact of Collective Action

Collective action can help reduce the occurrence of misconduct in an industry if enough companies participate. By joining forces, companies can leverage their efforts and pool information to help reduce opportunities for misconduct. Involving other partners, such as public authorities and civil society organizations, can further increase the positive impact of such activities. For example, if companies work collectively to consistently deny requests for illicit payments from public officials seeking bribes to carry out a regular function (e.g., sign-off on customs declarations), the officials may eventually stop asking for such payments. The likelihood of such an outcome can be increased if the companies work with public authorities to identify the officials who are acting improperly, and the public authorities take appropriate remedial action regarding such officials. Civil society organizations also can play a role by monitoring related activities and offering suggestions to all parties.

Internal Controls

Companies should have effective internal controls to manage the integrity risks in their businesses. In general, more resources should be devoted to areas of greater risk, as illuminated by the company's comprehensive risk assessment. As previously noted, SME managers often interact more directly with employees than in large companies, which may allow them to employ simpler control mechanisms in certain circumstances. For example, if the CCO works in the same office as all other company personnel, it may make sense for the CCO to directly review and approve important transactions without an extended chain of review.

As detailed in this section, companies should have appropriate internal controls in the following fundamental areas, to the extent necessary for each organization:

- seeking and obtaining business,
- due diligence of employees,
- employment contracts and integrity certifications,
- conflicts of interest,
- business partners and combinations,
- financial processes,
- audits,
- gifts, entertainment, travel, and hospitality,
- political and charitable donations, and sponsorships,
- facilitation payments,
- incentives,
- disciplinary mechanisms, and
- recordkeeping.

Seeking and Obtaining Business

When misconduct arises, it is often in connection with a company's efforts to get business. Examples include sales, business development, negotiations, consortium agreements, bid qualification, tendering, and related potentially high-risk activities. SMEs may be exposed to increased risks if they operate in environments with fewer formal regulations or processes in these areas. ICP protocols should be designed to ensure that such activities comply with applicable laws and rules and are based on truthful and complete representations. Examples of policies and procedures to incorporate in ICP documents, as appropriate based on each company's circumstances, include the following:

- segregation of duties between employees responsible for sales or business development and employees responsible for preparing, reviewing, or approving bid submissions,
- protocols for storing, verifying, and disseminating information about the company's qualifications, personnel, and past performance,
- policies and procedures governing particular aspects of the bidding lifecycle (e.g., designation of responsibilities, review and verification procedures, approval requirements),
- mandatory vetting and approval rules for engagements with consortium partners and other third parties involved in efforts to obtain business (e.g., a requirement that each partner sign an agreement clearly delineating its role in the transaction and the procedures and regulations it must follow),
- protocols requiring consideration of relevant "red flags" by individuals at an appropriate level of seniority, and
- mandatory review by the integrity function or other senior managers of documents, including bids, to be submitted to external parties, such as governmental agencies or multinational companies seeking local partners. Such reviews should focus on ensuring accuracy, completeness, and compliance with all applicable laws and rules.

Examples of “Red Flags” Relating to Business Development Activities

- *Pressure to select certain subcontractors or representatives.*
- *Unauthorized disclosure of confidential information related to pricing or tender specifications.*
- *Unnecessary use of intermediaries or offshore accounts.*
- *Indications of collusive behavior (e.g., price fixing).*
- *Requests that make a person uncomfortable or that would be embarrassing if made public.*

Employee Due Diligence

One unethical employee can put an entire company at risk. Accordingly, companies should conduct careful due diligence before hiring or promotion decisions are made. Core principles include the following:

Sorting by risk.

While all employment candidates should be scrutinized to some degree, more focus should be placed on candidates that may expose the company to greater risks. The company's overall risk assessment process should guide the design of due diligence protocols. For example, it is typically appropriate to conduct deeper vetting for:

- managers, directors, and others who will have decision-making authority or the ability to influence business results,
- employees who will have access to company finances,
- hiring into sensitive functions such as legal or human resources,
- hiring into functions otherwise considered to be high-risk in the context of the company's operations (e.g., sales, business development, procurement), and
- employment candidates who have served as public officials.

Written procedures.

Due diligence procedures should be designed to shed light on whether employment candidates may pose integrity risks to the company. Factors to consider include:

- whether the candidate has connections to public officials,
- whether the candidate has engaged in misconduct, or may do so in the future,
- whether the candidate has real or apparent conflicts of interest, and
- the candidate's background, qualifications, and personal attitude toward ethics and integrity compliance.

The procedures used to collect such information should be appropriate for each company's circumstances, including applicable employment laws. For particularly sensitive hires, it may be appropriate to commission detailed background investigations by external experts. Whatever the circumstances, companies should establish suitable written procedures based on the level of integrity risk and resources available.

Note

The laws of many jurisdictions require “cooling off” periods in which former public officials cannot be hired or cannot work in a particular industry. Even employment candidates who are not public officials themselves should be required to disclose any close relationships (e.g., parent, spouse, domestic partner, child, sibling, in-laws) with public officials, to minimize the risk of conflicts of interest.

Decision-making.

Hiring decisions should be made at an appropriately high level within the company. Depending on the position under recruitment, it may be necessary for the general manager or board of directors to be personally involved, especially for senior management candidates. The CCO generally should be involved in any decision to hire a candidate who is suspected of misconduct or who otherwise may pose integrity risks. Legal counsel and human resource professionals should be involved as appropriate.

Sample Due Diligence Methods Regarding Employment Candidates (as allowed under applicable law)

- *Hiring questionnaires.*
- *Interviews.*
- *Verification of information on curriculum vitae/resume.*
- *Reference checks.*
- *Background checks.*
- *Internet searches (e.g., social media accounts, adverse media).*
- *Searches of available government and international organization databases (e.g., administrative actions, criminal convictions, sanctions).*
- *Use of due diligence subscription services/screening tools.*
- *Use of third-party service providers to conduct due diligence.*

Employment Contracts and Integrity Certifications

Companies should obtain integrity commitments from employees in their employment contracts and through written certifications that employees sign upon joining the company and periodically thereafter. To the extent permissible under applicable law, employment contracts should contain detailed integrity clauses, including:

- an attestation that the employee has reviewed and understands the obligations set out in the ICP,
- an obligation to comply with the ICP,
- an obligation to comply with applicable laws and regulations,
- a commitment not to engage in misconduct,
- a duty to disclose potential conflicts of interest,
- a duty to report suspected misconduct or ICP violations to designated company personnel,
- a requirement to cooperate in investigations and audits, and
- reference to the remedies available to the company in case of any misconduct or violation, including termination of employment and lesser penalties, such as reprimands, as appropriate.

In jurisdictions where such clauses may not be readily included in employment contracts (and in companies that do not use employment contracts), other strategies may be adopted to bind employees to integrity rules, such as through discussions with works councils.

In addition, to the extent legally permissible, employees should be required to submit written certifications upon joining the company and on a regular basis thereafter to attest that they:

- have reviewed and understand their obligations under the ICP,
- commit to comply with the ICP and applicable laws and regulations,
- have complied with the ICP and applicable laws and regulations in the past (as part of recertification),
- will report, and have reported (as part of recertification), any known or suspected misconduct as required under the ICP,
- will cooperate, and have cooperated (as part of recertification), in any investigations or audits, and

- understand that they may be subject to discipline for any misconduct, including termination of employment as permitted under applicable law.

In most cases, such certifications should be completed at least annually (e.g., upon completion of yearly integrity training). More detailed certifications may be required for managers or employees in critical positions.

Companies often collect certifications following annual integrity trainings or at staff meetings where the ICP is discussed. Periodic certifications not only serve as reminders about the ICP, but also provide the company with documentary evidence that each employee has committed to comply with the ICP and has confirmed their compliance to date. In some jurisdictions, signed certifications may provide a basis for disciplinary action in the event of misconduct. Contracts and certifications should be stored in an auditable fashion.

Sample Employment Contract Integrity Clause Text

By signing this contract, I confirm that I:

- *have read and understand the obligations set out in [company's] integrity compliance program (ICP),*
- *will comply with the ICP,*
- *will comply with applicable laws and regulations,*
- *will not engage in misconduct,*
- *will disclose any potential conflicts of interest,*
- *will report any suspected misconduct or ICP violations as required under the ICP,*
- *will cooperate in any investigations or audits, and*
- *understand that any misconduct or violation of the ICP by me may result in disciplinary action, including termination of employment [to the extent permissible under applicable law].*

Sample Employee Recertification Text

By signing this certification, I confirm that I:

- have read and understand the obligations set out in [company's] integrity compliance program (ICP),*
- have complied and will continue to comply with the ICP,*
- have complied and will continue to comply with applicable laws and regulations,*
- have not and will not engage in misconduct,*
- have disclosed and will disclose any potential conflicts of interest,*
- have reported and will report any suspected misconduct or ICP violations as required under the ICP,*
- have cooperated and will cooperate in any investigations or audits, and*
- understand that any misconduct or violation of the ICP by me may result in disciplinary action, including termination of employment [to the extent permissible under applicable law].*

Conflicts of Interest

Companies should establish written protocols to effectively identify and manage conflicts of interest. Special attention should be paid to conflicts that may create incentives or opportunities for misconduct. This includes situations in which conflicts actually exist, and situations in which conflicts may simply be perceived or likely to arise. Companies should examine potential conflicts of interest involving individuals, such as when an employee's interests diverge from the company's, as well as potential conflicts of interest affecting the whole organization, such as when a company's participation in certain activities may prevent it from being impartial in a related transaction. SMEs may face particular conflict of interest-related risks, especially if they have informal ownership structures, close ties to local communities or political leaders, or operations in small locales where "everybody knows everybody."

Conflicts of interest should be avoided whenever possible. Otherwise, conflicts of interest should be managed appropriately to minimize the risk of misconduct. While conflicts of interest can arise in a variety of situations, the following areas merit special attention under an ICP:

Employees with outside interests or internal conflicts.

All employees should be required to disclose, up-front and ahead of time, any interests that they or their friends or relatives have in transactions affecting the company. For example, if an employee's spouse works for a regulatory agency with authority over the company, this relationship should be disclosed and analyzed by the CCO. When outside interests may affect an employee's judgment, the employee should be excluded from related information to the extent possible, or even removed from the affected transaction. If the individual cannot be removed entirely from the transaction, then appropriate restrictions should be imposed on the individual's discretion and authority, and the individual's work should be closely monitored by the integrity function. Additionally, as noted in the Integrity Function section of this Guide, employees can face conflicts between their roles within a company, such as when they work part-time in the integrity function.

Business partners.

Contractual terms with business partners should require timely disclosure of any interests that they or their friends or relatives have in transactions affecting the company. Companies should avoid business relationships with conflicted entities whenever possible. Otherwise, appropriate firewalls and monitoring arrangements should be implemented to minimize the risk of misconduct.

Public officials—hiring and other interactions.

As noted in the Employee Due Diligence section of this Guide, hiring public officials or their friends or relatives can lead to conflicts of interest. Conflict of interest concerns may be especially acute if a company engages in employment discussions with current or recent public officials. Care should be taken to ensure that all applicable laws are followed, including any restrictions on hiring processes or on the type of work that the official can perform once hired. In general, former public officials should not engage in business activities related to their former governmental roles, at least for an adequate period of time. Companies should also establish clear protocols to ensure that former public officials do not exert undue influence or create an appearance of impropriety, even if they only work part-time or in unpaid positions.

Other types of interactions with public officials can create conflicts as well. For example, a public official may request that the company comment on tender specifications related to a business opportunity that the company is pursuing. Special care should be taken to ensure that all interactions with public officials, and with persons who have close relationships with such officials, are fully transparent and in compliance with applicable laws and regulations.

Sample Disclosure Questions (as allowed under applicable law)

- *Have you served as a public official (e.g., local, regional, or national government or political party, or international organization)?*
- *Do you have any close relatives (e.g., parent, spouse, domestic partner, child, sibling, in-laws who have served or are serving as public officials)?*
- *Have you or a close relative ever been a candidate for public office?*
- *If the answer to any of the above questions is yes, please provide details as to such activities (e.g., role, entity, nature of service, dates, current status) and your relationship with the public official or organization, as relevant.*
- *Do you or any close relatives have any other business or relationships that may present a conflict of interest with respect to company business? If so, please provide details.*

Business Partnerships and Combinations

Engagements with external business partners are among the most common sources of misconduct.

What is a “business partner”? Business partners often include, for example:

- *Agents.*
- *Representatives.*
- *Consultants.*
- *Financiers and bankers.*
- *Investors.*
- *Brokers.*
- *Intermediaries.*
- *Distributors.*
- *Suppliers.*
- *Vendors.*
- *Subcontractors.*
- *Subconsultants.*
- *Consortium partners.*
- *Joint venture partners.*
- *Acquisition targets*

Written ICP protocols should incorporate the following principles, to the extent appropriate for each company, to mitigate integrity risks related to business partners:

Due diligence.

Companies should conduct an appropriate level of due diligence on prospective business partners, in consideration of factors such as the size of the transaction and the degree of integrity risk involved. Such risk-based due diligence should be conducted prior to engagement and should be repeated periodically thereafter in longer-term engagements (e.g., at least annually for business partner engagements that pose greater integrity risks, or every two years for others). Due diligence protocols should be designed to assess whether the partner has participated or may participate in misconduct, and also to gather information about the entity such as relevant experience, beneficial ownership, governmental connections, any ICP documents, and whether a conflict of interest may arise.

Written due diligence procedures should be tailored to each company’s unique circumstances and risk profile. Such procedures generally should include:

- completion of specified steps in the due diligence process (e.g., filling out standard questionnaires, completing reference checks using public sources available on the internet or third-party screening tools),
- deeper reviews for certain types of business partners such as agents or representatives,

- which typically pose greater risks than vendors or suppliers,
- consideration of specified criteria and “red flags” before a business partner is engaged,
- approval processes commensurate with the risk of each engagement, including mandatory CCO or integrity function approval for higher-risk transactions,
- protocols for informing business partners about the company’s ICP and expectations for ethical conduct and business integrity, and
- complete and appropriate recordkeeping, maintained in an auditable format.

In addition, at least for certain transactions, integrity function personnel should review the ICP of the prospective business partner to assess whether the partner’s program aligns with the company’s own ICP principles. Such reviews may be accomplished, for example, by examining the potential partner’s ICP documents, requesting copies of any third-party analyses of the ICP that the potential partner may be willing to share, and conducting interviews with relevant personnel of the potential partner as needed. This type of review is particularly important for SMEs that may be unable to impose integrity-related contractual terms on a larger partner or are required to abide by the partner’s ICP. If the company finds itself subject to the ICP of a business partner, it should clearly document that requirement in the appropriate contract files and should ensure that relevant company personnel are fully aware of the related obligations.

SMEs may take advantage of the numerous due diligence tools and resources that are provided online at little or no cost by various anti-corruption organizations. SMEs also may consider seeking guidance from other companies or industry groups regarding their due diligence protocols or screening tools.

***Sample Due Diligence Methods Regarding Prospective Business Partners
(as allowed under applicable law)***

- *Verification of questionnaire responses.*
- *Reference checks.*
- *Interviews and site visits.*
- *Internet searches regarding the prospective business partner (e.g., social media accounts, adverse media).*
- *Search of available government and international organization databases (e.g., administrative actions, criminal convictions, sanctions).*

- *Use of due diligence subscription services/screening tools.*
- *Use of third-party service providers to conduct due diligence.*

Similar checks should be conducted for beneficial owners and key personnel as needed.

Note

When assessing the level of integrity risk posed by each business partner, companies should consider not only the monetary value of the proposed transaction but also the nature of the proposed relationship and partner. For example, a low-value engagement with an agent may pose more risk than a higher-value purchase of office supplies.

Examples of Circumstances that May Indicate a “Red Flag” Regarding a Prospective Business Partner or its Owners or Key Personnel

- *Is located in a country or region that is generally known for widespread corruption.*
- *Has a history of known or suspected misconduct.*
- *Has been sanctioned by a national authority or international organization, or is known to be associated with sanctioned entities or individuals.*
- *Has a poor business reputation.*
- *Lacks an adequate ICP under the circumstances.*
- *Has one or more undisclosed beneficial owners.*
- *Has a complicated or opaque ownership structure.*
- *Is a shell company incorporated in an offshore jurisdiction.*
- *Has previous experience working as a public official.*
- *Has a senior official, member of the board of directors, or major shareholder that is also a government official.*
- *Has a family or business relationship with a public official or government agency related to the transaction.*
- *Makes frequent or large political contributions.*
- *Is in a different line of business than that for which it is to be engaged.*
- *Proposes vaguely described services to be provided.*

- *Has poor credit history.*
- *Requests suspicious payment arrangements (e.g., payments in a third country, to an individual or third party not linked to the project, through an intermediary, to an offshore account, in cash or cash equivalents, in cryptocurrency, using multiple bank accounts).*
- *Uses tax havens.*
- *Proposes financial arrangements (e.g., fees, rates, advance payments, percentage-based commissions, profit sharing) that seem disproportionate, excessive, or unusual under the circumstances.*

Contractual obligations.

Integrity-focused contractual terms should be in place for business partner engagements. Where possible, companies should use standard contract templates that incorporate the following terms, as appropriate for each transaction:

- obligate the business partner to comply with applicable laws and regulations and avoid misconduct,
- mandate, in appropriate cases, that the partner comply with the company's ICP, such as in engagements with sales agents who make deals on the company's behalf,
- set out remedies for any misconduct or other breaches by the partner, including the possibility of contract termination,
- require the partner to cooperate with any investigations or audits related to the business relationship, as directed by the company,
- require the partner to report promptly (i.e., ahead of time or as soon as identified) any potential conflict of interest to designated company personnel,
- require the partner to report promptly (i.e., immediately upon discovery) any known or suspected misconduct related to the engagement to designated company personnel, as appropriate, and
- require the partner to disclose any change in corporate structure and related matters (e.g., ownership, beneficial ownership).

As noted above, in some cases, SMEs may be unable to impose such contractual terms on their larger partners. In those situations, the CCO or integrity function should review the contract to ensure that it does not expose the company to undue risk. SMEs also may seek to obtain written integrity certifications from such partners, similar to the certifications described in the Employment

Contracts and Integrity Certifications section of this Guide. Where appropriate, such certifications should be obtained prior to engagement and also periodically during the engagement.

Sample Business Partner Contract and Certification Text

By signing this contract, [business partner], in connection with this contract, commits to:

- comply with applicable laws and regulations,*
- comply with [company's] integrity compliance program,*
- not engage in misconduct,*
- cooperate in any investigations or audits related to the business relationship, as directed by [company],*
- report promptly (i.e., ahead of time or as soon as identified) any potential conflict of interest to designated [company] personnel, and*
- report promptly (i.e., immediately upon discovery) any known or suspected misconduct or ICP violations to designated [company] personnel.*

[Business partner] acknowledges and understands that any misconduct or violation of the ICP by [business partner] or any of its personnel may result in [company] seeking remedies against [business partner], including contract termination.

Remuneration.

Companies should ensure that all payments to business partners are appropriate, justifiable, and based on actual and documented work performed. Market analysis may be warranted in some cases to ensure that a partner's fees or costs are reasonable. In addition, certain types of remuneration arrangements pose greater risks and may require additional due diligence or prior approval from the CCO. In all cases, payments should appropriately reflect the work being done and be justified as memorialized in company records. Remuneration arrangements should be detailed in the business partner contract.

Sample Remuneration Schemes that May Pose Greater Risks

- *Use of cash or cash equivalents.*
- *Use of cryptocurrency.*
- *Use of percentage-based commission fees.*
- *Financial arrangements (e.g., fees, rates, profit sharing) that seem disproportionate, excessive, or unusual under the circumstances.*
- *Requests for large advance payments.*
- *Use of intermediaries.*
- *Requests for payments to individuals.*
- *Requests for payments to third parties not linked to the project.*
- *Designation of multiple bank accounts.*
- *Payments outside the business partner's home country.*
- *Use of offshore accounts.*
- *Use of tax havens.*

Payments.

Like remuneration arrangements, payment terms and related documentation requirements should be specified in the business partner contract. Before payments are released, supporting materials such as invoices should be required, and appropriate company personnel should confirm satisfactory receipt of the goods or services. Dual reviews of relevant materials (e.g., the “four-eyes” principle requiring that two persons approve some action before it can be taken) should also be mandated where needed. Finally, approvals at appropriate levels should be required before payments are made, with higher-level approvals being required depending on factors such as transaction value and risk level. All payments should be made through bona fide channels, and payment records should be maintained in an appropriate fashion.

Monitoring.

During the course of the engagement, designated company personnel should regularly monitor business partners for signs of misconduct. Greater attention should be paid to riskier engagements such as agent and joint venture arrangements. For example, engagements with agents and consultants should be closely monitored to ensure that the services are not fictitious or lacking in substance and are not being used as a possible cover for illicit activity.

Reviews also should check for accurate and complete recordkeeping in areas such as due

diligence, contracts, integrity certifications, invoices, and payments. To the extent possible, contractual audit rights should be used where appropriate, especially in high-risk situations or if an integrity concern arises. Integrity function personnel should oversee the monitoring process and take action where necessary. The results of monitoring activities should be fully recorded as well.

SMEs may face more hurdles than larger companies in effectively auditing or terminating business partner contracts for suspected misconduct, especially when a replacement may be difficult to find, or when a larger partner imposed its contractual terms on the engagement. In all cases, SMEs should give proper weight to the risks posed by not exiting or curtailing the relationship, such as potential legal, commercial, and reputational risks. Where actions short of contract termination may be appropriate, protocols may be developed to possibly provide integrity training to the affected business partner, more closely monitor the affected engagement, and create records to protect the company.

Special considerations for joint ventures.

While appropriate levels of due diligence and monitoring should be carried out for all business partner engagements, special mention is warranted for joint ventures. Due diligence often needs to be more intensive for such transactions, and the types of monitoring needed can vary. Contractual integrity terms also may be different. Joint ventures that will be controlled by the company typically should adopt the company's ICP as a whole. Even if the company does not control the joint venture, it should seek to ensure that the joint venture adopts and implements policies and procedures that are aligned with the ICP. At a minimum, the company should be comfortable with the integrity compliance framework in place at the joint venture before agreeing to participate.

Information uncovered during due diligence should guide the process of integrating the joint venture into the company's ICP, including with respect to:

- rolling out trainings and communications to the employees of the joint venture,
- conducting due diligence on the key employees and business partners that will be working with the joint venture, and
- assigning or adding personnel to the integrity function as needed.

In the event that due diligence reveals any past or ongoing misconduct on the part of a prospective joint venture partner, the company should ensure that such issues are cured, or at least that there is an action plan with clear timing and milestones to address such issues, prior to any joint venture agreement being signed. Company leadership, including the CCO, should also assess the possible

liabilities the company may face as a result of such misconduct.

Special considerations for mergers and acquisitions.

Similarly, mergers and acquisitions pose unique integrity risks and therefore merit special consideration under an ICP. Careful due diligence should be undertaken to ensure that the integrity values of potential merger and acquisition targets align with those of the company and to identify any potential risk areas that may require mitigation if the transaction proceeds. The target company's ICP also should be scrutinized in comparison with the company's ICP to determine which elements of each program should be carried forward in the ICP of the newly combined entity. Accordingly, due diligence of the target company should be designed to provide a fuller picture of its business operations, integrity risk profile, and integrity compliance posture, to prepare for ICP integration. Appropriate monitoring also is needed during the acquisition and integration process. As with joint ventures, information uncovered during due diligence should guide the integration process, including with respect to:

- adding personnel to the integrity function as needed,
- rolling out trainings and communications to employees,
- conducting due diligence on key employees and business partners as necessary, and
- amending contracts if needed.

Likewise, in the event that due diligence reveals any past or ongoing misconduct on the part of a merger or acquisition target, the company should ensure that such issues are cured, or at least that there is an action plan with clear timing and milestones to address such issues, prior to any merger or acquisition being completed. Company leadership, including the CCO, should also assess the possible liabilities the company may be taking on under the transaction.

The CCO and other company leaders should guide these processes, and appropriate records should be kept. Companies sometimes only gain full access to an acquired entity's books and records after the acquisition is complete, in which case follow-up due diligence may be necessary.

Note

It is often useful to look for similarities in the parties' ICPs and consider adopting the strongest provisions from each for a joint venture or for the company as a whole where appropriate.

Financial Controls

Companies should implement appropriate internal controls over their accounting and financial practices. Controls should be designed and maintained in such a manner as to provide reasonable assurances that:

- financial transactions are properly identified,
- financial transactions are appropriately approved by senior management, with clear limits of authority set out at appropriate levels of management,
- all transactions are accurately and fairly recorded in the company's official books and records, with appropriate supporting documentation and in a manner that facilitates the effective classification of transactions, such as by project or business unit (i.e., cost-accounting),
- no "off the books" accounts are used,
- there is no recording of expenditures that do not exist, or of liabilities that are not correctly or adequately identified,
- regular internal and external audits are conducted, and
- there are clear consequences for improper activities.

Weak financial controls can increase a company's vulnerability to misconduct. For example, inadequate cash management and poor payment processes have led to misconduct that was sanctioned by multilateral development institutions in certain cases. Conversely, strong financial controls can help to prevent misconduct by identifying suspicious transactions and potential improper dealings. As discussed in the next section, internal and external financial audits should be conducted on a regular basis, as appropriate, to assess the effectiveness of financial controls.

Sample Financial Controls Regarding Cash Usage

The use of cash should be minimized to the extent possible, with some exceptions (e.g., appropriate types of consumer transactions). Moreover, clear controls should be established whenever cash is used. For example, companies may:

- *limit occasions where cash may be used,*
- *require written justification for cash usage,*
- *limit the amount of petty cash available,*
- *limit who has access to cash,*
- *require verification as to receipt of goods or services,*
- *require supporting documents (e.g., invoices),*
- *require dual approval for payments,*
- *require signed confirmation of receipt of cash payments, and*
- *include an examination of cash usage in periodic internal and external audits.*

Audits

The ICP's effectiveness should be regularly assessed via independent and objective audits. ICP documents should set out audit protocols that are appropriate for each company's operations and risk profile, such as:

- auditing at regular intervals by internal or external auditors,
- examination of the effectiveness of not only financial and accounting controls, but also other policies and procedures comprising the ICP,
- review of audit results and recommendations by senior managers, to develop plans for remediation,
- assignment of remedial action plans to personnel with adequate expertise and seniority, with the CCO or integrity function being involved as necessary, and
- the tracking of remedial actions to completion.

Gaps identified in audits should be seen as an opportunity to strengthen the ICP. Adequate records should be kept throughout the auditing and remediation process.

SMEs that do not have the resources for a standalone internal audit function may choose to engage part-time external professionals for this purpose. For example, internal audits can be outsourced to an external auditor who is separate from any auditor the company may already use. Such professionals typically should be engaged on behalf of management and any board of directors or other governing body. Local laws may require certain audits as well.

Case Study

Following a period of rapid growth, an organization hired its first Chief Financial Officer. The new Chief Financial Officer wanted to understand the state of the organization's financial processes and immediately initiated an internal audit.

The internal audit identified nearly 200 checks that were missing from the accounting records. These checks related to bank accounts that were in the care of the long-time personal assistant to the organization's general manager.

The general manager travelled frequently and so would sign blank checks for the personal assistant to use for the organization's expenses.

The personal assistant admitted to paying these checks into accounts that the personal assistant controlled. The internal audit also found that these outflows were offset by not recording a large royalty income deposit in the accounting records and deleting the opening bank balance in the accounting records.

Gifts, Entertainment, Travel, and Hospitality

Gifts, entertainment, travel expenses, and other hospitality (e.g., meals, hotel stays)—collectively called “G&E”—are sometimes used by unethical individuals to conceal bribery or other misconduct. Companies should establish written protocols to ensure that any G&E that is offered, given, or received:

- complies with applicable laws and regulations,
- is limited in nature and amount, as appropriate,
- is not used for improper purposes, such as bribery or funneling money to particular individuals,
- is not used to influence decision-making processes,
- does not provide an improper advantage or create an appearance of impropriety,
- is not otherwise inappropriate,
- is reviewed and approved at an appropriate level before being offered, made, or accepted,
- complies with any rules that may be mandated by clients or business partners, including restrictions that large companies sometimes impose on their supply chain partners, and
- is properly documented in the company’s books and records.

In many countries and industries, G&E is an ordinary part of business and local custom (e.g., new year acknowledgements). Appropriate G&E expenses can vary significantly, from company-branded gifts of negligible monetary value to the funding of overseas trips for public officials to supervise contract implementation (which should be expressly set out in the underlying contracts if planned). In all cases, whether G&E is appropriate depends on the situation, including the laws and standard business practices of the locale. Accordingly, companies’ overall risk assessments should include an analysis of any G&E practices and whether they are suitable under the circumstances. G&E policies may even be adapted within a company to account for local considerations (e.g., different value limits by country), subject to a central umbrella policy.

ICP documents should explain the ways in which G&E can create misconduct risks. Written pre-approval from the CCO or other high-ranking personnel should be required for G&E-related activities in specified situations (e.g., high-risk situations), and some types of G&E should be prohibited altogether. Regardless of a company’s particular situation, G&E should be reasonable, properly approved, and fully documented. Written protocols should clearly inform employees and business partners about what is acceptable and what rules must be followed, including:

- limits on the value and frequency of G&E, both per-transaction and cumulatively (e.g., annual or quarterly limits),
- types of G&E that should be avoided, such as cash gifts and pleasure trips,
- situations in which all G&E is forbidden, such as during contract negotiations or tender processes,
- mandatory approval procedures, and
- recordkeeping requirements, including required supporting documentation.

G&E records should include information such as a description of the transaction, details about all of the individuals involved, total and per-person costs, location details, justification as to why the G&E is necessary and appropriate, and copies of receipts and approvals. G&E-related expense records should be periodically audited as well.

Due to inherent risks, G&E relating to public officials requires greater scrutiny, whether done directly or indirectly (e.g., involving relatives). G&E relating to public officials also is often governed by local or national laws and regulations. Companies need to understand all applicable laws and rules whenever they may provide G&E to public officials. For example, in some countries, public officials cannot receive anything of value in connection with their work, regardless of whether it may influence the outcome of a transaction. Moreover, each governmental entity may have its own restrictions and protocols, which should be considered as well. Such matters should be examined before any G&E is exchanged.

Sample Restrictions under National Law

Pursuant to the Republic of Korea's Improper Solicitation and Graft Act, public officials in the Republic of Korea generally may not receive G&E, in any amount, in relation to their duties. However, there are some exceptions in Article 8 (3) for social relationships or rituals, including food and drink under KRW 30K, condolence money under KRW 50K, and gifts under KRW 150K (roughly USD 25, 40, and 120, respectively). Further, public officials in the Republic of Korea may not receive G&E in excess of KRW 1M (roughly USD 750) at one time and KRW 3M (roughly USD 2,300) per fiscal year from the same entity, regardless of the relationship between such G&E and their duties.

Political and Charitable Donations, and Sponsorships

Like G&E, donations and sponsorships may be used by unethical individuals to conceal bribery or other misconduct. SMEs may be exposed to greater risks in this area if they are closely tied to public officials or political organizations. Companies should establish written ICP protocols to ensure that all donations and sponsorships:

- comply with applicable laws and regulations,
- are limited in nature and amount, as appropriate,
- are not used for improper purposes, such as bribery or funneling money to particular individuals,
- are not used to influence decision-making processes,
- do not provide an improper advantage or create an appearance of impropriety,
- are not otherwise inappropriate,
- are reviewed and approved at an appropriate level before being offered or made,
- are properly recorded in the company's books and records, with detailed information and documentation along the lines of what is required in the G&E context,
- comply with any rules that may be mandated by clients or business partners, including restrictions that large companies sometimes impose on their supply chain partners, and
- are openly reported in a transparent manner (e.g., on the company's website or in its annual reports).

Companies should conduct due diligence on the proposed recipients of donations and sponsorships to ensure that they are reputable organizations and that no improper purpose is intended. The depth of due diligence should be based on the risks of each transaction. In addition, to the extent possible, donations and sponsorships should be subject to written contracts establishing the company's integrity-related expectations and rights. Many jurisdictions also require certain contributions to be publicly disclosed. Companies often disclose details about all of their donations and sponsorships to increase transparency and publicize their commitment to ethics, business integrity, and corporate social responsibility.

Examples of Situations that may Indicate a “Red Flag” Relevant to Donations and Sponsorships

- *The potential recipient is affiliated with government officials or existing or potential customers.*
- *The donation/sponsorship was made at the request of a government official or existing or potential customer.*
- *The donation/sponsorship was requested or hinted at during business discussions.*
- *There are conditions or expectations attached to the donation/sponsorship.*
- *A request was made that the funds be deposited into an unauthorized account or handled through a third-party intermediary.*
- *A request was made that the contribution be kept secret.*
- *The recipient seems reluctant to enter into a contract or to confirm compliance with integrity-related expectations.*
- *The donation/sponsorship exceeds limitations under local law or seems excessive under the circumstances.*

Facilitation Payments

Facilitation payments are a type of bribery in which an individual makes a small unlawful payment to a public official to obtain or speed up the performance of certain duties to which the individual is otherwise entitled. For example, a small unlawful cash payment “under the table” to a customs official to speed up the processing of a legitimate customs clearance would be considered a facilitation payment. While facilitation payments may be considered common in certain areas, they are still a form of bribery that reflects poorly on the integrity of all parties involved. ICP policies therefore should prohibit facilitation payments.

Facilitation payments can pose particular challenges for SMEs. This is especially true in transactions where such payments are often demanded, such as interactions with low-level permitting authorities or corrupt safety officials. Avoiding cash transactions and using pre-paid or electronic payment approval systems, which leave an audit trail, can help to stave off improper requests or at least more readily identify them if they have occurred.

In any case, SMEs should establish clear protocols for responding to any such requests. Well-trained employees may be able to rebuff an improper request by referring to applicable laws, the company's publicly available code of conduct, or the integrity rules imposed by the company's clients or business partners. Some companies even publish a prohibition of facilitation payments on employee business cards to make it clear to others that such payments will not be tolerated by the company. Employees should be required to promptly report any improper requests to the integrity function. Company leaders should also consider onward reporting to relevant authorities, which may be required in some jurisdictions.

Exceptions in Exigent Circumstances

ICP protocols should provide for exceptions if individuals are in danger—for example, if a corrupt government worker threatens to harm an individual unless an unlawful payment is made. Any payments made in such circumstances should be reported immediately to the CCO and fully documented, including as a designated line item in the company's books and records. Company leaders should consider whether to take remedial action, or to report the matter to relevant authorities, which might be required in some jurisdictions. Companies should plan their travel and business activities to avoid such circumstances to the greatest extent possible.

Incentives

Companies should incentivize all employees to support and comply with the ICP. In addition to clarifying that violations will lead to disciplinary actions, companies also should:

Emphasize the business case for compliance.

Employee communications should underscore the links between ethical behavior, business integrity, and the company's overall success. Experience indicates that ethical companies are often more attractive to investors, business partners, and employment candidates, and may be better able to maintain long-term partnerships or obtain higher valuations. A reputation for business integrity can be especially helpful for SMEs in high-risk jurisdictions where large companies often seek trustworthy partners for their supply chains.

Recognize outstanding contributions.

Where appropriate, employees should be recognized when they make exceptional contributions to the ICP. For example, companies might recognize an employee who insisted on following due diligence procedures in the face of pressure to bend the rules, or who developed an exemplary ICP training initiative. SMEs often can take advantage of smaller headcounts, flatter organizational structures, and greater familiarity between employees and managers, to impactfully communicate such "success stories" to the entire organization.

Consider incorporating integrity-related factors in performance reviews.

Ethical behavior and business integrity, including commitment to the ICP, may be included as factors in employee evaluations or promotions as appropriate. Managers or integrity function personnel, in particular, may be assessed on integrity-related performance indicators.

Look for other creative incentives.

Companies of all sizes are increasingly finding creative ways to incentivize integrity compliance. For example, many companies host "Integrity Days" or "Integrity Weeks" to keep the ICP front of mind. In addition to trainings and discussions, such events may feature games or contests designed to make learning about the ICP fun. Such activities often cost very little and can greatly motivate employees to participate.

Examples of “Integrity Week” Activities

- *Asking employees to answer daily compliance questions that pop-up when they log on to their computers during Integrity Week, with small prizes awarded at the end of the week.*
- *Playing integrity-themed games at team meetings, including at the management level, with small prizes being awarded. For example, some companies have developed their own integrity compliance board games.*
- *Asking employees to submit ideas for posters or other communication tools to promote the ICP, with the winning submissions being rolled out across the company during Integrity Week. Employees are often eager to showcase their artistic talents.*
- *Holding internal events (e.g., so-called brown-bag lunches) to bring in external parties, such as integrity compliance experts, CCOs from other companies, regulators, law enforcement personnel, or investigative journalists, to share experiences, cases studies, new developments, etc.*

Disciplinary Mechanisms

Companies should establish appropriate disciplinary mechanisms for employee misconduct. If an investigation substantiates that misconduct occurred, then the company should promptly take appropriate steps to respond. Designated individuals should decide on the disciplinary action or other corrective measures to be imposed, in consultation with the CCO, company leaders, and outside counsel if necessary. Discipline should be proportionate to the severity of the misconduct and may include actions such as warnings, reassignments, demotions, and termination of employment, in accordance with applicable law.

While it may be unnecessary for some smaller companies to adopt lengthy disciplinary policies, it is important to have a suitable written protocol prescribing how disciplinary actions are carried out and what the available remedies are. Proper written protocols help to:

- provide transparency and due process,
- ensure objectivity and consistency, and
- signal to all employees that the company is committed to enforcing applicable rules.

In some situations, it may be difficult to dismiss an employee for misconduct, especially in very small businesses where a replacement may be difficult to find. Nevertheless, companies should consider the risks posed by not taking appropriate disciplinary action, including potential legal, commercial, and reputational risks. Where disciplinary action short of termination may be appropriate, or mandated under applicable law, companies should establish protocols to closely monitor and seek to rehabilitate the affected employee. For example, a company might require the employee to complete special integrity training and might establish processes to carefully oversee the employee's work under the guidance of the CCO. In all cases, companies should keep adequate records concerning disciplinary decisions and remedial measures.

***Sample Scenario of a Difficult Disciplinary Decision that Ultimately
may Benefit the Company***

In one case, the company terminated the employment of a senior manager who had encouraged employees to “do whatever it takes” to get business, which had led the manager’s team members to engage in unfettered misconduct. The termination of the manager and related disciplinary action against other culpable team members sent a strong message to the company’s employees that “getting business at any cost” would not be tolerated and that they should resist and report any pressure to engage in misconduct.

Recordkeeping

Companies should maintain accurate and complete records on all aspects of their ICPs. Records should be held:

- in accordance with written retention rules for documents and records,
- in an organized and auditable fashion,
- in compliance with applicable laws and regulations (e.g., regulations governing the types of documents that must be retained and the time period of retention),
- in accordance with appropriate rules regarding access and security, and
- in sufficient detail to show that ICP protocols are being followed, and to evaluate whether updates to such protocols may be needed.

ICP policies should specify how different types of records are created and maintained, and who is responsible for them. The ICP should also require that records be made available to auditors, investigators, and others with a legal right to access them. It is generally a best practice to use electronic recordkeeping systems that are appropriate for each type of transaction. Where necessary, SMEs may be able to use paper systems effectively as well.

Examples of Recordkeeping Systems and Records to be Maintained

Records may be kept in various ways, such as:

- *hard copy files (e.g., well-organized and clearly labelled binders on specific topics),*
- *electronic folders organized by specific topics and with clearly labelled subfolders, and*
- *sophisticated databases that allow for advanced data tracking and reporting.*

Records should include, at a minimum and as relevant, materials such as:

- *risk analysis documents,*
- *due diligence review documents,*
- *contract materials (e.g., agreements, amendments, progress reports, performance reviews),*
- *bid files (e.g., approvals, verifications, supporting documents),*

- *financial documents (e.g., budgets and plans, invoices and related supporting documents, evidence of goods delivery or services provided, evidence of payment, audit materials, G&E logs), and*
- *other evidence of ICP implementation, including whistleblowing report logs, investigation reports, documentation of remedial measures, logs of requests for advice, training records, training and communication plans, and related documentation of other verifications, reviews, concurrences, approvals, and notices under the ICP.*

Conclusion

This Guide is intended to explain fundamental integrity compliance principles in terms that are useful and practical for companies of all sizes. While many publications offer guidance on sophisticated compliance methodologies for multinational corporations, less has been written about how SMEs—and particularly microenterprises—can design and implement ICPs that are effective for their operations and risk profiles. A properly scoped ICP should be seen as a competitive advantage, regardless of a company's size, in terms of protecting against misconduct risks, improving operations, and enhancing the company's attractiveness to investors and business partners. This is especially true for SMEs.

It is clear that SMEs are not only drivers of economic growth, but also can serve as drivers of integrity compliance on a global scale. Indeed, through the ICO mentorship program discussed in this Guide, some SMEs that were previously sanctioned for misconduct are now assisting other companies in their efforts to implement integrity compliance reforms. It is hoped that, as more companies work together, integrity compliance will become stronger and more widespread in the global marketplace, and tolerance for misconduct and unethical behavior will continually diminish. SMEs have a keen role to play in the collective effort to build a clean business environment across the globe.



THE WORLD BANK
IBRD • IDA



Ministry of Justice

Integrity Compliance Programs for SMEs
Practical Guidance and Resources

Integrity Compliance Programs for SMEs

Practical Guidance and Resources

