

Anti-bribery and corruption compliance

Building an effective
program that addresses
recent global trends

BRIBERY AND CORRUPTION remain a significant risk for organisations across the world. Many fraud schemes tend to have a corruption angle to them. Regulators across the world are continuing to increase their enforcement efforts and simultaneously setting to set comprehensive standards backed reduce instances of bribery and corruption. Organisations, now more than ever need to increase their efforts to address the risk of bribery and corruption.

Recent developments in the anti-bribery and corruption regulatory space include the following:

- In 2024, organisations worldwide paid, or agreed to pay, settlements collectively amounting to more than USD 920 million to the Securities and Exchange Commission (SEC) and the United States Department of Justice (US DOJ) for the US Foreign Corrupt Practices Act (FCPA) violations. This included involvement in corruption cases and books and records misconduct around the globe, including Angola, Brazil, Indonesia, the US, China, Russia, South Africa, India, and United Arab Emirates.
- More enforcement agencies, including Australia, Canada, Colombia, Cyprus, France, India, Netherlands, and the United Kingdom, are cooperating with their counterparts in other jurisdictions to facilitate cross-border anti-bribery and anti-corruption (ABAC) enforcements and using technology to uncover instances of corporate misconduct.
- The SEC aggressively pursued its enforcement agenda in 2023, and that included filing more FCPA

enforcement actions than in 2022. This includes the increased use of the SEC Whistleblower program. The SEC's whistleblower program was established to incentivise whistleblowers to report specific, timely and credible information about possible compliance violations. In May 2023, the SEC announced the "largest-ever award" in the whistleblower program's history, awarding nearly USD 279 million to a whistleblower who led to a successful enforcement of SEC and related actions.

- As part of a new anti-corruption package announced on 3 May 2023, the European Commission has proposed a new directive which would require EU member states to meet common standards in their anti-corruption legislation.
- Beginning January 2025, the EU Corporate Sustainability Reporting Directive (CSRD) mandates that organisations in scope publicly report information on their sustainability impacts, risks, and opportunities, including aspects such as ABAC and political engagement. This reporting must comply with the European Sustainability Reporting Standards (ESRS), detailing how organisations manage bribery and corruption risks.

Guidance on evaluation of corporate compliance programs

Smart leaders create a compliance program that is comprehensive, tailored, and defensible to global regulators. This involves a new way of thinking about ABAC programs—one that includes regularly revisiting the program to assess risk, upgrade technology, and incorporate best practices as they become available.

The US DOJ issued a guidance note to help US prosecutors understand what can be considered an **effective ABAC compliance program**. However, this also provides useful guidance for organisations..

Organisations that can demonstrate the effectiveness of their ABAC compliance programs, may receive lenient treatment from regulators in cases of bribery, corruption or other forms of corporate misconduct. The guidance is intended to be a roadmap for organisations to consider when designing an ABAC compliance program. It relies on three fundamental questions:

1. **Is the corporation's compliance program well designed?**
2. **Is the corporation's compliance program being implemented effectively?**
3. **Does the corporation's compliance program work in practice?**

The US DOJ guidance serves as a reminder that bribery and corruption remain key focal points for regulators. Similar trends are observed in other jurisdictions.

Regulators are enforcing stringent measures against bribery and corruption, recognising their detrimental impact on ethical business conduct, economies, and society as a whole.

Organisations are expected to develop ABAC compliance programs that are effective. **Organisations must align their operations with this guidance, not merely for compliance, but because it is the right thing to do.**



IS THE ORGANISATIONS'S COMPLIANCE program DESIGNED EFFECTIVELY?

Many ABAC compliance programs tend to use 'one size fits all' templates that do not reflect the risks organisations face at the ground level. The good news is that integrity controls can thwart corruption. By applying controls that close systemic weaknesses in roles and processes and neutralise enabling factors for corruption, organisations can protect the integrity and ethical business conduct.

01. RISK ASSESSMENT*

Organisations need to take measures to ascertain if the ABAC program is appropriately designed to detect the types of misconduct that are most likely to occur. A critical aspect of the DOJ guidance is its emphasis on risk-based compliance. Organisations are urged to identify and prioritise risks specific to their industry, operational footprint, and regulatory environment. It should also include an evaluation of the organisation's use of new technologies, including AI, as well as considerations for emerging risks and new technologies. This risk-based approach ensures that compliance resources are allocated efficiently and effectively.

**See next page for an overview of bribery and corruption risk factors and schemes*

02. POLICIES AND PROCEDURES

The mere presence of policies can be inadequate in curbing bribery and corruption. Organisations need to ascertain if the following aspects are included in policies:

- Design inputs from business units;
- comprehensiveness;
- accessibility; and
- responsibility for operational integration.

04. CONFIDENTIAL REPORTING STRUCTURE AND INVESTIGATION PROCESS

Organisations first need to put in place an efficient mechanism where employees can anonymously/confidentially report actual/potential breaches. This includes ascertaining the reporting mechanism's effectiveness, adequately scoping investigations (by professionals), putting in place a process for monitoring investigation outputs, and conducting a periodic analysis of investigation findings to find out compliance weakness. Availability of guidance relating to compliance policies. Additionally, have in place anti-retaliation policies, anti-retaliation training and incentivising reporting.

05. THIRD PARTY MANAGEMENT

Corruption risk posed by third parties remains high. Hence, organisations may need to apply risk-based due diligence to third-party relations that includes the following: Ongoing monitoring; risk-based and integrated processes; appropriate controls; relationship management; maintaining a depository of red flags noted during third party due diligence and how these red flags were resolved, if any of such third parties were on-boarded. Timely review of vendors and use of data analytics for ongoing monitoring

03. TRAINING AND COMMUNICATION

Organisations need to check whether policies and procedures have been integrated through periodic training and certifications. Training and other activities include the following:

- Risk-based training – Tailored for specific risks for different departments in an organization;
- form/content/effectiveness of training;
- regular communication about organisations' position on addressing misconduct; and
- availability of guidance relating to compliance policies.

It should include evaluation of engagement and learning from training sessions, as well as lessons learned from other organisations. Evaluation of metrics for training effectiveness

06. MERGER AND ACQUISITIONS

Many strategic associations have failed because of allegations of bribery and corruption. Therefore, organisations must ensure that their compliance programs include a comprehensive due diligence process for any acquisition target (to identify the target's corrupt practices or misconduct). Carefully integrate critical enterprise systems post-acquisition.

Risk assessment

An organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented.

Commonly encountered bribery and corruption risks can be categorised into five broad groups: geography, sectoral, transaction, business opportunity, and business partnership risks⁽¹⁾.

- **Geography risk:** This arises from perceived high levels of corruption, lack of effectively implemented anti-bribery legislation, and the failure of foreign governments, media, local business communities, and civil society to effectively promote transparent procurement and investment policies.
- **Sectoral risk:** Certain sectors are inherently higher risk than others. These include the extractive industries and large-scale infrastructure sectors.
- **Transaction risk:** Some types of transactions carry higher risks, such as charitable or political contributions, transaction related to licenses and

permits, commissions for agents and intermediaries, cash transactions, facilitation payments, and those related to public procurement and government entities.

- **Business opportunity risk:** These risks may occur in high-value projects, projects involving multiple contractors or intermediaries, or those not conducted at market prices or lacking a clear legitimate objective.
- **Business partnership risk:** Certain relationships pose higher risks, such as using intermediaries in transactions with foreign public officials, consortia or joint venture partners, and relationships with politically exposed persons where the proposed business relationship involves or is linked to a prominent public official.

Understanding how bribes are being paid in practice is one of the best approaches to identifying and assessing risks. Common forms⁽²⁾ are summarised below.

- **Bribery through agents, associates, middlemen:** The use of intermediaries, such as agents or introducers, is common and legitimate in global business for providing local expertise and services. However, intermediaries can also channel bribes through a chain to disguise the connection between the bribe payer and recipient. Professionals like lawyers, accountants, or bankers may be involved to lend an appearance of legitimacy.
- **Bribery through the supply chain, sub-contractors and distributors:** Complex supply chains increase bribery risks. Hiring local sub-contractors with ties to government officials can further obscure bribery under the guise of leveraging local expertise.
- **False or inflated invoicing and product pricing:** Bribes are often hidden within accounting records or through off-balance sheet transactions. Fake or inflated invoices can mask bribery, with additional amounts added to legitimate fees. Entirely fraudulent invoices may also be used, representing no real service.
- **Offshore arrangements and off-balance-sheet payments:** Bribes may pass through multiple bank accounts or front companies located in countries with lax regulations. This distances the bribe from both payer and recipient, concealing identities. Offshore slush funds, set up via fictional invoices, can pay bribes as needed.
- **Joint ventures:** Joint ventures can be structured to facilitate bribery, potentially without all partners' knowledge. In some cases, a joint venture may be created specifically to distance a company from corrupt practices.
- **Training and education:** Customer training may serve as a cover for bribery. Funds allocated for training might be used for lavish hospitality under the guise of training budgets, including per diems, travel or entertainment.
- **Rebates and discounts or kickbacks:** Incentive schemes like rebates and discounts can be diverted as kickbacks to individuals responsible for procurement, essentially serving as bribes to secure contracts.
- **Employment contracts and consulting agreements:** Hiring relatives or associates of clients or officials can become a form of bribery, potentially influencing business decisions. This may include creating 'ghost' employees to extract cash, with fabricated documentation to suggest proper hiring processes.

(1) Source: UK Bribery Act Guidance (<https://assets.publishing.service.gov.uk/media/5d80cfc3ed915d51e9aff85a/bribery-act-2010-guidance.pdf>)

(2) Source: How to bribe: A typology of bribe-paying and how to stop it (https://www.transparency.org.uk/sites/default/files/pdf/publications/How_to_Bribe_-_A_Typology_of_Bribe_Paying_and_How_to_Stop_it_0.pdf)

Testing the effectiveness of the compliance program

An organisation periodically assesses the effectiveness of its ABAC compliance program through dedicated compliance audits and transaction testing.

Managing an ABAC program is a continuous, iterative process that requires thorough scrutiny of its design to ensure it meets the ABAC objectives. Monitoring and testing of the program should encompass all the organisation's activities, including those of controlled entities and intermediaries. This comprehensive approach helps maintain a strong defense against bribery and corruption.

Regular assessments help identify weaknesses and reinforce defenses against potential risks. This process also helps with detecting and preventing corporate misconduct, showing a commitment to ethical business practices. It reassures stakeholders that the organisation is actively protecting itself against fraud, corruption and corporate misconduct, while meeting regulatory requirements.

Periodic testing and review is a key expectation from regulator to establish whether an ABAC program is effective or not. Organisations should test that its systems and controls are operating as intended.

Moreover, **transaction testing** should be performed so that improvement areas are being accurately identified and that red flags, unusual activity and violations of the anti-bribery policy are detected.

Transaction testing should combine advanced technologies like data analytics, AI tools, and machine learning with skilled compliance professional knowledge of bribery and corruption risks.

In addition to regular monitoring, audits, and external evaluations, organisations are recommended to conduct periodic self-assessments or benchmark analyse. This to compare its ABAC program to industry best practices. It allows organisations to evaluate how well their ABAC strategies align with the recommended standards and expectations of regulators.

Approach to testing the effectiveness of and ABAC compliance program



Planning testing

- Define the scope and objectives of the monitoring and testing.
- Develop a plan of approach that outlines necessary resources, timelines, and key areas of focus.



Risk assessment:

- Conduct a risk assessment to identify high-risk areas within the organisation.
- Prepare a detailed test plan to test and monitor the high-risk areas, as well as whether these are sufficiently addressed.



Review of systems and controls:

- Test and evaluate existing systems and controls to ensure they can prevent and detect bribery and corruption effectively.
- Verify that policies and procedures are current and aligned with regulations and best practices.



Data analysis and transaction testing:

- Perform transaction testing to identify anomalies or red flags in financial records.
- Use data analytics to detect unusual patterns or activities that may indicate potential violations.



Reporting and continuous improvement:

- Compile findings into a report, highlighting areas of concern and recommending improvements.
- Present the report to management for review and action.
- Establish a process for continuous monitoring and periodic reassessment.

In particular, organisations should ensure that it monitors vulnerable functions such as⁽³⁾:

- Procurement and contracting
- Sales and marketing, especially to public officials
- Mergers and acquisitions
- Third parties.
- Recruitment and Board appointments
- Public or corporate affairs, especially in relation to political engagement
- Sponsorship management
- Community affairs: Charitable donations
- Finance, including accounts payable and assets management
- Functions engaged in obtaining critical regulatory approvals

Transactions should be regularly and systematically monitored, for example⁽³⁾:

- **Expenses.** Checks should include high risk general ledger accounts (see previous page for high-risk areas) review and samples of transactional records making sure that they are correctly accounted for in the books and supported by documentation. In particular, the business rationale and proof of performance should be assessed
- **Cash disbursements.** Review and testing of cash payments. Check the business rationale and proof of performance.
- **Payments to high-risk third parties.** Test that payments to/from third parties such as intermediaries are appropriate for the services, that the payments match contracts and are paid through appropriate channels, rather than off-shore accounts.
- **Payroll transactions and expense reports.**
- **Transactions surrounding key date.** E.g., period surrounding winning a contract, obtaining a license, obtaining a concession, etc. Select transactions can be done by performing analytical procedures on the period surrounding the key date and select outlier items.

(3) Source: Transparency International anti-bribery guidance (<https://www.antibriberyguidance.org/guidance/17-monitoring-review/guidance#11>)

IS THE CORPORATION'S COMPLIANCE PROGRAM BEING IMPLEMENTED EFFECTIVELY?

Many organisations tend to have processes and programs on paper but fall short on certain implementation aspects. If a program is running effectively, often there is little incentive to review it regularly. The DOJ's guidance urges organisations to ascertain whether the program is static or dynamic, i.e., is it regularly reviewed and revised. The consideration included in this section helps distinguishing between a static program and a dynamic program.

COMMITMENT BY SENIOR AND MIDDLE MANAGEMENT

If senior management is committed to fostering a culture of compliance from the top, and demonstrates the following

- Zero tolerance for bribery and compliance issues;
- shared commitment through their actions; and
- complete oversight of ABAC compliance programs.

AUTONOMY AND RESOURCES

Senior management gives sufficient autonomy and resources to run the ABAC compliance program in terms of the following:

- The structure, seniority, and stature of the compliance function compared with other strategic functions;
- experience and qualification of resources running the compliance function and the funding available for it;
- accountability and reporting to the board/audit committee or the similar designated bodies within a company;
- reliable and sufficient data sources and analytical tools.

INCENTIVES AND DISCIPLINARY MEASURES

If the program includes incentives for compliance, and penalties and deterrents for non-compliance, and the following:

- The human resources process defining the authority and process flow for each instance of misconduct
- Consistent application of disciplinary actions and incentives across organisation
- Well-defined incentive system.

This includes detailed metrics for evaluating the consistency and effectiveness of disciplinary measures.



DOES THE CORPORATION'S COMPLIANCE PROGRAM WORK IN PRACTICE?



CONTINUOUS IMPROVEMENT

Organisations need invest in continuous improvement, periodic testing and review their compliance program. They need to ensure that it is current. To do this, they can adopt approaches, including undertaking regular internal audits and controls testing; and sharing updates on the evolving business and risk landscape with stakeholders. Consider monitoring and testing of new technologies, including AI.



MISCONDUCT INVESTIGATION

Organisations need to be able to timely detect misconduct and have effective response protocols in place, a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations/suspicions of misconduct by its employees, suppliers or agents. Organisations should have adequate response and investigations protocols in place, which include policies for preservation and collection of personal devices, communication platforms, and messaging applications.

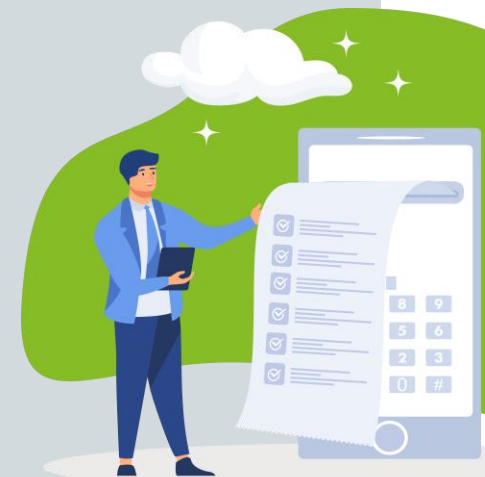


ANALYSIS AND REMEDIATION

Organisations need to be able to conduct a thorough root cause analysis and address the issue:

- Were the controls effective when misconduct took place?
- How the misconduct in question was funded?
- Other third parties involved and how were they onboarded?
- Were any red flags noted before the misconduct and how were those dealt with?
- What was the remediation plan to ensure that the similar misconduct will not take place in the future?
- Were any disciplinary actions taken?

To ensure that the compliance program works in practice, organisations need to determine whether the program was adequate and effective at the time of the offense in addressing existing and changing compliance risks. They also need to undertake a thorough analysis to understand what went wrong and the remediation needed to prevent similar events in the future.



Do you want to know more? **Contact us.**



GERRIE LENTING

Partner Forensic & Financial Crime

Office: +31 (0) 88 288 0781
Mobile: +31 (0) 61 099 9221
E-mail: glienting@deloitte.nl



FRANK CEDERHOUT

Director Forensic & Financial Crime

Office: +31 (0) 88 288 7283
Mobile: +31 (0) 65 359 8411
E-mail: fcederhout@deloitte.nl



NICK TEN DAM

Manager Forensic & Financial Crime

Office: +31 (0) 88 288 3132
Mobile: +31 (0) 65 008 8557
E-mail: ntendam@deloitte.nl



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s more than 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte organization shall be responsible for any loss whatsoever sustained by any person who relies on this communication.