

Corporate Compliance Forms and Tools

Compliance Program Effectiveness Self-Assessment

In June of 2020, the U.S. Department of Justice issued updated guidance on the key elements necessary for an effective compliance program.^[1] The guidance asks three primary questions:

1. ‘Is the corporation’s compliance program well designed?’
2. ‘Is the program being applied earnestly and in good faith?’ In other words, is the program adequately resourced and empowered to function effectively?
3. ‘Does the corporation’s compliance program work’ in practice?

Below is a self-assessment detailing the requirements of the U.S. Department of Justice guidance against which you can measure your own program to find opportunities for incremental improvement and advancement to a higher level of program maturity.

Is the Corporation’s Compliance Program Well Designed?

Risk Assessment

Measure of Effectiveness	Current Status/Actions Already Taken	Improvement Opportunities	Action Plan for Incremental Improvement
Risk management process: Company has documentation to show it has identified the varying risks presented by, among other factors, the location of its operations; its industry sector; the competitiveness of the markets in which it operates; the regulatory landscape; risks posed by potential clients and business partners; transactions with foreign governments; payments to foreign officials; use of third parties; gifts, travel, and entertainment expenses; and charitable and political donations.			
Company has documented its analysis and prioritization of the particular risks it faces based on factors including frequency, severity, likelihood, impact, and the effectiveness of existing controls and mitigation measures.			

Company can show its compliance program has been tailored based on the metrics and information identified in its risk assessment, including an assessment of the risk of criminal conduct, and has taken appropriate steps to design, implement, or modify each aspect of its compliance program to reduce the risk of criminal conduct.			
Risk-tailored resource allocation: Company can demonstrate it prioritizes addressing high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors, instead of spending a disproportionate amount of time policing low-risk areas. The company can also show it gives greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than it does to more modest and routine hospitality and entertainment expenditures.			
Updates and revisions: Company's risk assessment process is documented and periodically updated and revised to reflect lessons learned, and it is based upon continuous access to operational data and information across functions. Company can show its periodic review has led to updates in policies, procedures, and controls to account for risks discovered through misconduct or gaps in the compliance program.			
Lessons learned: The company has a documented process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region.			

Policies, Procedures, and Controls

Measure of Effectiveness	Current Status/Actions Already Taken	Improvement Opportunities	Action Plan for Incremental Improvement
Design: Company has a written code of conduct that sets forth, among other things, its commitment to full compliance with relevant laws, and it is accessible and applicable to all company employees.			

Company has established written policies and procedures that incorporate the culture of compliance into its day-to-day operations.			
Company has a documented process for designing and implementing new policies and procedures, and updating existing policies and procedures, that involves input from the business units.			
Company has a documented process for the management of policies and procedures, including authoring, approvals, version control, audit trail, and archives.			
Company can demonstrate the steps it has taken to determine whether specific policies/procedures/practices make sense for particular business segments/subsidiaries.			
Comprehensiveness: Company can demonstrate it monitors and implements policies and procedures that reflect and help to effectively mitigate the spectrum of risks it faces, including changes to the legal and regulatory landscape.			
Accessibility: Company can show it has communicated its policies and procedures to all employees and relevant third parties, ensuring there are no linguistic or other barriers to foreign employees' access.			
Policies and procedures have been published in a searchable format for easy reference and company tracks access to various policies and procedures to understand which policies are attracting more attention from relevant employees.			
Responsibility for operational integration: Company has a documented process for integrating policies and procedures and ensures they have been rolled out in a way that ensures employees' understanding of the policies.			
Company can show it ascertains whether employees understand policies and procedures related to high-risk laws and regulations, as well as the code of conduct, using surveys or knowledge checks, and makes modifications as warranted.			

Company can show its compliance policies and procedures are mapped to specific risks and reinforced through the company's internal control systems.			
Company has documentation to show it performs audits on policies, procedures, and controls to determine whether they have been implemented effectively—especially in high-risk areas.			
Company can show it has taken steps to ensure policies and procedures have been integrated into the organization, including through periodic training (see section C on training) and through certifications and attestations from all directors, officers, relevant employees, and, where appropriate, agents and business partners.			
Gatekeepers: Company can demonstrate it has provided guidance and training to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities) to ensure they know what misconduct to look for and when and how to escalate concerns.			

Training and Communications

Measure of Effectiveness	Current Status/Actions Already Taken	Improvement Opportunities	Action Plan for Incremental Improvement
Risk-based training: Company has a training program designed to reinforce its policies, procedures, and controls and to relay information in a manner tailored to the audience's size, sophistication, and subject matter expertise. For instance, some employees might receive practical advice or in-depth case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise, while others might receive shorter, more targeted training sessions to enable employees to spot issues and raise them to appropriate compliance, internal audit, or other risk management functions.			
Company has documentation of it having provided training that adequately addresses lessons learned from prior compliance incidents.			

Company can demonstrate it has conducted a risk-based analysis to determine who should be trained and on which subjects and ensures tailored training for high-risk and control employees, including training to address specific risks in areas where misconduct has previously occurred as well as enhanced or supplementary training for supervisory employees.			
Company tracks and maintains a record of attendance and completion for all company training programs and has a documented method for informing senior management of employees who fail to attend/complete required training.			
Form, content, and effectiveness: Company can show it tests employees on what they have learned and has a documented process for addressing gaps in understanding for employees who fail all or a portion of the testing.			
Company has a documented process through which employees can ask questions arising out of training.			
Company has established and documented methods to measure the effectiveness of its training curriculum and evaluates the extent to which training has an impact on employee behavior and operations.			
Company can show it has offered training in the form and language appropriate for the audience and provided it in both online and in-person formats with a clear rationale for its choice of format.			
Communications about misconduct: Company can demonstrate its senior management takes action to ensure employees know the company's position concerning misconduct, including communications when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (e.g., anonymized descriptions of the types of misconduct that lead to discipline.)			
Availability of guidance: Company can show it makes resources available to employees to provide guidance relating to compliance policies.			

Company has documentation to show it periodically assesses whether its employees know when to seek advice and whether they are actually willing and know how to do so.			
--	--	--	--

Confidential Reporting Structure and Investigation Process

Measure of Effectiveness	Current Status/Actions Already Taken	Improvement Opportunities	Action Plan for Incremental Improvement
Effectiveness of the reporting mechanism: Company can demonstrate it has established corporate governance mechanisms that can effectively detect and prevent misconduct, including an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct.			
Company can show it has ensured the reporting mechanism has been publicized to the company's employees and other third parties.			
Company can demonstrate it takes measures to test whether employees are aware of the hotline and feel comfortable using it and whether it is actually being used.			
Company has a documented method for assessing the seriousness of allegations it receives.			
Company's complaint-handling process is well documented and includes proactive measures to create appropriate processes for the submission of complaints, processes to protect whistleblowers, and a workplace atmosphere without fear of retaliation.			
Company has documented processes for handling the investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.			

Company can demonstrate it has ensured the compliance function has full access to reporting and investigative information.			
Properly scoped investigations by qualified personnel Company has a documented method for determining which complaints or red flags merit further investigation and ensures investigations are properly scoped.			
Company can show it takes steps to ensure investigations are independent, objective, appropriately conducted, and properly documented.			
Company has a clear and documented process to determine who should conduct an investigation and who has the authority to make that determination.			
Investigation response: Company can demonstrate it applies timing metrics to ensure responsiveness in the handling of investigations.			
Company has a documented process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations.			
Resources and tracking of results Company can show its reporting and investigation mechanisms are sufficiently staffed and funded.			
Company can show it collects, tracks, analyzes, and uses information from its reporting mechanisms, reports, and investigation findings to uncover patterns of misconduct or other red flags indicating compliance weaknesses.			
Company can show it periodically tests the effectiveness of its hotline, for example by tracking a report from start to finish.			

Third-Party Management

Measure of Effectiveness	Current Status/Actions Already Taken	Improvement Opportunities	Action Plan for Incremental Improvement
Risk-based and integrated processes: Company can show it applies risk-based due diligence to its third-party relationships in a manner appropriate for the size and nature of the company, transaction, and third party and corresponding to the nature and level of the enterprise risk identified by the company.			
Company can show it has ensured its due diligence process has been integrated into the relevant procurement and vendor management processes.			
Company can demonstrate an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.			
Appropriate controls: Company can show it ensures there is appropriate business rationale for needing a third party in a transaction as well as the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials.			
Company has documented how it monitors its third parties, whether it has audit rights to analyze the books and accounts of third parties, and, if so, whether the company has exercised those rights in the past.			
Company has documented how it trains its third-party relationship managers about compliance risks and how to manage such risks.			
Company can demonstrate how it incentivizes compliance and ethical behavior by third parties and whether it engages in risk management of its third parties throughout the lifespan of the relationship or only during the onboarding process.			

Management of relationships: Company can show it has considered and analyzed the compensation and incentive structures for third parties against their compliance risks to ensure they are appropriate for the industry and geographical region, and to ensure that compensation is commensurate with the services to be rendered.			
Company can demonstrate it has ensured that contract terms with third parties specifically describe the services to be performed and the applicable payment terms.			
Company has an established and documented method for ensuring services have actually been performed by its third parties prior to payment.			
Company can show it is engaged in ongoing monitoring of third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications from third parties.			
Real actions and consequences: Company can demonstrate it tracks red flags that are identified from due diligence on third parties and has an established and documented method addressing those red flags.			
Company documents and tracks third parties that do not pass its due diligence process or that are terminated following a compliance failure and takes steps to ensure that those third parties are not hired or rehired at a later date.			
If company discovers a third party is involved in misconduct, company can show it reviews the due diligence performed to determine how any red flags were resolved to ensure there are no gaps in the due diligence process and determines whether similar third parties should be suspended, terminated, or audited as a result of compliance issues.			

Mergers and Acquisitions (M&A)

Measure of Effectiveness	Current Status/Actions Already Taken	Improvement Opportunities	Action Plan for Incremental Improvement

Due diligence process: Company can show it performs comprehensive pre-M&A due diligence on any acquisition targets, allowing the company to accurately evaluate each target's value and take into account the costs of any corruption or misconduct by the target.			
Integration in the M&A process: Company can show the compliance function has been integrated into the merger, acquisition, and integration process.			
Process connecting due diligence to implementation: Company has documented any misconduct or risk of misconduct, identified during due diligence, as well as the specific persons who conducted the risk review for the acquired/merged entities, and the M&A due diligence process generally.			
Company has a documented process for tracking and remediating misconduct or misconduct risks identified during the due diligence process.			
Company has a documented process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities.			
Company has a documented process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls.			

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)