Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A New Measuring Stick For Anti-Bribery Compliance Programs

John J. Pease III

Louis Ramos

Benjamin D. Klein

Law360, New York (October 16, 2016, 4:25 PM EDT) -- On Oct. 15, 2016, the International Organization for Standardization adopted ISO 37001,[1] a certifiable international "anti-bribery management system" that has the potential to change how the U.S. Department of Justice, U.S. Securities and Exchange Commission, and foreign regulators evaluate and grade corporate compliance programs. While the ISO is a voluntary, nongovernmental organization, it is composed of both public- and private-sector experts, and many of its standards have been described as international benchmarks. This article examines ISO 37001 — which has been under development for over three years — and its potential implications for companies concerned about their compliance credentials.

Summary

ISO 37001 was developed to help companies and other organizations establish, operate and improve their anti-bribery compliance programs. It outlines the anti-corruption controls considered to be "international good practice[s]" for preventing, detecting, deterring, and remediating corruption risks.[2]

To be certified as ISO 37001-compliant, an organization will be required to develop and implement an anti-bribery management system designed not only to prevent, detect, and deter bribery, but also to "comply with anti-bribery laws and voluntary commitments applicable to its activities."[3] Such "systems" must address not only the bribery of foreign government officials, as proscribed by the Foreign Corrupt Practices Act, but also bribery in the "private and not-for-profit sectors."[4] In addition, anti-bribery management systems are expected to address the risks posed by both active bribery (bribery by an organization, its personnel, and its associates) and passive bribery (bribery of an organization, its personnel, and its associates).[5] ISO 37001 recognizes that laws like the FCPA and the U.K. Bribery Act 2010 criminalize both direct and indirect acts of bribery, and calls on organizations to account for third-party risks, such as "bribe[s] offered or accepted through or by a third party."[6]

ISO 37001 was drafted by an ISO committee composed of advisory groups

from 37 countries — including the United States — and is designed for "small, medium and large organizations in all sectors, including public, private and not-for-profit sectors."[7]

Requirements

Like the FCPA Resource Guide, ISO 37001 recognizes that companies cannot "completely eliminate the risk of bribery" and declines to prescribe a "one-size-fits-all" model for anti-corruption compliance.[8] Instead, ISO 37001 embraces a "reasonable and proportionate" risk-based approach for developing compliance programs and instructs companies to consider the following factors:

- Size and structure of the organization;
- Locations and sectors in which the organization operates or anticipates operating;
- Nature, scale, and complexity of the organization's activities and operations;
- Entities over which the organization has control;
- The organization's business associates;
- Nature and the extent of interactions with public officials; and
- Applicable statutory, regulatory, contractual, and professional obligations and duties.[9]

When developing anti-corruption compliance programs, companies are expected to account for any issues identified in their "bribery risk assessment[s]."[10] Such assessments should be designed and performed in a manner that enables companies to identify, evaluate, prioritize and respond to bribery risks as well as assess "the suitability and effectiveness of the organization's existing controls."[11] Companies should use risk assessment results to make more informed decisions about the "allocation of anti-bribery compliance personnel, resources and activities."[12]

In addition to conducting risk assessments, ISO 37001 requires companies to do the following:

- Develop and Maintain Compliance Policies and Procedures: "Well-managed organization[s]" are "expected to have compliance polic[ies] supported by appropriate management systems."[13] In addition, companies are expected to "implement procedures that are designed to prevent the offering, provision or acceptance of gifts, hospitality, donations and similar benefits where the offering, provision or acceptance is, or could reasonably be perceived as, bribery."[14] Companies should ensure that their anti-corruption compliance policies/procedures are "communicated in appropriate languages" to both employees and business associates.[15]

- Implement Compliance Training Programs: Companies are expected to provide their employees with "adequate and appropriate anti-bribery awareness and training," and "retain documented information on the training procedures, the content of the training, and when and to whom it was provided."[16] Moreover, when a company engages a third party whose employees "could pose more than a low bribery risk to the organization," the company should ensure that those individuals receive anti-corruption compliance training by the company, the third party or a designee.[17]

- Demonstrate Effective Tone at the Top: The "top management," defined as the "group of people who directs and controls [the] organization at the highest level,"[18] is expected to demonstrate leadership and commitment to anti-corruption compliance including "communicating internally the importance of effective anti-bribery management and of conforming to the anti-bribery management system requirements" and "promoting an appropriate anti-bribery culture within the organization."[19] The "governing body" is expected to demonstrate a similar commitment by "approving the organization's anti-bribery policy," "requiring that adequate and appropriate resources ... are allocated and assigned," and "exercising reasonable oversight over the implementation of the organization's anti-bribery management system by top management."[20]

- Conduct Risk-Based Due Diligence: Companies should conduct due diligence on "specific transactions, projects, activities, [and] business associates" — as well as company personnel — considered to have more than a "low bribery risk" — a term that is not defined in the standard.[21] ISO 37001 recognizes that "[t]he nature, type and extent of due diligence undertaken will depend on factors such as the ability of the organization to obtain sufficient information, the cost of obtaining information, and the extent of the possible bribery risk posed by the relationship."[22]

- Obtain Third-Party Compliance Certifications and Termination Rights: Companies should require third parties that "pose more than a low bribery risk" to certify that they will "commit to preventing bribery ... in connection with the relevant transaction, project, activity, or relationship."[23] In addition, companies should ensure that their third-party contracts contain termination provisions that allows them to terminate their contracts if the third party engages in bribery.[24]

- Obtain Compliance Commitments from Employees: Companies must "require [their] personnel to comply with the anti-bribery policy and anti-bribery management system, and give the organization the right to discipline personnel in the event of non-compliance."[25]

- Implement Internal Controls: Companies must implement both "financial controls" and "non-financial controls," with the latter consisting of "procurement, operational, sales, [and] commercial" measures that manage bribery risks.[26]

- Develop Reporting Channels and Ensure Whistleblower Protections: Companies are expected to implement procedures that enable and encourage personnel and third parties to "report in good faith or on the basis of a reasonable belief attempted, suspected and actual bribery, or any violation of or weakness in the anti-bribery management system."[27] The procedures should

"allow anonymous reporting" and "prohibit retaliation, and protect those making reports from retaliation."[28]

- Document Compliance Efforts: Companies are expected to document their efforts to comply with ISO 37001, but the extent of the documentation depends on the size of the organization, the nature of its activities, and the complexity of its processes.[29]

- Periodically Review and Improve Anti-Corruption Compliance Controls: Companies are expected to continually assess and review their anti-bribery management systems in order to ensure their "suitability, adequacy and effectiveness."[30]

- Prohibit Facilitation Payments: While the FCPA allows for "facilitation payments," which are described by U.S. regulators as payments "made to further 'routine government action' that involves non-discretionary acts,"[31] ISO 37001 states that "they are illegal in most locations and are treated as bribes for the purpose of this document, and they should be prohibited by the organization's anti-bribery management system."[32]

Certification

The ISO does not provide a road map to certification for any of its standards; in fact, the ISO explicitly disclaims any involvement in the certification process.[33] Certification can only be obtained through an "external certification body."[34]

Prior to engaging a certification body, a company should conduct an internal review of its policies, procedures, and practices to ensure that they align with ISO 37001, as well as a risk assessment as required by Section 4.5 of ISO 37001. While the internal review and risk assessment can be performed using company resources, companies may be better served by engaging a law firm or other third-party with anti-corruption compliance counseling experience.

Once the internal review and risk assessment are complete, the company should take steps to implement any necessary reforms — e.g. update compliance policies, improve internal controls, increase employee training, and test for and monitor new third-party risks. The company should document these improvements and ensure that the other components of its compliance program are adequately documented (e.g., training records, compliance certifications, records clearing indicating third-party due diligence and monitoring, and functioning reporting channels).

Within a matter of months, some of the implemented reforms should be tested by the company's "audit programme."[35] The company is expected to conduct "reasonable, proportionate and risk based" audits that review "procedures, controls and systems" for, inter alia, "weaknesses in, or opportunities for improvement to, the anti-bribery management system."[36] The results of those audits must be reported to "relevant management, the anti-bribery compliance function, top management and, as appropriate, the governing body."[37] Thus, the company's internal auditing function should work to ensure that the

company has made the necessary strides to satisfy an external certification body.

In an abundance of caution, one month before the ISO certification review, the company should conduct a final internal audit to ensure its compliance with ISO 37001.

The duration of the ISO certification process will ultimately depend on the size of the organization and the amount of policies, procedures, internal controls, and practices that need to be examined.

Implications

ISO 37001 provides companies with a new "measuring stick" for evaluating their compliance programs and ensuring that they meet a common international standard. In addition, ISO 37001 enables companies to make more informed decisions about business partners and other third-party representatives. Companies that receive an ISO 37001 certification — especially those that work in corruption-prone countries or high-risk industries or that have frequent exposure to government officials — will potentially have a comparative advantage against competitors that do not have the qualification.

ISO 37001 may also prove helpful to companies caught in the crosshairs of government investigations, which increasingly involve multiple jurisdictions and enforcement authorities. Although the ISO 37001 certification does not absolve companies from liability for anti-corruption law violations, it is expected to offer an independent validation of a company's anti-corruption compliance program, and therefore may help a company make the case that its internal controls are both "strong on paper" and strong in practice.[38]

In the United States, effective compliance programs may help companies avoid a contemplated prosecution entirely or otherwise achieve a more favorable settlement where charges are filed. The U.S. Department of Justice's Principles of Federal Prosecution of Business Organizations counsel prosecutors to evaluate "the existence and effectiveness of the corporation's pre-existing compliance program" when determining whether to charge a corporation with a crime.[39] Chapter 8 of the U.S. Sentencing Guidelines provides that prosecutors should consider whether a company had an "effective compliance and ethics program" at the time of the offense when assessing culpability, and such a compliance program could result in a reduction in the company's culpability score, which is used to calculate the fine range. [40]

ISO 37001 may have even broader implications for companies subject to U.K. jurisdiction because the Bribery Act — unlike the FCPA — contains an "adequate procedures" defense. According to the U.K. Ministry of Justice, "[i]t is a full defence for an organisation to prove that despite a particular case of bribery it nevertheless had adequate procedures in place to prevent persons associated with it from bribing."[41] Companies that wish to invoke this defense must "prove that [they] had adequate procedures in place to prevent bribery,"[42] and an ISO 37001 certification may serve as an independent and objective validation of a compliance program's adequacy.[43]

In conclusion, ISO 37001 offers a uniform set of anti-corruption measures across industries and regions, and provides companies with opportunities to mitigate risks and achieve greater clarity in measuring their compliance programs' effectiveness. It remains to be seen whether enforcement authorities will rely on ISO 37001 as the ultimate measuring stick to evaluate compliance programs, but companies with anti-corruption programs that receive ISO 37001 certifications will likely be better positioned to withstand government scrutiny.

—By John J. Pease III, Louis Ramos, Benjamin D. Klein and Andrew W. Katz, Morgan Lewis & Bockius LLP

John Pease is a partner in Morgan Lewis' Philadelphia office and former executive counsel for Teva Pharmaceuticals. He served as an assistant U.S. attorney for the Eastern District of Pennsylvania from 1997 to 2013 and as chief of the Government and Health Care Fraud Section in the Criminal Division from 2009 to 2013.

Louis Ramos is a partner in the firm's Washington, D.C., office. He was assistant general counsel in the compliance division at Pfizer for four years and served for nearly six years as an assistant U.S. attorney in the District of Columbia

Benjamin Klein is an associate in the firm's Washington office.

Andrew Katz is an associate in the firm's Philadelphia office.

[1] http://www.iso.org/iso/catalogue_detail?csnumber=65034.

[2] ISO 37001, Introduction.

[3] Id. at Sec. 1.

[4] Id.

[5] Id.

[6] Id.

[7] Id. at Introduction. For information about countries involved in the drafting of ISO 37001, see ISO, "Technical Committees – ISO/PC 278 – Anti-bribery management systems" (2016),http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee_participation.htm?commid=4515115.

[8] Id. at Sec. 4.4; Crim. Div. of the US Dep't of Justice & Enforcement Div. of the US Sec. & Exch. Comm'n, A Resource Guide to the U.S. Foreign Corrupt Practices Act at 57 (Nov. 14, 2012),http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf [hereinafter FCPA Resource Guide] ("[R]ecognizing that companies may consider a variety of factors when making their own determination of what is appropriate for their specific business needs."); see also id. ("[E]ach compliance program should be tailored to an organization's specific needs, risks, and challenges.").

[9] ISO 37001, Sec. 4.4.

[10] Id. at Sec. 4.5; see also id., Annex, Sec. A.4. Section 4.5of ISO 37001 is devoted to the design, implementation, and documentation of risk assessments.

[11] Id. at Sec. 4.5.

[12] Id. at Annex, Sec. A.4.1.

[13] ISO 37001, Introduction. See also id. at 5.2.

[14] ISO 37001, Sec. 8.7.

[15] ISO 37001, Sec. 5.2.

[16] ISO 37001, Sec. 7.3.

[17] ISO 37001, Annex, Sec. A.9.8.

[18] ISO 37001, Sec. 3.6.

[19] ISO 37001, Sec. 5.1.2.

[20] ISO 37001, Sec. 5.1.1.

[21] ISO 37001, Secs. 8.2, 7.2.2.2

[22] ISO 37001, Annex, Sec. A.10.3.

[23] ISO 37001, Sec. 8.6.

[24] ISO 37001, Sec. 8.6.

[25] ISO 37001, Sec. 7.2.2.1.

[26] ISO 37001, Sec. 8.4.

[27] ISO 37001, Sec. 8.9.

[28] ISO 37001, Sec. 8.9.

[29] ISO 37001, Sec. 7.5.1; see also id. at Annex, Sec. A.17.

[30] ISO 37001, Sec. 10.2; see also id. at Sec. 9.4.

[31] FCPA Resource Guide at 25.

[32] ISO 37001, Annex, Sec. A.2.2.1.

[33] “ISO Standards: Certification” (2016), http://www.iso.org/iso/home/standards/certification.htm.

[34] Id.

[35] ISO 37001 at Sec. 9.2.2.

[36] ISO 37001 at Sec. 9.2.3(d).

[37] ISO 37001 at Sec. 9.2.2(d).

[38] FCPA Resource Guide at 57.

[39] US Dep't of Justice, Secs. 9-28.300, 9-28.800, https://www.justice.gov/usam/usam-9-28000-principles-federal-prosecution-business-organizations.

[40] See US Sentencing Guidelines, Sec. 8B2.1; see also id. at Sec. 8C2.5(f) ("If the offense occurred even though the organization had in place at the time of the offense an effective compliance and ethics program, as provided in §8B2.1 (Effective Compliance and Ethics Program), subtract 3 points.").

[41] UK Ministry of Justice, The Bribery Act 2010: Guidance 6 (Mar. 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf.

[42] Id.

[43] While neither the Bribery Act nor the official "Guidance" define the term "adequate procedures," a government "Consultation Paper" presents "six broad management principles" intended to "help relevant commercial organisations devide what bribery prevention procedures they can put in place." See UK Ministry of Justice, "Consultation on guidance about commercial organisations preventing bribery (section 9 of the Bribery Act 2010)," 11 (2010).
