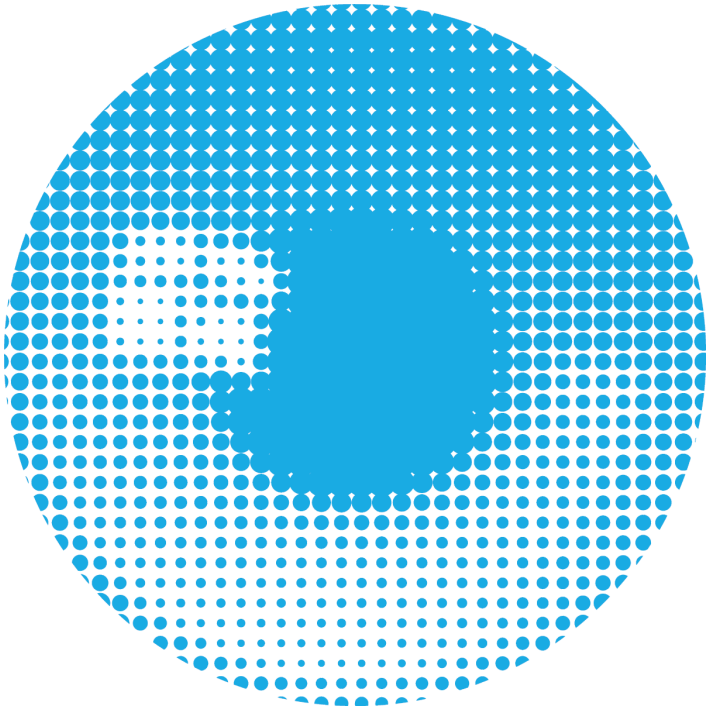
Deloitte.



# Focus on 5

## Five insights on ISO 37001

Multinational businesses around the world may be considering how to address the recently issued ISO 37001:16, *Anti-bribery management systems — Requirements with guidance for use* (ISO 37001). Released in late 2016, ISO 37001 addresses "establishing, implementing, maintaining, reviewing, and improving an anti-bribery management system," whether as a stand-alone initiative or part of a broader anti-corruption compliance program.[1]

Several law firms and certification organizations have offered helpful summaries of and recommendations for implementing the standard and becoming certified; yet for many companies, questions still exist: Is there value in pursuing ISO 37001 certification or should our focus be on using it to strengthen our existing anti-corruption compliance programs independent of certification? What does the standard suggest that we aren't already doing? What are the benefits of fully implementing the standard relative to the costs?

Here are five insights for consideration to help you address these and other important questions your organization may have:

**Start by understanding how the standard fits in the regulatory and compliance ecosystem.**

From a US regulatory perspective, definitive guidance on anti-corruption compliance is contained within information issued by the US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) in 2012's *"A Resource Guide to the U.S. Foreign Corrupt Practices Act"* (FCPA). This Resource Guide, along with the updated US Sentencing Guidelines, the "Yates Memo," and other authoritative guidance, provides a compilation of information about the provisions and enforcement of the FCPA, as well as an essential resource on the foundational elements and characteristics of an effective anti-corruption compliance program.

Importantly, the Resource Guide provides principles-based, *not rules-based*, guidance to encourage thoughtful, risk-based design and implementation of anti-corruption compliance programs that fit the particular circumstances of an individual company. There is no "one size fits all" answer. By so doing, it effectively discourages the notion that by meeting any one set of check-the-box "rules," a company has done everything necessary for compliance. Circumstances change, and corporate compliance programs must continually evolve and adapt to those changed circumstances.

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

ISO 37001 is the newest addition to the *non-regulatory* ecosystem of guidance and standards that provide additional insights into and substance around the implementation of principles-based anti-corruption guidance issued by US regulators and other authorities around the world, including the UK and Brazil. Prominent within this ecosystem are guidance from The Committee of Sponsoring Organizations of the Treadway Commission (COSO); the American Institute of Certified Public Accountants, Institute of Internal Auditors, and Association of Certified Fraud Examiners; and the Open Compliance and Ethics Group (OCEG), among others.

That body of guidance and standards, including the standards laid out in ISO 37001, should be considered and implemented as appropriate within the context of a company's specific risk profile. In other words, in the eyes of a regulator, the mere certification under a standard, or adherence to specific guidelines, are unlikely to provide a compliance "safe harbor" or defense to prosecution for violations. The substance of the anti-corruption program elements subject to the certification will be critical from a regulatory perspective, taking into consideration the quality of information provided, the skill, thoughtfulness, and proactivity of the certifying body, and the thoroughness of the review performed. As such, most regulators are likely to assess the facts of how a company implements a compliance program, tailored to its specific risk profile — i.e., the substance, not the form of the program — to determine its effectiveness.

### ISO 37001 does not preclude the need for a risk assessment of an existing compliance program.

ISO 37001 only addresses anti-bribery management systems, not broader fraud and other corruption issues. Seeking certification or implementing requirements of the standard should be viewed as a way of enhancing, not replacing, a company's existing anti-corruption compliance programs.

The opportunity — and challenge — for companies is to carefully assess and prioritize all of their anti-corruption-related risks, including those addressed by the anti-bribery standard. Then they can thoughtfully review and assess how their existing anti-corruption program addresses those risks: first, in the context of specific regulatory guidance; second, with consideration of non-regulatory guidance and standards; and third, with as few redundancies as possible.

If, after a company completes its review and assessment of its existing anti-corruption compliance program, it determines that thoughtful consideration has been given to both the regulatory and non-regulatory guidance available, no further action may be needed. However, for other companies that may have less mature anti-corruption programs, ISO 37001 may be effective guidance for quickly moving up the maturity curve without necessarily investing significant time in wading through the regulatory and non-regulatory ecosystem to develop their approach.

### Certification is not mandatory, but pressure to become certified may grow.

ISO certification is viewed by many companies as meeting a very high standard of leading practices for business systems and processes. As a result, some companies may view ISO 37001 certification as a sort of "insurance policy" to be used with regulatory investigators or other companies performing third-party due diligence as part of their own anti-corruption programs. To the extent that the number of companies pursuing certification increases over time, pressure could grow for others to follow suit, particularly for third-party intermediaries. It is, therefore, important for companies to monitor the external environment in consultation with their professional advisers, as they weigh the costs and benefits of certification. What effort will be required, what costs will be incurred, how might other businesses view certification, and how might certification contribute to — or potentially detract from — the company's compliance program in general and its anti-bribery efforts specifically? Each company's answers to these questions may be very different.

### A check-the-box approach won't be sufficient.

Regardless of a company's objectives for seeking ISO 37001 certification, merely checking the boxes on a form will not be good enough. The standard's requirements contain many qualifiers, such as "appropriate" and "reasonable," in describing the elements of effective management systems, leaving much subjectivity in how those systems are designed and deployed. The effectiveness of a company's approach, therefore, will depend on the depth, breadth, and overall thoroughness of the certification process it undertakes; the methods of addressing those "appropriate" and "reasonable" qualifiers; and how outcomes are implemented, documented, monitored, and assessed over time. Similarly, the rigorousness of the reviewer and the reviewer's approach to the standards (and the qualifiers) in ISO 37001 will impact the worth of the certification. Again, it's the substance, not the form, of a compliance program that determines its effectiveness, not the certification alone.

### Whether seeking ISO 37001 certification or not, these steps are important.

To avoid a check-the-box approach, the process of ISO 37001 certification — or further assessment or enhancement of a company's anti-corruption program — should begin with a strong compliance health check, maturity assessment, or risk assessment. Such an assessment should include a detailed inventory on a global basis of areas of corruption risk, including government touch points and risk profiles, broken down by geography and business operations. It should also include a detailed assessment of internal controls, business processes, and technology supporting the company's anti-corruption compliance program.

As part of a compliance health check, companies should evaluate the presence

and quality of other important compliance program elements, including:

- Commitment from senior management and the board, and a clearly communicated tone related to corruption
- A code of conduct and compliance policies and procedures
- Program resources and autonomy
- Employee communication, training, and awareness
- Incentives and disciplinary measures
- Third-party due diligence and monitoring procedures
- Confidential reporting and internal investigation and response mechanisms
- Continuous improvement, including periodic auditing, testing, and control gap analysis
- For mergers and acquisitions, pre-acquisition due diligence and post-acquisition integration
- Technology used to strengthen anti-corruption compliance programs, including tools for detecting red flags in financial statements and data analytics used to address anti-corruption risk and facilitate risk assessment and monitoring.

Perhaps most importantly, a mature compliance program is not one that is merely well-designed or even fully implemented — it also must be effective in preventing and detecting corruption-related misconduct. As noted above, a company with a mature program must routinely assess the effectiveness of its program and continually improve it over time.

## Our take: Enhance rather than reinvent

ISO 37001 offers valuable direction for companies establishing new, or strengthening existing, anti-corruption compliance programs and management systems. Its requirements and guidance appear thoughtfully designed to help companies prevent, detect, and respond to bribery while complying with anti-bribery laws. However, companies seeking ISO 37001 certification alone as a compliance "silver bullet" could be in for a surprise if they fall under regulatory investigation — certification is not a "get out of jail free" card. Instead, the many valuable elements of the ISO 37001 guidance should be viewed as additive to and enhancements of, rather than a replacement for, a company's broader anti-corruption compliance program.

**Contact:**

**Rob Biskup**
Managing Director | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
rbiskup@deloitte.com
+1 313 396 3310

**Bill Pollard**
Partner | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
wpollard@deloitte.com
+1 773 640 0225

**Holly Tucker**
Partner | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
htucker@deloitte.com
+1 214 394 5352

**Matt Queler**
Principal | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
mqueler@deloitte.com
+ 1 202 220 2156

**Rebecca L. Burtless-Creps**
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
rburtlesscreps@deloitte.com
+1 313 396 2542