SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

AUGUST 2018

Meet Laura Ellis

Ethics Program Manager for Global Compliance Enablement
Cisco International Limited
Feltham, UK

This article, published in *Compliance & Ethics Professional*, appears here with permission from the Society of Corporate Compliance & Ethics. Call SCCE at +1 952.933.4977 or 888.277.4977 with reprint requests.

by Maurice L. Crescenzi, Jr.

ISO 37001 Certification: Understanding and navigating the process

- The International Organization for Standardization (ISO) is a non-governmental organization that facilitates the international unification of industrial standards and management systems.
- Registrars or "certifying bodies" issue ISO certifications, and leading practices suggest it is best to obtain ISO certifications from accredited registrars.
- ISO 37001 establishes a standardized management system for managing the risk of bribery and corruption in both the public and private sectors.
- Although ISO 37001 has been received positively in the international ethics and compliance community, there is an accompanying sentiment that it does not introduce anything fundamentally new.
- How quickly and widely ISO 37001 will be adopted in the public and private sectors remains to be seen.

__Maurice Crescenzi__ (mcrescenzi@aol.com) is Managing Director, Ethics and Compliance Practice Leader at Grant Thornton LLP in New York, NY.

The International Organization for Standardization (ISO) is a non-governmental organization based in Geneva, Switzerland. ISO was formed in 1947 as a result of the merger of two previously separate standards-setting organizations, the International Federation of the National Standardizing Associations and the United Nations Standards Coordinating Committee. ISO's charge is to "facilitate the international coordination and unification of industrial standards."[1,2] In pursuing its mission, ISO works closely with more than 700 international, regional, and national organizations across approximately 162 countries to establish business standards. ISO's list of partners includes the World Trade Organization (WTO), World Standards Cooperation (WSC), and the United Nations (UN).[3]

Crescenzi

To date, ISO has published more than 21,000 international standards that apply across a range of industries and organizational functional areas. These standards help organizations improve operational efficiency and effectiveness. They also promote good management practices. Generally, ISO standards are neither industry- nor product-specific.

Perhaps the most well-known ISO standards relate to quality and environmental management systems; however, ISO has also published standards that help organizations improve in other areas, such as social responsibility, sustainability, and enterprise risk management—standards that reflect the cross-industry, global imperative of achieving long-term organizational growth, and at the same time minimizing negative environmental and social impacts.[4]

Not all ISO standards carry the same weight or effect, however. In some instances, ISO standards simply set forth guidance, good practices, and advice. In other instances, ISO standards set forth actual *requirements*. Organizations may strive to be formally certified with regard to the latter category of requirements-based standards. ISO 37001 is considered a requirements-based standard—with regard to which organizations may strive for certification.

ISO 37001: Anti-bribery management systems

In October 2016, after a three-year drafting process, ISO published standard 37001, which sets forth a comprehensive framework for designing, implementing, and maintaining anti-bribery and anti-corruption programs.[5] The drafting effort was led by lawyer Neill Stansbury, who served as the secretariat and chairperson for the drafting committee—ISO Technical Committee ISO/TC 309. Supporting this effort were approximately 37 participating countries, 22 observing countries, and 8 liaison organizations.[6, 7] ISO 37001 applies to public, private, and non-governmental organizations equally. ISO 37001 is voluntary.

ISO developed and published this standard because bribery and corruption is a widespread, global issue affecting both the public and private sectors. One of the most destructive and complex problems of our time, and a trillion dollar crisis by all accounts, ISO links bribery and corruption to social, moral, economic, and political concerns—as well as to poor organizational governance and unfair competition in the global marketplace.[8]

ISO acknowledges that governments around the world have made progress combatting bribery and corruption through various laws, guiding frameworks, conventions, and regulatory agency guidance and enforcement; however, ISO maintains that public and private organizations must also play a critical role in battling corruption. Organizations can help pursue this objective by proactively developing anti-bribery and anti-corruption programs and extending them to the third parties with which they do business.[9] ISO 37001 is intended to help organizations do just that.

In some instances, ISO standards simply set forth guidance, good practices, and advice. In other instances, ISO standards set forth actual *requirements*.

ISO 37001 sets out a framework for an organization's anti-bribery and anti-corruption program. Notwithstanding the structure of the table of contents, the ISO 37001 program framework—when distilled to its essence—is composed of the following ten elements: (1) culture, (2) governance and oversight, (3) risk assessments and due diligence, (4) policies and procedures, (5) training and communications, (6) speaking up (whistleblowing), (7) investigations and case management, (8) auditing and monitoring, (9) third-party risk management, and (10) continuous improvement. Each element is composed of detailed guidance and requirements. ISO 37001 also expects organizations to document all aspects of its program sufficiently.

Despite the generally positive splash that ISO 37001 has made on the international ethics and compliance scene, there is an accompanying sense that ISO 37001 does not introduce anything fundamentally new. In fact, some ethics and compliance professionals view the release of ISO 37001 as a "complete yawner," because the standard reflects a program framework previously established in numerous other leading-practices sources.[10]

For example, ISO 37001 resembles closely the framework set forth in an elder-sibling standard, ISO 19600—Standard on Compliance Management Systems (2014). ISO 19600 establishes a framework for a compliance program management system that can be applied across a host of compliance risk areas, including anti-bribery and anti-corruption, antitrust and competition law, anti-money laundering, and so on. Some ethics and compliance professionals, therefore, question the need for ISO 37001, since much of its essence had been previously covered in ISO 19600.

The standard reflects a program framework previously established in numerous other leading-practices sources.

Moreover, the anti-bribery and anti-corruption compliance program framework set forth in ISO 37001 reflects—albeit in an ISO management-system format and in an ISO writing style—many of the same underlying requirements, expectations, and guidance set forth in key legislation (e.g., U.S. Foreign Corrupt Practices Act [FCPA], UK Bribery Act), guiding frameworks (e.g., U.S. Federal Sentencing Guidelines, OECD), agency guidance (e.g., Department of Justice and Securities and Exchange Commission Guidance, UK Ministry of Justice Bribery Act 2010 Guidance), and program-design requirements set forth in many deferred prosecution agreements related to FCPA violations. However, although a common programmatic structure recurs across many of these guiding frameworks, it is equally true that the level of guidance and technical prescription set forth in ISO 37001 goes beyond other forms of guidance in many respects.

For instance, although the U.S. Federal Sentencing Guidelines generally call for organizations to "periodically assess the risk of criminal conduct and…take appropriate steps to design, implement, or modify [the program] to reduce the risk of criminal conduct identified through this process," ISO 37001 drills into this programmatic element with greater specificity and prescription, requiring organizations to: (1) undertake regular bribery risk assessments; (2) identify, analyze, assess, and prioritize bribery risks; (3) evaluate the maturity of the related controls intended to mitigate bribery risks; (4) review the risk assessment process on a regular basis; and (5) document the risk assessment process.[11] ISO 37001 also provides approximately two pages of guidance as to designing and implementing the risk assessment process.

In addition, although the "risk assessment" section of ISO 37001 is technically limited to Section 4.5, it can be said that ISO 37001 addresses additional risk assessment-related requirements in other sections, too (e.g., Section 4.1, Understanding the Organization and its Context; Section 4.2, Understanding the Needs and Expectations of Interested Parties; Section 4.3, Determining the Scope of the Management System; Section 4.4, Management System Processes). The risk assessment example is just one comparative example between one particular guiding framework (i.e., the U.S. Federal Sentencing Guidelines) and ISO 37001. There are many other examples, too—across other programmatic elements (e.g., communications and training) and other guiding frameworks and agency guidance.

Regardless of whether ISO 37001 introduces anything fundamentally new, it is important to remember that ISO 37001 is an internationally agreed-upon standard that can apply equally to public and private organizations around the world. Some of the more well-known anti-bribery and anti-corruption laws and pieces of guidance, whose releases predated the issuance of ISO 37001, are limited to certain geographies and jurisdictions. ISO 37001, on the other hand, is truly global. More than 50 countries supported the drafting effort.

Moreover, ISO 37001 is auditable, which means that an independent body can certify that an organization's anti-bribery and anti-corruption compliance program meets the minimum requirements and expectations set forth in ISO 37001.[12] These are important distinctions between the myriad legacy anti-bribery and anti-corruption frameworks and pieces of guidance—and ISO 37001.

Accreditation and certification

Although ISO develops standards, it does not—itself—certify organizations with regard to its standards. The ISO certification process is administered by external certification bodies (CBs) or "registrars." These CBs and registrars commission onsite audits of the organization's program to determine whether the program satisfies the requirements of the ISO standard in question. Certifications are typically good for three years, with the first year involving the initial certification review, and the subsequent two years involving annual surveillance reviews. In all instances, CBs and registrars may only base their audit and review work on the scope of the standard in question. They may not audit or review aspects of the organization that are outside of the scope of the ISO standard under consideration.

CBs and registrars are sometimes (but not always) accredited by bodies that sit one level above the CB or registrar. These bodies are known as regional accreditation agencies. For example, in the United States, the ANSI-ASQ National Accreditation Board (ANAB) accredits CBs and registrars that, in turn, certify organizations with regard to their ISO-based programs. This hierarchy is intentional, positioning accreditation one level higher than certification. This one-over-one model is analogous to higher education, where students receive a degree or certification from a university that, itself, has been accredited by a higher accreditation body.[13]

From an organizational perspective, it is recommended—although not required—that organizations strive to obtain ISO certification from certifying bodies and registrars that are accredited by accreditation agencies, since this is thought to give more weight and credibility to the certification. In the United States, ANAB appears to be positioned to accredit CBs and registrars with regard to ISO 37001, which ANAB considers a "base standard program." However, as of the date of this writing (February 2018), it does not appear as though any accredited CBs or registrars have been established in the United States regarding ISO 37001.[14]

Scope and cost of certification

Generally speaking, ISO certifications attained at the parent company or headquarters level of an organization are only valid for that organizational entity. Headquarters-level certifications typically do not extend to other parts of the organization, such as subsidiaries, business units, or country markets, unless those aspects of the organization were included in the scope of the review performed by the CB or registrar. In most instances, each organizational entity must apply for its own certification. At times, however, a "group certification" can be issued at the headquarters level and applied to other aspects of the organization, if the initial review or audit is scoped that way in the first place, and if the fees take this extended scope into consideration.[15]

The cost of striving for ISO certification can vary. The cost depends on a number of factors that include: (1) the pricing models and fee ranges of the CBs and registrars; (2) the organizational, functional, and geographic scope of the certification; and (3) the number of organizational entities striving for certification.[16]

Costs associated with ISO 37001 certification may also be contingent on whether it is the first, second, or third attempt to achieve certification. Organizations often seek a second or third attempt when the CB or registrar identifies major non-conformities (i.e., significant gaps in the program) and minor non-conformities (i.e., minor gaps). The pricing related to second or third attempts can also vary depending on the remediation window allowed.

> Costs associated with ISO 37001 certification may also be contingent on whether it is the first, second, or third attempt to achieve certification.

Early adopters: Public sector

Since its release, several countries and local governments have adopted ISO 37001 as their official anti-corruption standard. These countries and governments include Singapore, Peru, Philippines, Malaysia, and the Chinese province of Shenzhen. It also appears that certain European countries are in the process of adopting ISO 37001.

In the public sector, "adoption" can mean various things. In some cases, a country will "adopt" ISO 37001 and create an accreditation system for the CBs or registrars who will, in turn, perform independent ISO 37001 certifications. For instance, the United Kingdom is in the process of developing an accreditation model of its own, but it has yet to be completed.

Other countries will "adopt" ISO 37001 such that their national standards bodies embrace the standard and encourage organizations to comply with it locally. For instance, Singapore recently adopted ISO 37001 and announced its own version of the standard: Singapore Standard (SS) ISO 37001. Singapore has also created an agency under its Ministry of Trade and Industry, which will provide training, consulting, and financial support for organizations interested in obtaining certification.[17] The same sort of activity is underway in Malaysia and China.[18]

The Malaysia Department of Standards and the Anti-Corruption Commission (MACC), together, implemented a country-specific version of ISO 37001 known as the Malaysian Standard 37001. The MACC intends to strive for ISO 37001 certification to further strengthen its efforts to combat corruption. In China, the Shenzhen Institute of Standards and Technology (SIST) has adopted ISO 37001 and intends to provide ISO 37001 certification and guidance. The SIST continues to work across China to generate support for adopting ISO 37001.[19]

The third meaning of ISO 37001 "adoption" in the public sector refers to when a federal, state, or local government itself strives for certification. Research indicates that the Quebec cities of Granby and Brossard will strive for ISO 37001 certification in 2018.

Early adopters: Private sector

Since the release of ISO 37001 in 2016, several organizations have achieved ISO 37001 certification. These organizations include Terna Group and ENI SpA (Italy), Robert Bosch Middle East (UAE), Alstom (France), CPA Global (Jersey, UK), and Ekvita (Azerbaijan). In addition, research suggests that, as of February 2018, about a dozen organizations have achieved certification in Malaysia. In the United States, several companies, such as Walmart and Microsoft, have publicly announced their intention to strive for certification once accredited CBs and registrars are established in the United States.

Benefits of ISO 37001 certification

Many benefits are associated with designing, implementing, and maintaining an anti-bribery and anti-corruption program in line with ISO 37001. Although some of these benefits relate to concepts like competitive advantage or board-level assurance, it is important to highlight the most important benefit: An effectively designed anti-bribery and anti-corruption program reduces the risk of bribery and corruption. This is good for business. It is good for employees, stakeholders, and communities. And it is good for the free markets. There are other benefits too.

First, ISO 37001 certification may help to assure the governing authorities and executive teams of organizations that sound, efficient, and effectively designed anti-bribery and anti-corruption controls and processes are in place and operating as intended. This helps the governing authorities of organizations satisfy their obligation to be knowledgeable about the content and operation of the compliance programs in place within their organizations.

Second, designing and implementing an anti-bribery and anti-corruption program in line with ISO 37001 will help to provide a defense, if there is ever a breach, regulatory inquiry, enforcement action, or investigation. ISO 37001 provides a comprehensive, end-to-end framework for managing the risk of bribery and corruption, and it also requires establishing and maintaining extensive documentation, both of which will help evidence a well-designed program.

Third, ISO 37001 is, at its core, a management system. Over time, management systems have helped organizations run smoothly, efficiently, and effectively. Such systems help organizations manage interrelated aspects of their operations in order to achieve their strategic objectives. ISO 37001 helps organizations organize, streamline, and optimize their anti-bribery and anti-corruption risk-management efforts — rather than attempting to manage the risk of bribery and corruption in a disintegrated, siloed, or fragmented manner.

Fourth, compliance is a journey in any organization. Even the most established organizations with mature and highly optimized compliance programs can benefit from incorporating additive aspects of ISO 37001 into their programs, thereby taking their programs to the next level. New, younger, or rapidly growing organizations can benefit from ISO 37001 too, because the program framework can help manage risk in a resourceful, effective manner. This can be valuable if or when the young organization strives to raise capital or undertake an initial public offering.

Fifth, it is no secret that more than 75% of enforcement actions related to bribery and corruption involve the misconduct of third parties.[20] Over the years, some US-based global organizations have struggled to develop and implement anti-bribery and anti-corruption programs and controls with regard to the third parties with which they do business, in part because such efforts are often seen as US-centric exercises and FCPA-focused. ISO 37001 establishes a common, global approach to managing bribery and corruption risk, regardless of where organizations are headquartered and where their third parties are conducting business.

Sixth, research suggests that, over time, organizations may begin to require ISO 37001 certification as a condition of doing business. Therefore, organizations, contractors, suppliers, and consultants that are not ISO 37001 certified will be at a competitive disadvantage. Similarly, the public sector may soon require organizations that bid on government contract work to be ISO 37001 certified. Uncertified organizations will be at a competitive disadvantage when it comes to government work.

ISO 37001 establishes a common, global approach to managing bribery and corruption risk, regardless of where organizations are headquartered.

Seventh, even when ISO 37001 is not a tender requirement, organizations that are ISO 37001 certified will be able to demonstrate to the procuring organization that they have designed an anti-bribery and anti-corruption compliance program in line with internationally recognized standards—and that they have had the program independently certified. This may help give the certified organization a competitive advantage over the uncertified organizations that are competing with it for business.

Lastly, organizations that achieve ISO 37001 certification will shine brightly in the ethics and compliance community and elsewhere. ISO 37001 certified organizations will be able to attract and retain top talent across the organization, especially the ethics and compliance function. Accomplished, dynamic, and forward-looking professionals are drawn to organizations that demonstrate a genuine commitment to organizational values, long-term sustainable growth strategies, and robust and meaningful risk-management practices.

Certification readiness

Striving for ISO 37001 certification—as with striving for any ISO certification—is a substantial undertaking. It involves a significant level of time, resources, and documentation. Some organizations move through the certification process efficiently and successfully, because they are prepared for the certification process. Other organizations experience challenges and findings of nonconformities, which will require remediation and perhaps a second or third attempt at certification.

Given the level of effort associated with striving for certification, some organizations elect to undertake an ISO 37001 readiness assessment exercise. This helps organizations evaluate the current state of their anti-bribery and anti-corruption program against the framework, expectations, and guidance set forth in ISO 37001. A readiness assessment helps organizations understand what they are doing well and where there may be opportunities for enhancement. Readiness assessments also help organizations pull together the documentation that will eventually be needed for the certification process.

Even organizations that do not aspire to ISO 37001 certification undertake a readiness assessment simply because it is a healthy and worthwhile exercise. They conduct readiness assessments because it establishes a baseline against which to enhance the program at a strategic and tactical level moving forward, and because it helps them satisfy the expectation that their programs be evaluated periodically, an expectation set forth in other guiding frameworks (e.g., U.S. Federal Sentencing Guidelines.).

Conclusion

ISO 37001 establishes a management system and compliance program framework for managing the risk of bribery and corruption in both the public and private sector. ISO issued this standard to help combat global corruption — a trillion-dollar problem. Although ISO developed the standard, it does not issue certifications. The ISO certification process is administered by CBs or registrars, which are sometimes accredited by higher organizations called regional accreditation agencies.

Although it is debatable whether ISO 37001 introduces anything fundamentally new, ISO 37001 — by its very existence — will help to bring greater consistency to the manner in which anti-bribery and anti-corruption compliance programs are designed, implemented, and audited around the world. ISO 37001 certification will also help organizations organize a defense if faced with a breach, inquiry, investigation, or enforcement action.

As of February 2018, several governments have adopted this new standard, and several organizations have become certified. Because more than 50 countries supported the development of ISO 37001, it is likely that additional countries will adopt the standard. It is also likely that other organizations will strive for ISO 37001 certification, once additional CBs and registrars become accredited.

While ISO 37001 continues to gain traction around the world, many organizations remain in a wait-and-see mode, while weighing the cost-benefit of striving for ISO 37001 certification. In the meantime, some organizations will elect to undertake an ISO 37001 readiness assessment, which will allow them to gain a deeper understanding of the current state of their anti-bribery and anti-corruption programs, if they eventually decide to go for certification — or even if they do not.

The opinions in this article are the author's and do not necessarily represent the position of any institution.

[1] ISO Quality Services Ltd. website available at http://bit.ly/2N1j7aO.

[2] Neill Stansbury: "International Anti-bribery Standard ISO 37001" Transparency International UK. November 2, 2016. Available at https://bit.ly/2JetvgW

[3] *Idem*.

[4] ISO 2600 — Social Responsibility; ISO 20121 — Event Sustainability Management Systems; ISO 3100 — Risk Management — A practical guide for SMEs.

[5] See ISO 37001 (2016). Available at http://bit.ly/2lwYS8d

[6] *Ibid* Ref #2

[7] Diana Trevley: "Certifying Your Anti-bribery Program with ISO 37001: What's In It For Me?" Society of Corporate Compliance and Ethics, January 23, 2017. Available at https://bit.ly/2xR23kf.

[8] ISO 37001, Introduction (2016)

[9] *Idem*

[10] Mike Koehler: "ISO 37001 Is a Complete Yawner" FCPA Professor; October 24, 2016. Available at https://bit.ly/2sJjUDG

[11] *United States Sentencing Commission, Guidelines Manual*, §(8)(B)(2)(1)(c); and ISO 37001 § 4.5.1 through ISO 37001 § 4.5.4

[12] Russ Berland and Michelle Shapiro: "International Standards Organization Issues Certification Standard for Anti-bribery Compliance Systems," Lexology; November 1, 2016. Available at https://bit.ly/2sL0BtT

[13] Cynthia D. Woodley: "Who Accredits the Accreditor?" *Professional Testing Blog*; April 20, 2017. Available at https://bit.ly/2JBGwk5

[14] Center for Responsible Enterprise and Trade: "ISO 37001: A Year in Review" November 15, 2017. Available at https://bit.ly/2M9mPOS

[15] Discussion with ISO representative on 28 September 2017

[16] Spark Consulting "ISO 37001: Your Questions Answered." Available at http://bit.ly/2lx6tUn

[17] *Ibid*, Ref #15

[18] *Idem*

[19] *Idem*

[20] OECD: Foreign Bribery Report: An Analysis of the Crime of Bribery and Foreign Public Officials. OECD Publishing, 2014. Available at http://bit.ly/2lj1bLS