COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2018
ISO 37001 Certification: Understanding and navigating the process

by Maurice L. Crescenzi, Jr.

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]

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.

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.

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.