Spark Compliance
CONSULTING

ISO 37001 ✓

ENSURE YOUR ORGANIZATION HAS
A WORLD-CLASS ANTI-BRIBERY PROGRAM -
BECOME ISO 37001 CERTIFIED

Frequently Asked Questions

www.SparkCompliance.com

What is ISO?

ISO is the International Organization for Standardization, a global non-governmental organization (NGO) comprised of national standards bodies from 163 countries. ISO was formed in 1946 at the suggestion of the United Nations to help reconcile differing standards and practices across ISO's member nations in order to facilitate commerce. To date ISO has published over 20,000 international standards, including over 50 management systems standards.

What is ISO 37001?

ISO 37001 - Anti-Bribery Management Systems (the "Standard") is the first certifiable international anti-bribery standard. The Standard was published on October 15, 2016 and was drafted over a three-year period with participation from anti-bribery experts from 56 countries and a number of liaison groups from various regions throughout the world. The Standard sets forth requirements and provides guidance for establishing, implementing, maintaining, reviewing and improving an organization's anti-bribery program – which ISO refers to as a "management system." These requirements consist of recognized best practices and, taken together, create a management system that provides organizations with a robust and comprehensive anti-bribery program.

What types of bribery does ISO 37001 address?

ISO 37001 is designed to combat many different types of bribery, including bribery as defined under the FCPA and UK Bribery Act.

The Standard applies to bribery in a broad context, including commercial bribery, bribery of public officials and government entities, passive (incoming) bribes, and bribes committed by business associates acting on an organization's behalf. In addition, under the Standard, an organization must take into account any applicable bribery laws, including local laws.

Is ISO 37001 designed for a particular type of organization or industry?

No - ISO 37001 was designed to be a broad standard applicable to public, private, non-profit organizations and to government entities and agencies.

The Standard requires that an organization conduct a bribery risk assessment that considers a variety of factors, including the organization's business model, size and structure, and business operations, in order to determine its unique bribery risks and the severity of those risks. Based on this comprehensive bribery risk assessment, an organization must implement policies, procedures, and controls that are reasonable and proportionate to the organization's bribery risks. A large organization operating in high risk countries in a high-risk sector will need to implement stronger controls and devote more resources to its anti-bribery program than a smaller organization operating in an industry with relatively low bribery risks. It is this reasonable and proportionate requirement, based on the risk assessment, that allows ISO 37001 effectively to be applied to different types of organizations in any industry.

What is ISO 37001?

ISO 37001 certification is a designation awarded to organizations that meet all the requirements of the Standard and choose to undergo a certification audit.

Certification audits are performed by independent certification bodies who use auditors who have experience in anti-corruption and anti-bribery and an in-depth knowledge of the requirements of the ISO 37001 standard. Following the certification audit, provided there are no major non-conformities, the certification body then awards the organization with ISO 37001 certification. A mark of this certification can be used on an organization's internal and external materials as desired in order to demonstrate the organization's commitment to fighting corruption.

Is my organization required to become ISO 37001 certified by any country or regulatory authority?

At present, no country or regulatory authority requires an organization to become ISO 37001 certified. However, some governments, including Mexico, are considering requiring organizations who wish to bid for government contracts to first be ISO 37001 certified.

What are the benefits of ISO 37001 certification?

Your organization will be implementing a certified global anti-bribery program, consisting of policies, procedures, and controls that are recognized by anti-bribery and anti-corruption experts as best practices. This will significantly reduce an organization's bribery risks. Having a certified program in place demonstrates to your organization's stakeholders, including shareholders, investors, personnel, business associates, customers, regulatory authorities and the public that your organization is committed to ethical business practices and fighting corruption. This commitment, in turn, can provide a significant competitive advantage in the global marketplace.

In the event that bribery does occur within your organization and there is a governmental investigation, having ISO 37001 certification can serve as evidence that your organization did its utmost to prevent such an event from occurring. The requirements in the Standard also ensure that your anti-bribery program is well documented – which is essential when trying to prove to government authorities that an organization was committing to ethical business conduct. ISO 37001 certification greatly reduces the risk of suffering the high costs, penalties, lost opportunities and reputational damage associated with bribery.

Furthermore, ISO 37001 certification imbeds transparency and ethical conduct in the procedures and policies of your organization and becomes part of the way your organization does business. With these procedures in place, your organization should experience increased efficiency, the assurance of better business relationships and a more ethical culture.

Do I need to create an anti–bribery program separate from the rest of my organization's compliance program to become ISO 37001 certified?

No. Your anti-bribery program can be part of your organization's compliance program or it can be a stand-alone program. The Standard also allows for outsourcing certain requirements, such as whistleblowing hotlines and due diligence.

What are the requirements for ISO 37001 certification?

ISO 37001 sets forth a number of requirements that relate to the following categories: context, leadership, planning, support, operations, performance evaluations, and improvement.

Below are the key requirements that must be implemented prior to obtaining ISO 37001 certification:

- Bribery risk assessment based on the organization's context and the needs and requirements of its stakeholders

- Anti-bribery objectives

- Anti-bribery policy

- Governing body and top management oversight, program review and commitment to combatting bribery

- Anti-bribery compliance function and other designated roles and responsibilities

- Proper planning

- Adequate resources

- Awareness and training

- Communications

- Operational procedures and controls including

  - Due diligence on personnel, projects, transactions and business associates posing more than a low risk of bribery

  - Financial and non-financial controls

  - Policies dealing with gifts, hospitality, donations and similar benefits

  - Reporting procedures, including a non-retaliation policy

  - Investigation procedures and disciplinary measures

- Continuous monitoring and periodic audits

- Corrective action and continuous efforts to improve the program

Your organization has likely already implemented many, if not all, of these key requirements. However, the Standard also requires more detailed processes and controls related to these key requirements, as well as approporiate documentation that the requirements are in place and being carried out as planned.

For example, the governing body and top managment are required regularly to review the program and to provide feedback regarding any changes to the program.

Does ISO 37001 certification mean that my organization is fully protected from bribery, government investigation, or prosecution?

There is no silver bullet that will eradicate the risk of bribery occurring or, in the event that it does occur, that there will be no government investigation or prosecution. However, ISO 37001 consists of well-established best practices embedded into a comprehensive management system and provides the best defense against incidents of bribery occurring in your organization.

Having an effective compliance and ethics program is a strong mitigating factor when facing penalties or prosecution by the U.S. Department of Justice, the Securities and Exchange Commission, and the U.K. Serious Fraud Office, as well as other international regulatory and prosecutorial bodies. The Standard meets the requirements for an effective anti-bribery program as set forth in the Federal Sentencing Guidelines, as well as meeting guidelines published by the DOJ and the SEC, and certification can assist an organization's efforts to demonstrate its commitment to fighting bribery and corruption.

How long will it take my organization to be ready to become ISO 37001 certified?

The time it takes an organization to prepare for and complete the ISO 37001 audit depends on the size and scope of an organization, the nature of its bribery risks and its current anti-bribery processes and controls already in place. Some organizations may be ready to schedule their ISO 37001 certification audit after less than a month of preparation, while other organizations may spend a year bringing their anti-bribery program into line with the Standard's requirements.

The best way to determine how long it will take for your organization to become ISO 37001 certified is have a gap analysis conducted on your anti-bribery program, by an experienced outside analyst. The results of the gap analysis will indicate which requirements your organization does and does not meet, as well as which requirements are partially met, and will give the best indication of timescale.

Once my organization is ready to become ISO 37001 certified, how does the certification process work?

Once an organization has all the requirements of ISO 37001 in place, an independent certification body will conduct a certification audit. An organization should only work with a certification body that has experience with anti-bribery and anti-corruption. Certification bodies should follow the standards established in ISO/IEC 17021-1 and ISO/IEC 17021-9 to ensure that audits are fair and unbiased and that the auditors have sufficient anti-bribery experience to carry out a thorough and fair review.

The first step of the audit consists of a review of an organization's documentation of its anti-bribery program. The second step is an on-site audit to an organization's headquarters. Depending on a company's structure and operations audits may be performed on a selection of the organization's other offices and/or subsidiaries. During the on-site audits, the auditor will speak with the organization's compliance personnel, top management, and other personnel in support roles and operations as needed to determine whether the requirements of the Standard are met.

How much does the ISO 37001 certification audit cost?

The cost of an ISO 37001 certification audit varies depending on the size of the organization and the number of its subsidiaries. Spark Compliance estimates that an audit may cost an organization between $15,000 to $100,000. Spark Compliance can obtain a more precise cost estimate for your organization from an independent certification body.

My organization already has a great anti-bribery program – can we schedule the certification audit right away?

Spark Compliance recommends that every organization first conduct expert-led external gap analysis to determine those gaps which exist its current anti-bribery program compared to the program elements required by the ISO37001 standard. Most organizations will find there are some gaps that must be addressed prior to scheduling the certification audit. Spark Compliance can assist your organization in conducting an analysis to determine where those gaps exist.

## How can Spark Compliance help my organization become ISO 37001 certified?

Spark Compliance provides organizations with bespoke ISO 37001 preparation and certification consulting services. Below is an overview of the services Spark provides to organizations considering or seeking ISO 37001 certification.

- **Gap Analysis.** An essential step prior to pursuing ISO 37001 certification, Spark Compliance will conduct a gap analysis of your current anti-bribery program against the requirements of ISO 37001 to determine where your organization meets the requirements and where it falls short.

- **Remediation & Optimization Plan.** Based on the results of the Gap Analysis, Spark Compliance will prepare a detailed Remediation & Optimization Plan that sets forth the projects and tasks necessary to remediate the gaps in your current anti-bribery program and bring it into line with ISO 37001 requirements.

- **Remediation & Optimization.** Spark Compliance will help you efficiently and effectively remediate the gaps in your current anti-bribery program prior to the ISO 37001 audit.

Our services are tailored to your organization's unique risk profile, operations, resources and objectives and include bribery risk assessments, reviewing and creating written policies and procedures, and conducting leadership training. We can conduct compliance function and company-wide training on anti-bribery and ISO 37001 requirements, creating and helping to implement communication, investigation, monitoring and audit plans, establishing effective and efficient financial and non-financial controls, establishing clear procedures related to reporting, due diligence, investigations and corrective action, working with outside vendors such as due diligence firms and whistleblower hotlines, and assisting with corrective action and program improvements.

- **Audit Preparation.** In preparation for the ISO 37001 audit Spark Compliance will ensure that all documents meet the requirements of the standard. We will also prepare management, and other relevant personnel, for their audit interviews, Spark Compliance will then conduct a mock audit, and, if necessary, help to correct any major non-conformities within the 90-day window following the audit.

- **Continuous Improvement.** Following your ISO 37001 certification, Spark Compliance will ensure that your organization maintains the Standard's requirements, including the requirement of continuous improvement, and will ensure that your organization is ready for its annual surveillance audit.

- **Training Seminars.** If you want to learn more about ISO 37001, and ask in-depth questions of an expert on how the Standard can be applied to your organization, Spark Compliance offers in-person and online training seminars.

SPARK'S ISO 37001 CERTIFICATION PROCESS
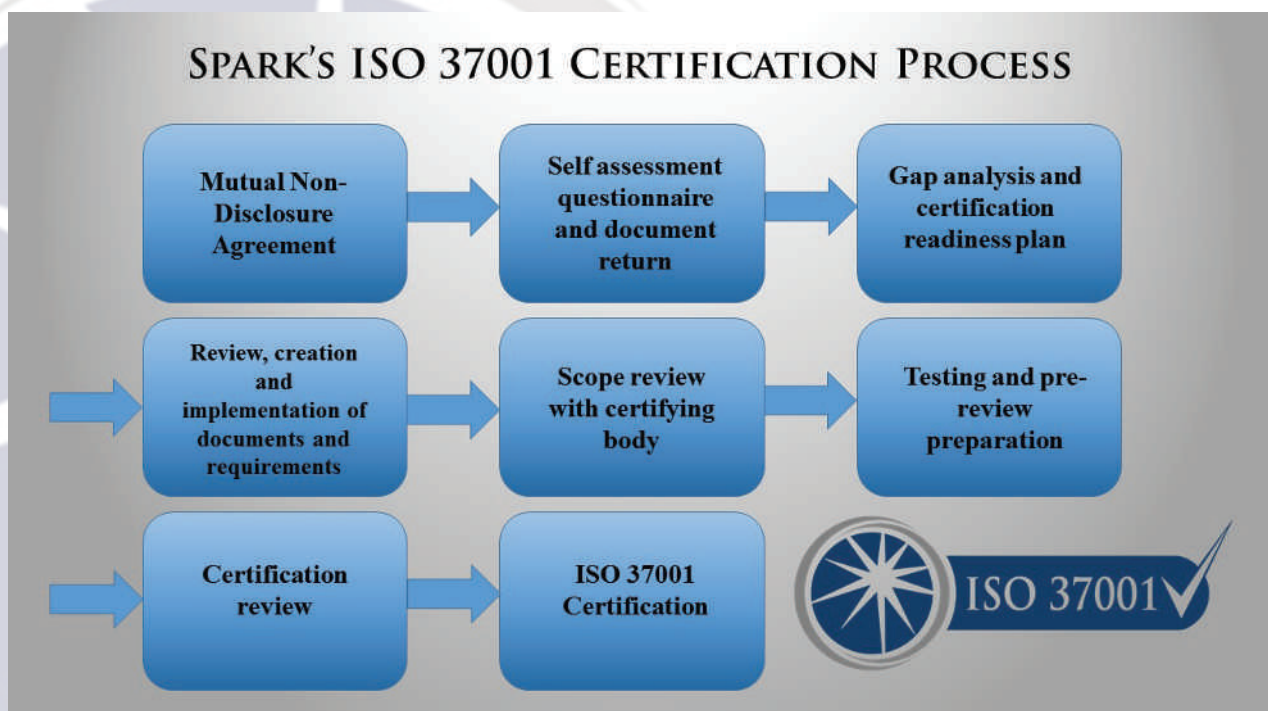
How Do I Get Started?

Email: info@SparkCompliance.com

Phone: +44 (0)203 514 1443   (United Kingdom)

                    +1 310-299-0955   (United States)

London: Los Angeles:

71-75 Shelton Street,   2355 Westwood Boulevard,

Covent Garden,   Suite 429,

London   Los Angeles

WC2H 9JQ   CA 90064