FAQ on ISO 37001:2016

Version – December 2017

This document is designed to provide additional insight to users of ISO 37001:2016.

The terms "HLS" and "Annex SL" refer to the high level structure, identical core text, common terms and core definitions for use in management system standards (MSS) set out in Annex SL to the ISO Directives Part 1 2016 (7th edition).

ISO – GENERAL

1. Who is ISO and what is a Standard?
   ISO is an independent, non-governmental international organization based in Geneva, Switzerland with a membership of 163 national standard bodies. It has developed and published over 20,000 international standards of which the most well-known are ISO 3166 – Country Codes, ISO-4217 – Currency Codes and, in the field of management systems, ISO 9001 – Quality Management.

   www.iso.org/about-us.html        www.iso.org/standards.html

2. What is a Management System?
   A management system is the way in which an organization manages the inter-related parts of its business in order to achieve its objectives. These objectives can relate to a number of different topics, including product or service quality, operational efficiency, environmental performance, health and safety in the workplace and many more.

   www.iso.org/management-system-standards.html

3. How are standards developed?
   For information on how Standards are developed, please see: www.iso.org/developing-standards.html

4. Where can I obtain copies of standards?
   Standards can be purchased on-line from the ISO store: www.iso.org/store.html.
   Standards may also be purchased from national ISO member body. For a list of ISO members, see: www.iso.org/members.html.

5. What is “certification”?
   Certification is the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.
   Certification can be a useful tool to add credibility, by demonstrating that your product or service meets the expectations of your customers and other stakeholders. For some industries, certification is a legal or contractual requirement.

   www.iso.org/certification.html
6. **Does ISO certify organizations to its Standards?**

ISO develops international standards, but does not perform certification and does not issue certifications. This is performed by certification bodies external to ISO, thus an organization cannot be certified by ISO. However, ISO’s Committee on Conformity Assessment (CASCO) has produced a number of standards related to the certification process, which are used by certification bodies.

www.iso.org/certification.html
www.iso.org/committee/54998/x/catalogue/p/1/u/0/w/0/d/0

---

**ISO 37001 – GENERAL**

7. **What is ISO 37001?**

ISO 37001 Anti-Bribery Management Systems – Requirements with Guidance for Use was designed to help an organization establish, implement, maintain and improve an anti-bribery compliance program. It includes a series of measures and controls that represent global anti-bribery good practice.

www.iso.org/iso-37001-anti-bribery-management.html

8. **Why was ISO 37001 proposed and developed?**

Bribery is one of the world’s most destructive and challenging issues. With over US$ 1 trillion paid in bribes each year*, the consequences are catastrophic, reducing quality of life, undermining the rule of law and government, increasing poverty and eroding public trust. For companies, bribery can destroy value and cause harm to individuals and external stakeholders. *source: OCDE/OECD

Yet despite efforts on national and international levels to tackle bribery, it remains a significant issue. Recognizing this, ISO has developed a new standard to help organizations fight bribery and promote an ethical business and organizational culture.

www.iso.org/iso-37001-anti-bribery-management.html

9. **Are there other ISO standards related to ISO 37001?**

Yes. Some of the Standards related to ISO 37001 include:

- ISO 19600 Compliance management systems-Guidelines
- **ISO 26000 Guidance on Social Responsibility**
- ISO 31000 Risk Management - Principles and Guidelines

Unlike these Standards which state principles that can be used freely as guidance, ISO 37001 establishes requirements for compliance with the Standard, which enables an organization to pursue certification, if desired.

10. **Is compliance with ISO 37001 mandatory?**

Generally, no. It is a voluntary standard that an organization can adopt, if desired. However, it is possible for compliance with the Standard to become a legal or contractual requirement for certain organizations or industries. Examples might include public procurement and supply chains.
11. **What types of bribery does the Standard address?**

   For the purpose of the Standard bribery is defined as the offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person’s duties.

   This definition is broadly in line with the definition of bribery used in international instruments and is further informed by a reference to the law specifically applicable to the organization; it includes the bribery of officials in both the public and the private sectors.

   The Standard further includes bribery by the organization (active bribery) or of the organization (passive bribery). It extends to bribery by its personnel or business associates acting on the organization’s behalf or for its benefit as well as to bribery of its personnel or of its business associates in relation to the organization’s activities.

   The Standard specifically does not address fraud, cartels, anti-trust/competition offences, money-laundering or other activities related to corrupt practices (such as those covered by the United Nations Convention Against Corruption) although an organization may choose to extend the scope of its management systems to such activities.

   [www.iso.org/standard/65034.html](http://www.iso.org/standard/65034.html)

12. **What is the difference between bribery and corruption?**

   Corruption is a wider concept than bribery. In addition to bribery in the public and the private sectors, the United Nations Convention Against Corruption thus includes other offenses such as embezzlement, misappropriation or other diversion of property by a public official, trading in influence, abuse of functions, illicit enrichment, embezzlement of property in the private sector, laundering of the proceeds of crime, concealment and obstruction of justice.

13. **Does ISO 37001 define “bribery”?**

   “Bribery” is specifically defined by the various laws and regulations that are applicable to an organization. ISO 37001 generally defines bribery as: offering, promising, giving, accepting or soliciting of an undue advantage of any value, directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person’s duties.

14. **Who can use ISO 37001?**

   ISO 37001 is flexible and can be adapted to a wide range of organizations, irrespective of size, sector, structure, geography, or jurisdiction. It is applicable to small, medium, and large organizations, as well as parts of an organization. In the private sector, ISO 37001 can be used by business enterprises as well as not-for-profit and non-governmental organizations. ISO 37001 can also be used in the public sector.

15. **What does the Standard require?**

   To comply with the Standard, the organization must implement a series of measures and controls in a reasonable and proportionate manner to help prevent, detect, and deal with bribery, including:

   - An anti-bribery policy that prohibits bribery
   - The expression of leadership commitment and responsibility
   - Communication of the policy directly to both personnel and business associates
   - Appointment of a person or function to oversee the program
- Personnel controls and training
- Regular assessments of the bribery risk to which the organization is exposed
- Due diligence on projects and business associates
- Implementation of anti-bribery controls by controlled organizations and by business associations
- Implementation of appropriate financial and non-financial controls to prevent the bribery risk
- Reporting, monitoring, investigating, and auditing
- Corrective action and continual improvement

16. Does the Standard require a stand-alone management system?

The Standard provides minimum requirements and supporting guidance for implementing or benchmarking an anti-bribery management system. It is a risk management tool and brings assurance to management, investors, employees, customers and other stakeholders that an organization is taking reasonable steps to prevent, detect, and appropriately manage bribery risk.

In the event of an investigation, the Standard may also be taken into account as evidence that an organization has taken reasonable, proactive steps to prevent bribery.

Implementation of the Standard can also provide an organization with a competitive advantage and increased stakeholder, shareholder, and customer trust.

17. How will the Standard benefit an organization?

The Standard provides minimum requirements and supporting guidance for implementing or benchmarking an anti-bribery management system. It is a risk management tool and brings assurance to management, investors, employees, customers and other stakeholders that an organization is taking reasonable steps to prevent, detect, and appropriately manage bribery risk.

In the event of an investigation, the Standard may also be taken into account as evidence that an organization has taken reasonable, proactive steps to prevent bribery.

Implementation of the Standard can also provide an organization with a competitive advantage and increased stakeholder, shareholder, and customer trust.

18. Does use of the Standard protect an organization against prosecution in case of bribery by its personnel or its business associates?

Use of the Standard, with or without third party certification, does not offer an absolute protection against the prosecution of the organization for bribery occurring in its sphere of activity. It may, however, serve as evidence that the organization has put adequate measures in place to prevent bribery, which may reduce or even exclude its liability. This evidence may be reinforced by third party certification.

19. Does implementation of and conformity with ISO 37001 guarantee that bribery will not occur?

No. ISO 37001 cannot provide assurance that bribery has not or will not occur in an organization. It can help the organization to prevent, detect and respond to bribery risk, and strengthen the anti-bribery culture.
ISO 37001 – GENERAL

20. How is the Standard used?
Organizations may decide to use the Standard in a number of ways. For example:
- Guidance material to provide to potential or current stakeholders to assist in development of their anti-bribery management system or set expectations
- A benchmark to evaluate the:
  - Organization’s existing anti-bribery management system
  - Anti-bribery system of an organization already within an existing value chain
  - Anti-bribery system of a new organization being considered for entry into an existing value chain
- A blueprint to design a new anti-bribery system or improve an existing one
- A program to reference when reviewing, monitoring, or auditing a business associate
- A basis for certification to the ISO 37001 Standard
- A competitive advantage, once implemented, to differentiate an organization from its competitors
- A requirement as a condition to start or continue business with an organization

21. Does the Standard have to cover an entire organization?
No. The Standard may be used by an entire organization, such as e.g. a group of companies, but may also be used for parts of an organization, e.g., for only certain activities of an organization or for only one or more companies of a group of companies.

22. Who in the organization is involved in ISO 37001 planning, implementation, management, and maintenance?
Everyone in the organization has roles and responsibilities related to the design, planning, implementation, management, and ongoing maintenance of an ISO 37001 Anti-Bribery Management System. For example, leadership is responsible for supporting the program by prohibiting bribery and ensuring sufficient resources are allocated to implement the programme. Management is responsible for implementing and managing the programme. All employees are responsible for knowing, and complying with, the anti-bribery policy, completing training, and reporting actual or potential cases of non-compliance.

23. How long will it take to implement the Standard?
The time needed to implement the Standard can vary greatly from one organization to another, depending on factors like size, structure, geographical spread, complexity, resources, subject matter expertise, etc. For a large organization, it is reasonable to allow for one year or two, while a small organization may put all requirements in place in a matter of months.

Complying with the Standard is an on-going process, not a one-time event.

ISO 37001 – CERTIFICATION

24. Can an organization be certified to ISO 37001?
Yes. ISO 37001 is a requirements standard, making it capable of independent certification. An organization may invite an independent certification body to verify that it is in conformity to the standard.
25. **If an organization implements ISO 37001, is certification mandatory?**
   Generally, no. Like the decision to implement the Standard, pursuit of certification is a decision made by the organization. However, for some industries, or in procurement, certification may be a legal or contractual requirement.

26. **Does an organization need to create a new, separate anti-bribery program to get ISO 37001 certified?**
   No. The measures required by ISO 37001 are designed to be integrated with existing management processes and controls. ISO 37001 follows the common high-level structure for ISO management system standards, for easy integration with, for example, ISO 9001 – Quality Management or ISO 19600 – Compliance Management Systems. New or enhanced measures can be integrated into existing systems.

27. **What requirements do certifying bodies need to adhere to when providing audit and certification of management systems for an organization?**
   While ISO does not conduct any certification itself, it has issued together with the International Electrotechnical Commission certain requirements for bodies providing audit and certification of management systems (ISO/IEC 17021). [www.iso.org/standard/61651.html](http://www.iso.org/standard/61651.html)

   Because of the specificity of anti-bribery management systems, specific additional competence requirements have been issued for auditing and certification of anti-bribery management systems (Technical Specification ISO/IEC TS 17021-9). [www.iso.org/standard/70158.html](http://www.iso.org/standard/70158.html)

28. **What should an organization consider when selecting a certification body?**
   When choosing a certification body, you should:
   - Evaluate several certification bodies.
   - Check if the certification body uses the relevant CASCO standard
   - Check if it is accredited. Accreditation is not compulsory, and non-accreditation does not necessarily mean it is not reputable, but it does provide independent confirmation of competence. To find an accredited certification body, contact the national accreditation body in your country or visit the International Accreditation Forum.

   [www.iso.org/certification.html](http://www.iso.org/certification.html)