International Organization for Standardization
BIBC II, Chemin de Blandonnet 8 , CP 401, 1214 Vernier, Geneva, Switzerland
Tel: +41 22 749 01 11, Web: www.iso.org

ISO 37301:2021 Compliance management systems — Requirements with guidance for use

Frequently Asked Questions (FAQs)

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.

More information about ISO and its standards.

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.

3. *How are standards developed?*

For information on how Standards are developed, please see.

4. *Where can I obtain copies of standards?*

Standards can be purchased on-line from the ISO store.

Standards may also be purchased from national ISO member body.

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.

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.

ISO 37301 GENERAL

7. *What is ISO 37301?*

ISO 37301 published on 13 April 2021, specifies requirements and provides guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization. It represents global compliance good practice.

ISO 37301 is a requirement Standard which was developed by ISO Technical Committee 309 Governance of Organizations.

8. *Why was ISO 37002 proposed and developed?*

Following the systematic review of ISO 19600:2014 Compliance management systems - Guidelines, TC309 requested a task group to examine the options for a revision and in September 2018, it was agreed to revise ISO 19600 as a new requirements standard-ISO 37301. The work was assigned to ISO/TC 309 Working Group 4 (WG4). ISO 37301 has been developed to assist organizations to promote an ethical business and positive culture of compliance.

9. *Are there other ISO standards related to ISO 37301?*

Yes. Some of the Standards related to ISO 37301 include:

- ISO 9001 Quality management system – Requirements
- ISO 14001 Environment management system – Requirements with Guidance for Use
- ISO 37001 Anti-bribery management systems – Requirements with Guidance for Use
- ISO 26000 Guidance on Social Responsibility
- ISO 31000 Risk Management - Principles and Guidelines
- ISO 37002 Whistleblowing management systems — Guidelines

10. *Is compliance with ISO 37301 mandatory?*

Generally, no. It is a voluntary standard that an organization can adopt, if desired. However, it is possible for compliance with ISO 37301 to become a legal or contractual requirement for certain organizations or industries. Examples might include public procurement and supply chains.

11. *Who can use ISO 37301?*

ISO 37301 is flexible and can be adapted to a wide range of organizations, irrespective of size, sector, nature and industry, 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 37301 can be used by business enterprises as well as not-for-profit and non-governmental organizations. ISO 37301 can also be used in the public sector.

12. *What does ISO 37301 require?*

To comply with ISO 37301, the organization must implement a series of measures and controls in a reasonable and proportionate manner to establish, implement, maintain and improve a compliance management system including:

- Identify compliance obligations related to the organization's products, services, or activities, and evaluate compliance risks
- Determine the boundaries and scope of the compliance management system
- The expression of leadership commitment and responsibility
- Communication of the policy directly to both personnel and business associates
- Establish appropriate compliance objectives, responsibilities and authorities at each function and level, and plan the process that needs to be established to achieve compliance objectives
- Personnel trainings and communications
- Regular assessments of the compliance risk to which the organization is exposed
- Reporting, monitoring, investigating, and auditing
- Measuring, analysing and evaluating the performance and effectiveness of the compliance management system
- Corrective actions, continuously management review and improvement

13. *How will the Standard benefit an organization?*

ISO 37301 provides minimum requirements and supporting guidance for establishing, implementing or benchmarking a compliance management system. It brings assurance to management, investors, employees, customers and other stakeholders that an organization is taking reasonable steps to prevent, detect, and appropriately manage compliance risk.

In the event of an investigation, ISO 37301 may also be taken into account as evidence that an organization has taken reasonable, proactive steps to prevent violation of compliance obligations.

Implementation of ISO 37301 can also provide an organization with a competitive advantage and increased stakeholder, shareholder, and customer trust.

14. *Does use of ISO 37301 protect an organization against prosecution in case of violations of compliance obligations by its personnel or its business associates?*

Use of ISO 37301, with or without third party certification, does not offer an absolute protection against the prosecution of the organization for violation of compliance obligations occurring in its sphere of activity. It may, however, serve as evidence that the organization has taken adequate measures in place to prevent violations of compliance obligations, which may reduce or even exclude its liability. This evidence may be reinforced by third party certification.

15. *Does implementation of and conformity with ISO 37301 guarantee that non-compliance/violations of compliance obligations will not occur?*

No. ISO 37301 cannot provide assurance that non-compliance/violation of compliance obligations has not or will not occur in an organization. It can help the organization to prevent, detect and respond to compliance risk, and strengthen the compliance culture.

16. *How is the Standard used?*

Organizations may decide to use the Standard in a number of ways. For example:

- As guidance material, provide to potential or current stakeholders to assist in development of their compliance management system or set expectations
- As a benchmark to evaluate the:
- Organization's existing compliance management system
- Compliance management system of an organization already within an existing value chain
- Compliance management system of a new organization being considered for entry into an existing value chain
- As a blueprint to establish a new compliance management system
- As a program to reference when reviewing, monitoring, or auditing a business associate
- As a basis for certification to the ISO 37301and self-declaration
- As a competitive advantage, once implemented, to differentiate an organization from its competitors
- As a precondition to start or continue business with an organization
- As a systematic approach for organisations to improve their own compliance management capabilities
- As a reference for regulatory bodies and the judicial agencies to adopt the organisation's compliance management system practices when determining sentencing
- As common rules to facilitate trade, communication and cooperation between interested parties on a global scale

17. *Does ISO 37301 have to cover an entire organization?*

No. ISO 37301 may be used by an entire organization, such as 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.

18. *Can an organization be certified to ISO 37301?*

Yes. ISO 37301 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 ISO 37301.

19. *If an organization implements ISO 37301, is certification mandatory?*

Generally, no. Like the decision to implement ISO 37301, 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.

20. *Does an organization need to create a new, separate compliance management program to get ISO 37301 certified?*

No. The measures required by ISO 37301 are designed to be integrated with existing management processes and controls. ISO 37301 follows the common high-level structure for ISO management system standards, for easy integration with, for example, IS0 9001 – Quality Management or ISO 31000 – Risk Management Systems. New or enhanced measures can be integrated into existing systems.

21. *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).

Because of the specificity of compliance management systems, specific additional competence requirements have been issued for auditing and certification of compliance management systems (ISO/IEC TS 17021-13).

22. *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.