Compliance standardized

Forensic & Integrity Services
ISO 37301: compliance management

EY
Building a better working world

Today, most companies are operating on the edge of technological innovation, potentially far from the knowledge and understanding of regulators' intentions, and they could find themselves in a regulatory "no-man's-land." In many cases, the current set of laws and regulations are not – or only partly – applicable to new business models. In the absence of certainty, it is up to the company to weigh ethical decisions and blaze the trail itself.

Long-lasting economic success is strongly correlated with a culture of integrity and compliance. The first step – design and implement a systematic compliance program – is a hurdle many organizations have already taken. However, implementing a management system by continuously learning from past experiences and leading practices remains a challenge to be addressed for many organizations.

The journey from a compliance program to a compliance management system is important but may be daunting if there is not a widely accepted reference. That's why the International Organization for Standardization (ISO) published a new certifiable standard for compliance management systems in April 2021.

Compliance management sounds simple – it's following laws and regulation. However, it can sometimes be challenging to have an organization move in an ethical direction. The avoidance of compliance and the committed misconduct of employees, business partners and corporate management is and will remain a central challenge of modern business management. Moreover, there is the tightening of national and international legislation and regulation, particularly in the areas of anti-corruption, cartels and competition, but also in the area of cybercrime or data protection. In all important markets, authorities intensify the enforcement of regulations and focus more on the personal responsibility of the management. Thus, knowing their risks and defining clear responsibilities to manage is crucial for organizations.

Why standardization of compliance matters

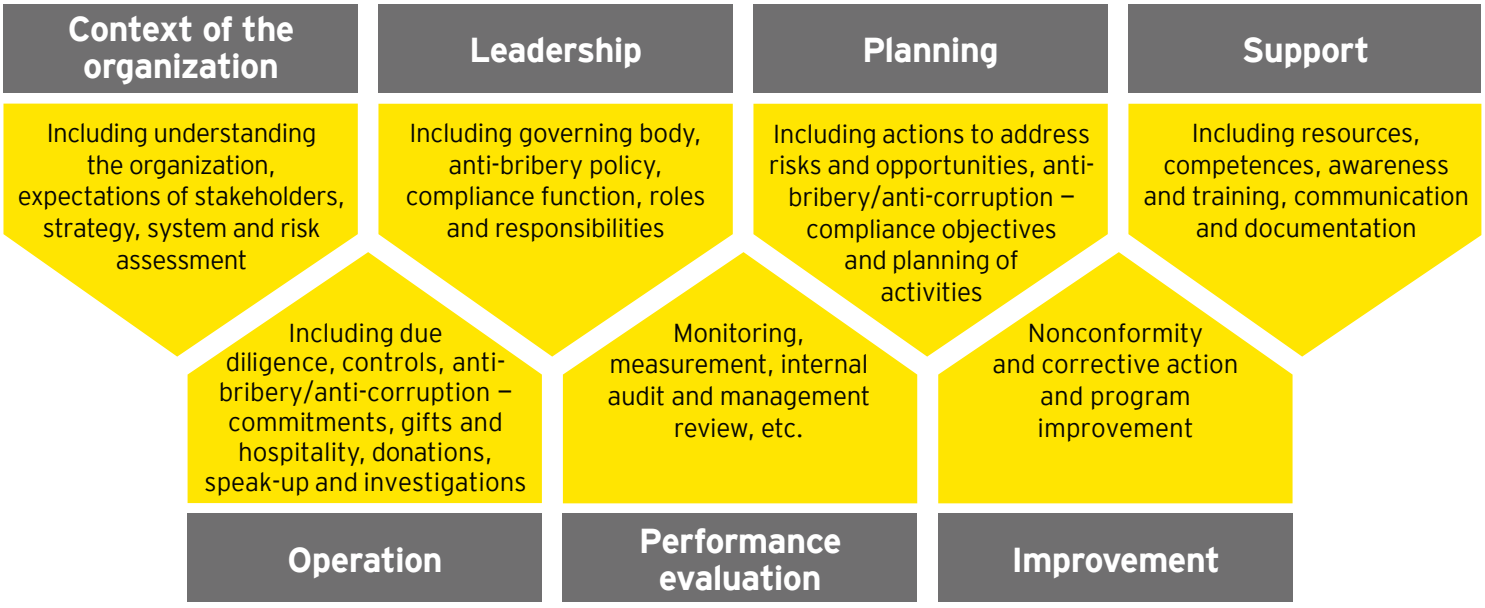
In a world that grows more connected every day, and with trade flows stretching far beyond the borders of an organization's headquarters, the world of compliance becomes increasingly complex. Regulators and supervisors are holding organizations responsible not only for the actions of their own employees but also for the actions of agents and suppliers. Just contractually obliging subsidiaries, agents or suppliers to have a compliance program might not be enough to reduce the risk of noncompliance. This is where ISO 37301 comes in.

ISO 37301 was designed by a committee of professionals and experts from many different countries and has the support of the majority of ISO member nations. It provides trust that risks are regularly assessed, business partners are screened (based on a risk-based approach), the organization has a working system to raise concerns and, in case of nonconformities, the organization is improving its systems.

The standard outlines significant and mandatory components of corporate compliance programs while offering a high level of flexibility to design, implement and operate an organization-centric, specific compliance program that is fulfilling the needs of the individual corporation.

The key elements of an ISO 37301 compliance management system

The standard is based on well-established and globally recognized principles of good governance, proportionality, transparency and sustainability. It can be drilled down to the following building blocks:



Four reasons to consider ISO 37301 for an organization:

1. ISO 37301 provides an organization with a practical structure for a dynamic compliance program

ISO 37301 changes often static compliance programs to dynamic compliance management systems. The standard follows practical basic principles that can be adjusted to accommodate factors like size, geography or industry. Once an organization is certified, a "surveillance audit" will be done annually (recertification is required after the third year) by an independent third-party auditor, which means that an extra set of eyes will critically look at the compliance system and further stimulate an organization's learning process.

2. ISO 37301 provides an organization with a powerful defense

In case of an investigation, an ISO 37301 management system not only shows that a compliance program is in place, but also equips organizations with documented evidence to substantiate the program's viability and provide a reliable audit trail. Regulators and supervisors, such as the U.S. Department of Justice,[1] are taking these into account when determining the fines that need to be paid in instances of noncompliance. Also, the upcoming German corporate criminal law points in this direction.

3. ISO 37301 can help protect an organization against third-party risks

According to the EY Global Integrity Report 2020, only one-third of organizations are very confident that their third parties demonstrate integrity in the work they do.[2] This opens the possibility for third-party risks that may result in penalties or fines for an organization. Over the years, several organizations have faced enforcement due to actions of third parties. Working with organizations that are ISO 37301-certified shows that their compliance programs correspond with the international standard and are audited by an independent third party on a yearly basis.

4. ISO 37301 contributes to an organization's ethical reputation

Becoming certified for ISO 37301 is a way tfor an organization to show that its compliance efforts are ahead of the curve and a good way to gain competitive advantage over peers in tenders and high-value contracts. Government institutions increasingly demand that parties have a compliance management system in place to qualify (and explicitly refer to ISO standards as a leading standard).

---

[1] "Evaluation of Corporate Compliance Programs (Updated June 2020)," U.S. Department of Justice Criminal Division, https://www.justice.gov/criminal-fraud/page/file/937501/download, accessed 28 June 2021.

[2] Global Integrity Report 2020, EYGM Limited, 2020, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-is-this-the-moment-of-truth-for-corporate-integrity.pdf, accessed 28 June 2021.

A standard that can be tailored to organizations of any shape or form

Every organization needs to comply with laws and regulations. However, smaller companies might be demotivated by the notion of building a compliance management system that is similar to the ones large multinationals use. Therefore, ISO 37301 is designed to be applicable to all organizations, regardless of type, size or nature of activity and whether in the public, private or not-for-profit sectors.

Based on the size or nature of the organization, some risks can be lower or higher. Organizations can decide to focus on certain risk categories and accept the risks involved with the others. Also, the compliance function under ISO 37301 needs to be adequate relative to the size of the operations. It is possible to have only a fraction of a full-time employee's time or outsource the operation (rather than accountability) of the compliance function entirely. This frees organizations from the burden associated with compliance, given that their management system is operational and effective.

Better prepare than repair

ISO 37301 has the potential to become the single international standard for compliance management systems. The core elements are not new, but brought together in this standard, they form a solid base for organizations of any size and from any sector or country to lift their compliance efforts to the next level. For organizations that intend to be proactive and mitigate compliance risks, ISO 37301 gap analysis, based on the draft version, can help evaluate areas of improvement of compliance efforts.

Global experience, local knowledge and relevant skills

The EY Forensic & Integrity Services Team has the global reach to assist companies in developing a strategic corporate compliance program. Our Integrity, Compliance and Ethics Services (ICE) Team is well positioned as an independent, objective advisor. The ICE Team has deep risk management experience and global resources familiar with major compliance risks to help companies effectively manage their corporate compliance obligations. Developing and embedding a prevention program and a culture of ethics, values and integrity in line with ISO 37301 will help organizations sustain global compliance.

We can help organizations build better processes on issues of critical corporate and personal importance.

Our teams provide the following support:

Gap analysis

- Identify and prioritize the company's significant integrity and compliance risks
- Assess the design of the company's compliance infrastructure, including the compliance function, people, processes and entity-level controls
- Compare compliance risks and infrastructure with the requirements of ISO 37301 to identify improvement opportunities

Implementation of compliance management systems

- Assist in developing and implementing policies and procedures based on ISO 37301 requirements
- Conduct training and communication and provide implementation support
- Help with performance evaluation and improvement
- Prepare for ISO certification

EY contacts

Global and Area
subject-matter resources

Brenton
Steenkamp
brenton.steenkamp@nl.ey.com

Andreas
Pyrcek
andreas.pyrcek@de.ey.com

Vinay
Garodiya
vinay.garodiya@in.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 008737-21Gbl
2106-3803843
ED None

ey.com