Nimonik

Why ISO 37301 is the key to Ethical Business Practices

A step-by-step guide to implement the new ISO compliance standard.

Executive Overview

In today's business landscape, organizations face an increased need to comply with global standards of ethical conduct and legal compliance. And in an increasingly connected world, with trade flows stretching far beyond the borders of an organization's headquarters, compliance becomes increasingly complex. As organizations adapt to new realities in an ongoing pandemic, the need for a uniform standard of compliance has become even more apparent.

According to Nancy Hayt, Vice-President of Corporate Responsibility at AdventHealth, *"Today, we must be able to continually update our programs and risk assessments to adapt as the risk landscape shifts,"* additionally, she said, *"A stagnant, siloed program that's isolated from the business is not conducive to effective compliance."* [1]

Modern organizations that aim to establish themselves as responsible and ethical entities must implement a robust Compliance Management System (CMS). While some organizations already align with ISO 19600:2014 and understand how a robust CMS helps build sustainable businesses, others must evolve to meet new demands and challenges. This is why the International Organization of Standardization (ISO) created ISO 37301:2021 – a comprehensive framework for modern compliance management.

A key emphasis of the new standard has been to elevate the role of culture in the compliance process, calling on organizations to measure and manage their culture of compliance actively.

This paper discusses how organizations benefit from transitioning to the new standard. It will also provide practical insights into how organizations can implement the new standard effectively and the critical success factors

This paper discusses how organizations benefit from transitioning to the new standard. Furthermore, it will provide practical insight and critical success factors to help organizations implement the new standard successfully. The results? An improved compliance management process with greater clarity, consistency, and transparency.

In the following pages, we look closer at creating a culture of compliance, the key differences between ISO 19600 and ISO 37301, and the benefits of transitioning to the new standard.

Navigating the new risk and compliance landscape

COVID-19 has transformed the workplace environment for millions of people globally. And with hybrid and remote work policies becoming more prevalent, maintaining an organization's cultural norms can be challenging. Organizations struggle to keep up with the increased complexities and volume of laws and regulations worldwide.

Moreover, businesses must rapidly adapt to changing legislation, regulations, and standards. And with the ever-evolving nature of global business, it can be difficult for organizations to keep up with compliance requirements and maintain the highest ethical standards.

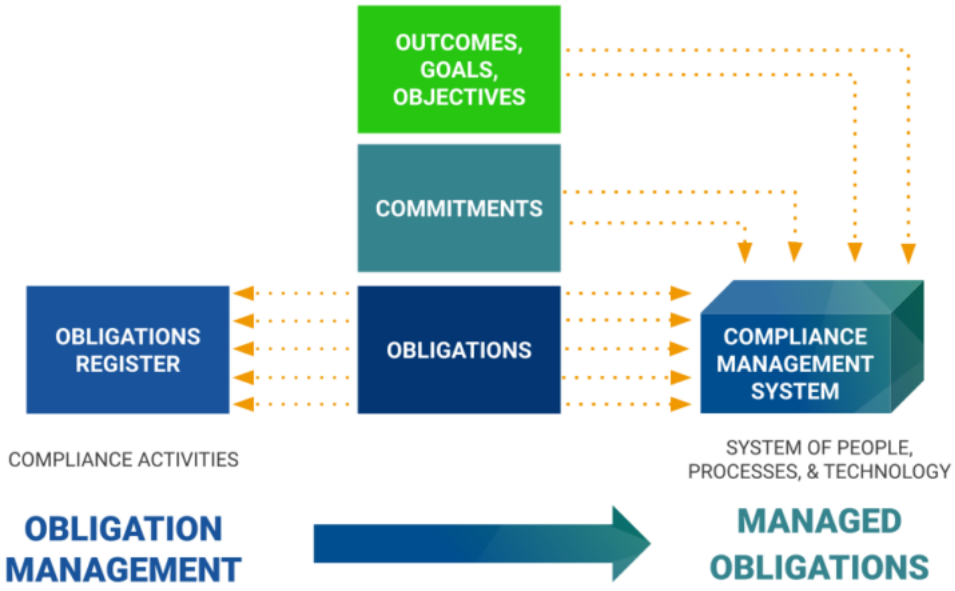
Aside from that, challenges persist for corporate ethics and compliance programs due to increased scrutiny from enforcement officials and the public, the costly consequences of non-compliance, and the potential for reputation damage.

The transition from obligation management to managed obligations

Many organizations focus on compliance activities called *Compliance Management* to meet their legal obligations and manage risk.

And when it comes to compliance management, organizations should understand two concepts: Obligation Management and Managed Obligations. These two are often confused, but they have distinct differences.

Let's take a look at how these two differ.



- **Obligation Management** - involves identifying, monitoring, and verifying an organization's adherence to legal, regulatory, and voluntary obligations. As an essential part of your compliance maturity, *this responsibility falls under the compliance and audit functions of the organization*.
- **Managed Obligations** - emphasizes a systematic approach to achieving compliance outcomes by *integrating compliance into an organization's culture and strategy* to establish appropriate behaviors and procedures to fulfill obligations throughout their entire lifecycle. It enables organizations to fully realize the benefits of compliance while accounting for the associated costs.

In managed obligations, organizations embed compliance into their everyday operations. They do this by fostering a compliance culture.

A culture of compliance is an environment where everyone in the organization understands and follows ethical standards, laws, and regulations. It's possible through strong leadership from the top down and fostering a sense of shared responsibility throughout the organization.

During her speech to the Insurance Council of Australia, Helen Rowell, Deputy Chair of APRA, noted that *'10 years on, [from the Global Financial Crisis] there continue to be major risk and compliance weaknesses'* with a need for *'instilling stronger risk culture across the business.'* [2]

There's also an increasing recognition among compliance professionals, regulatory bodies, and the business community that culture plays a crucial role in managing compliance.

The ultimate goal: managed obligations

Overlaying ethics and compliance onto an existing organization don't result in anything. And despite substantial investment in compliance programs, cultural influence has led to notable compliance failures, suggesting a need for a different approach.

Effective compliance requires integration.

Research shows that many companies prioritize their culture more than ever despite all business areas' unpredictability and uncertainties.[3]

In her keynote address at the ABA 36th National Institute on White Collar Crime, Deputy Attorney General Lisa O. Monaco said, *"A corporate culture that fails to hold individuals accountable, or fails to invest in compliance—or worse, that thumbs its nose at compliance leads to bad results."* [4]

That's why moving towards managed obligations should be the goal of organizations.

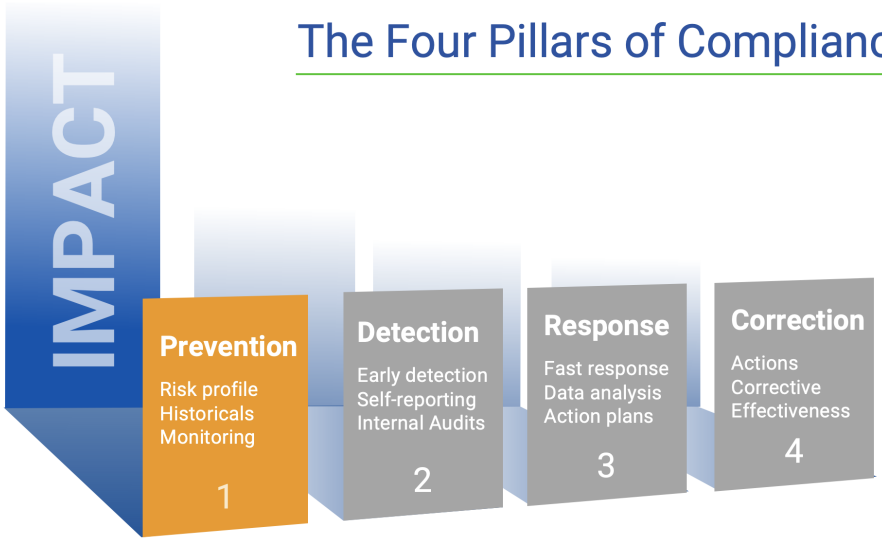
Managed obligations represent a significant milestone in an organization's compliance maturity beyond identifying obligations, tracking commitments, and assessing risks. It allows organizations to go beyond mere compliance with a *'check-the-box'* mindset and fully embrace their obligations by implementing a more strategic and holistic approach.

Characteristics of managed obligations

- **It creates clarity** - properly managed obligations are clearly defined, with specific goals, timelines, and responsibilities established.
- **It's consistent** - a transparent process exists for identifying, prioritizing, planning, executing, and reviewing obligations.
- **It builds conformity** - obligations are managed in compliance with relevant laws, regulations, and ethical standards, ensuring that the individual or organization meets legal and ethical requirements.
- **It has accountability** - clearly defined accountability systems exist, with individuals or teams responsible for fulfilling obligations.
- **It fosters transparency** - the management of obligations is transparent, with information shared openly and stakeholders kept informed about progress and outcomes.
- **It's efficient** - a timely and cost-effective approach is taken to managing obligations, with resources allocated effectively.
- **It can be improved over time** - properly managed obligations are subject to ongoing review and improvement.

Benefits of managed obligations

- **Reduced legal and regulatory risks** - a proactive approach to managing obligations allows organizations to identify and mitigate compliance risks before they become problematic. *By far, this is the most impactful area.*



- **Improved operational efficiency** - it reduces duplication of effort and minimizes disruptions to operations by promoting greater clarity, consistency, and efficiency in compliance processes.
- **Increased stakeholder trust** - a commitment to compliance and ethical behavior can increase confidence among all stakeholders, including consumers, investors, and regulators.
- **Enhanced reputation** - an ethical and compliance culture can enhance an organization's reputation, making it more attractive to investors, customers, and employees.
- **Competitive advantage** - an organization that adopts a managed obligations approach may gain a competitive advantage, particularly in industries where regulation is intense or ethical behavior is a critical factor.

Given these characteristics and benefits, how easy is it to transition to managed obligations? Let's take a look.

The journey towards managed obligations

Transitioning to managed obligations requires a shift in mindset from simply complying with regulations to actively managing obligations.

It means proactively identifying and assessing obligations and developing processes and controls to ensure compliance. It also involves monitoring and evaluating performance and continuously improving the management of obligations over time.

But moving from obligation management to managed obligations may be daunting if there isn't a widely accepted reference.

That's why the International Organization for Standardization (ISO) published standards to help organizations on their journey.

A new standard - ISO 37301:2021

Following its predecessor, ISO 19600, initially published in 2014, ISO 37301 provides a structured approach to help organizations move towards managed obligations.

While ISO 19600 was comprehensive, it only gave *recommendations*. In contrast, ISO 37301 is a Type A Management System Standard (MSS) and can be certified by any accredited auditor.

Type A MSS contains requirements that an organization must meet to claim compliance.

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

Every organization must comply with all laws and regulations. However, smaller companies may be discouraged by the idea of developing a compliance program similar to those used by large multinationals. Additionally, an organization's risk level may vary based on size and nature. And specific risk categories may receive more attention while others are accepted.

Because of this, ISO 37301 is intended to apply to organizations of any type, size, or purpose, whether in the public, private, or non-profit sectors.

Further, ISO 37301 doesn't require the compliance function to be full-time, but it needs to be adequate based on the size and scope of the business. Hence, you can outsource the compliance function or use only a fraction of a full-time employee's time.

Why move from ISO 19600 to ISO 37301?

People familiar with ISO may ask why the change is necessary. The answer is simple - ISO 37301 provides *requirements* for establishing, implementing, and maintaining a Compliance Management System (CMS), while ISO 19600 only provides ***guidance*** for establishing a CMS.

ISO 37301 also has the potential to become a global standard for compliance management systems.

Also, ISO 37301 is closely related to ISO 37001. An important aspect of ISO 37001 is its focus on anti-bribery management systems. Organizations that are already considering ISO 37001 certification could save time and costs by implementing ISO 37301 at the same time.

But what is a Compliance Management System (CMS)?

A CMS system goes beyond the "responsible managers" and "authorized representatives"; it involves everyone in the organization. It includes a set of policies, procedures, and controls to ensure the company meets its compliance obligations.

Furthermore, a Compliance Management System provides a framework for fulfilling compliance obligations, including those mandated by laws and other governing regulations and those they voluntarily comply with, such as internal guidelines and protocols.

What does ISO 37301 offer?

Whether an organization decides to certify its CMS or uses ISO 37301 as a starting point to implement a compliance program that meets international standards, ISO 37301 offers many advantages, such as the following.

Takes a risk-based approach

ISO 37301 emphasizes risk assessment more than ISO 19600. Organizations must identify, assess, and prioritize compliance risks under ISO 37301. Meanwhile, ISO 19600 only suggests considering compliance risks in the compliance management system.

Considers a broader context

ISO 37301 requires organizations to consider internal and external contexts for their compliance management system. It includes culture, values, and stakeholders. The standard acknowledges that companies operate within a broader approach and are affected by societal factors. It mandates examining the socio-political environment and considering the competition, socio-economic conditions, and territorial variables. On the other hand, ISO 19600 only requires consideration of external context.

Creates a compliance culture

The culture of compliance is at the heart of this new standard. Organizations must promote an ethical culture based on values, where everyone understands their responsibilities and roles. It'll help ensure a resilient organization that can minimize compliance disruption. Aligning culture with objectives is essential to avoid internal organizational conflicts.

Establish a whistleblowing policy

The new standard emphasizes the importance of whistleblowing and reporting channels in detecting compliance issues and outlines specific requirements to ensure their effectiveness. It also promotes a culture where every organization member is responsible for compliance.

Implement performance evaluation

ISO 37301 mandates that organizations implement a compliance performance evaluation process. It involves monitoring and measuring compliance performance, analyzing the findings, and taking corrective actions when needed. Meanwhile, ISO 19600 standard only recommends evaluating the effectiveness of compliance management systems.

Protects from third-party and supplier risks

[5]According to the EY Global Integrity Report 2020, approximately one-third of organizations aren't confident in the honesty of their third parties. It puts organizations at risk of penalties and fines due to third-party actions. And some organizations have faced sanctions in the past due to third-party behavior. Organizations that are ISO 37301 certified adhere to international compliance standards and undergo an independent audit every year. Working with these organizations is an excellent way to mitigate third-party risks.

What is the role of ISO 37301 in transitioning to managed obligations?

A smooth transition from obligation management to managed obligations requires a robust CMS to establish policies and procedures, define roles and responsibilities, identify and evaluate risks, implement controls, monitor and report compliance, and continually improve their CMS.

And this is where ISO 37301 can help.

As previously discussed, ISO 37301 provides organizations with the requirements to implement a CMS. These requirements are based on established and globally recognized principles of *good governance*, *proportionality*, *transparency*, and *sustainability*.

Moreover, managed obligations require some essential components of ISO 37301, and we'll discuss these in the following section.

Key aspects

Managed Obligations	ISO 37301
Develop a comprehensive understanding of obligations that involves identifying and understanding all legal, regulatory, and voluntary obligations that apply to the organization.	Stresses the importance of understanding legal requirements and other obligations that apply to the organization as part of establishing an effective compliance management system.
Prioritize obligations based on their impact on the organization's operations, reputation, and stakeholders.	Requires organizations to prioritize compliance risks based on the potential impact on the organization and allocate resources accordingly.
Integrate obligations into the organization's overall strategy to ensure compliance is embedded in its business practices.	Emphasizes the need to integrate compliance into the organization's strategy and culture to establish a culture of compliance.
Monitor and measure compliance with obligations to ensure they meet their requirements. It includes establishing KPIs to track compliance and conducting regular audits and assessments.	Organizations must monitor and measure compliance with legal requirements and other obligations to ensure that the compliance management system is effective.

Regularly review the compliance management system and make necessary improvements to ensure the organizations meet their obligations effectively.	Stresses the need for continuous improvement. It requires organizations to review and improve their compliance management system regularly.
Establish a compliance culture that promotes ethical behavior and encourages employees to take responsibility for compliance.	Highlights the importance of establishing a compliance culture and providing training and resources to employees to promote compliance.

Making it work

There are Critical Success Factors (CSF) you must consider to successfully implement an ISO 37301-based CMS and elevate the role of culture in the compliance process of your organization.

These factors can vary depending on the organization and its unique circumstances but generally include the following:

Top management support

Strong support from your top management is essential for successfully implementing ISO 37301. Leaders should communicate their commitment to ensuring its effective implementation and continued success.

Involvement of stakeholders

Your CMS should involve all relevant stakeholders, including employees, suppliers, customers, and regulators. Failure to involve these stakeholders can lead to resistance to the system and a lack of buy-in.

Obligation identification

Knowing your obligations is critical for effective compliance. Lack of knowledge will contribute to gaps in compliance, excessive risk, and failure to provide stakeholder assurance. It should include knowing about your legal, regulator, and stakeholder obligations.

Risk assessment

Your CMS should be built around assessing the organization's compliance risks. This assessment should identify and prioritize the organization's risks based on their severity and likelihood of occurrence.

Clear policies and procedures

Your policies and procedures should align with your organization's goals, risk profile, and compliance requirements. Communicating these to everyone is important so they understand their roles and responsibilities in achieving compliance.

Training and awareness

Educate your employees about their roles and responsibilities in complying with CMS through training and awareness programs. Regularly doing this will ensure they remain current on changes and compliance requirements.

Monitoring and measurement

You should include options on your CMS for monitoring and measuring effectiveness and ensuring it meets its objectives. Some of these options include regular compliance audits, reviews, and assessments.

Continuous improvement

Your CMS should be flexible enough to adapt to changes in your organization's compliance risks, regulatory requirements, and business objectives.

Based on these CSFs, is adopting ISO 37301 a simple process?

Structured implementation process

The good news is that whether your organization is new or established, adhering to an ISO 37301-based CMS is achievable and doesn't have to be daunting.

Below is a general framework Nimonik recommends for implementing the standard. However, your approach will depend on your organization's nature, size, and complexity.

Step 1: Understand the standard

Understanding the standard involves reviewing its requirements, definitions, and clauses to understand its scope and objectives.

You can start by reading the ISO 37301 document, which outlines the compliance requirements for an effective compliance management system. As you learn more about the standard's requirements, you may seek expert guidance, attend training sessions, or participate in webinars and workshops to better understand.

Step 2: Conduct a gap analysis

This step involves identifying any gaps or areas of non-compliance between your current management system and the requirements of ISO 37301. It's a crucial step in the implementation process, allowing you to identify and prioritize your company's significant integrity and compliance risks.

Step 3: Define the scope

After identifying the areas of improvement from Step 2, the next step is to define the boundaries of your compliance management system. It includes determining the processes, activities, products, and functions the CMS will cover.

When defining the scope, consider the nature of your business, objectives, risks, and legal obligations.

Step 4: Establish a compliance policy

Your compliance policy should outline your organization's commitment to compliance and approach to managing compliance risks. It should guide your employees' and stakeholders' roles and responsibilities in ensuring compliance with applicable laws, regulations, and ethical standards. It should also establish a process for monitoring and reporting on compliance activities, including regular reviews and audits.

Finally, it's crucial to inform all stakeholders about the policy.

Step 5: Develop a compliance management framework

After establishing the policies, the next step is to create a framework that will serve as your blueprint for your organization's compliance efforts and outlines the steps needed to ensure compliance with all relevant laws, regulations, and standards.

The framework will provide a structured approach to managing compliance risks, including identifying and assessing risks, implementing controls, monitoring and reviewing performance, and reporting compliance issues.

Step 6: Implement the compliance management system

This step is about putting your CMS into action. It's where you implement all your planning and preparation in your organization.

First, you must assign roles and responsibilities and train your employees to ensure they understand their compliance responsibilities. It includes everything from how to report potential compliance issues to how to handle customer complaints.

You can start implementing the new system once everyone is trained and up to speed. It may involve changing your existing processes or creating new ones altogether. You'll also need to set up a system for monitoring and measuring your compliance performance so that you can track your progress and identify areas for improvement.

Step 7: Monitor and measure performance

Implementing new systems is bound to have hiccups since they aren't perfect immediately. So, it's essential to establish metrics and monitoring procedures to measure the effectiveness of the compliance management system. These metrics may include the number and type of compliance incidents, compliance training frequency, and employee engagement in compliance activities.

Step 8: Continuously improve

This step ensures that your CMS continuously evolves and improves to meet your organization's changing needs and the standard's requirements.

Analyze and review performance data regularly to update policies and procedures to comply with the latest regulatory requirements. It'll help you stay ahead of the curve and ensure your CMS is always up-to-date and effective.

Step 9: Get certified

Once your organization has implemented the compliance management system, and it has been in operation for a sufficient period, you can seek certification to ISO 37301 from a recognized certification body.

Certification proves that your organization has met the standard's requirements and is committed to ethical business practices. It also demonstrates to stakeholders, customers, and regulators that your organization is trustworthy and responsible.

The steps seem straightforward. But is there an easier way to implement it? What tools can be leveraged for successful implementation?

The role that technology plays

More forward-looking technology tools are available today that weren't around 10 years ago that can help organizations take a more proactive approach to compliance management.

In our work with our clients, the Nimonik team has greatly found technology to help the compliance management process. Tools like NimonikApp provide automated solutions to keep up with regulatory changes, track and monitor compliance issues and tasks, provide easy access to internal documents and other resources, and allow team collaboration.

But more importantly, before we start working with a client, we help them assess their current compliance management process and identify areas of improvement. Here's how we do it.

Set clear expectations

We'll gather information through interviews with internal and external stakeholders to understand their organizational priorities. We then use these insights to pinpoint key challenges and develop a roadmap aligning with their business strategy.

Perform control and process evaluation

We'll conduct deep dives into their existing business processes and controls, assess the cost of compliance, and determine what needs to change and be true to achieve significant quality improvements.

Define your regulatory universe

Assess the current new and amended regulations affecting their business and ensure they appropriately respond to regulators and authorities.

Ensure better governance

Establish good governance practices, such as regular review processes and an operating model to meet compliance needs.

Scale the solutions

Build a framework and strategy for long-term compliance, develop controls as needed, and identify other solutions that can scale over time.

Monitor, manage, and report

Help organizations proactively navigate regulatory change and build sustainable compliance solutions with ongoing monitoring, management, and reporting.

These days, many companies face challenging regulatory environments and the risk of costly fines and sanctions. To add to the stress, manual compliance management processes are time-consuming, inefficient, and prone to errors. But with the right tools and strategies, organizations can build a successful compliance management system that is industry standard and meets their needs and those of their stakeholders.

As the ISO 37301 organization states, "An effective, organization-wide compliance management system enables an organization to demonstrate its commitment to comply with relevant laws,

regulatory requirements, industry codes, and organizational standards, as well as standards of good governance, generally accepted best practices, ethics, and community expectations" [6].

About Nimonik Inc.

Nimonik Inc. provides an integrated compliance management solution to meet regulatory requirements and industry standards. The Nimonik software helps businesses and governments identify their obligations and requirements, track regulations for changes, and determine their compliance through audits and registers.

Based in Montreal, Canada with offices in Calgary and Toronto and offices in Shanghai, China.

If you need help implementing a Comprehensive Compliance program for your organization and stakeholders, please contact us at **info@nimonik.com** or **+1-888-608-7511**

Resources:

1. Relationships Are Critical to Compliance, Says AdventHealth Leader - WSJ
2. Culture of (and beyond) compliance | Deloitte Australia | Audit & Assurance
3. Culture's effects on corporate sustainability practices: A multi-domain and multi-level view - ScienceDirect
4. Embrace a Culture of Compliance, Don't Just Check the Box - Ethisphere Magazine
5. Global Integrity Report 2020, EYGM Limited, 2020, accessed 13 April 2023.
6. ISO 37301:2021(en), Compliance management systems — Requirements with guidance for use