COMPLIANCE RISK AND ISO 37301: RESHAPING COMPLIANCE MANAGEMENT

LexisNexis® | *Regulatory Compliance*

Introduction

When the U.S. Department of Justice (DOJ) investigates a company, it is required to look at specific factors. One of the key issues that must be evaluated before determining whether to bring charges is the adequacy and effectiveness of the company's compliance program.

It is for good reason that the DOJ places such importance on the strength of an organization's compliance system. Meeting the full gamut of a company's legal obligations is not easy. It requires the development and careful maintenance of complex systems. It also requires a genuine commitment to continuous improvement. As risk and compliance professionals and seasoned company officers know, the one area of risk that grows at an exceptionally high rate for every organization in every sector is compliance risk.

Compliance risk can be managed by developing an organization-wide compliance regime that is robust yet agile. Organizations are wise to seek and make use of tools that assist in creating and maintaining their compliance systems.

This white paper outlines how the new ISO 37301 standard is reshaping the future of compliance and how it can assist businesses in mitigating compliance risk.

Compliance Risk in Context

Compliance risk describes an organization's exposure to penalties and other forms of loss for failing to meet its obligations. Mandatory obligations generate the most obvious compliance risks. These are the concrete legal requirements created by laws, regulations and contract provisions.

An organization in its first year of operation will accumulate mandatory obligations immediately as a result of its regulatory environment. The nature and extent of these obligations will vary in accordance with the organization's industry and corporate structure.

However, mandatory obligations are only part of an organization's compliance risk profile. Voluntary obligations also create compliance risks. These are the softer obligations created by an organization's values and social commitments.

An Illustration: Health Tech Start-up in New York

Consider a start-up organization in the tech industry beginning as a limited liability company (LLC) and operating out of New York City. The organization is building a phone app to help New Yorkers find and book fitness classes in their area.

At this early stage the organization already carries mandatory obligations created by numerous areas of federal law. The organization must provide workers with conditions and entitlements as required by the Fair Labor Standards Act (1938), the Occupational Safety and Health Act (1970) and the Immigration and Nationality Act (1952). The organization will also be required to comply with the terms of its own privacy policy under the Federal Trade Commission Act (1914).

Under federal taxation law, a range of requirements in relation to paying and withholding federal income tax, social security taxes and other federal taxes will apply to the organization. Compliance with the Securities Act (1933) and the Securities and Exchange Act (1934) will also be required for start-ups that offer equity in the company to workers or investors.

State legislation adds another layer. The organization must comply with the laws of the state in which it has incorporated, as well as the states in which it conducts its business. Under New York State law, the organization is required to protect information it collects about its users on its app. Requirements relating to private information and data protection apply under New York's Information Security Breach and Notification Act (2005) and SHIELD Act (2019).

In the area of employment law, both federal and state workforce protections call for careful attention by the company's compliance professionals. The organization must also meet corporate governance obligations, as well as report on and pay New York state's franchise taxes.

In addition, a growing list of states and municipalities—including New York City—have been implementing pay transparency laws requiring companies to post or disclose a pay range for available jobs in an effort to close gender and race-related pay gaps. This start-up in New York would need to prepare guidance and policies for compliance with pay transparency and disclosure laws.

In addition, the organization must comply with the provisions of service contracts entered with its consumers and suppliers.

To draw attention to the value of its services, the organization may promote its commitment to wellness, social good and accessibility. Meeting this voluntary obligation and social commitment requires the company to take actions to ensure that its services are both affordable and effective at improving the health and well-being of New Yorkers.

Failure to meet this myriad obligations can attract a variety of severe consequences, including:

- Financial penalties imposed by a court
- The cost and time commitment of mounting a legal defense
- Permanent damage to brand and reputation, reducing demand for services and longer-term restriction of growth

If the organization were to expand its services to other jurisdictions, this would require compliance with multiple regulatory regimes simultaneously. Providing services in multiple U.S. or international cities could lead to complications with information management and asset management. Maintaining a social commitment would require the organization to undertake constant community engagement in multiple locations.

The expansion of the app's functionality could also create new compliance issues (for example, adding a feature where users can search and make appointments with healthcare providers). This could attract complex regulation under federal, state and international healthcare and privacy laws.

A team of compliance professionals cannot manage risks of this range, volume and magnitude in a haphazard manner. Achieving effective compliance risk mitigation demands a formal compliance management system.

Implementing a Compliance Management System

A compliance management system (CMS) presents a framework of best practice measures designed to keep an organization on the right side of all of its obligations.

The core of every CMS is an obligations register that catalogs the mandatory and voluntary obligations of the organization. On top of the register sits a compliance control matrix that links obligations with objectives, risks, policies, controls and responsibilities.

A CMS provides visibility and control over the compliance status and activities of the organization. This enables senior officers and other interested stakeholders to understand:

- The obligations of the organization
- How/when those obligations are met
- Who has ownership of each obligation
- How new and changing laws will affect these obligations in the future

The level of control provided by a CMS program empowers senior officers to tune risk management activities to suit the organization's risk appetite.

A CMS also contains governance measures for embedding compliance into the culture of the organization. This is a critical function of the system, as mitigating compliance risks requires the effective cooperation of every officer, employee and contractor.

A well-designed CMS scales alongside the organization through continuous improvement systems. An organization that establishes a comprehensive CMS in 2021 should be able to mitigate compliance risks just as effectively with the same CMS in 2031.

Implementing a CMS brings numerous benefits. These include:

- The ability to recognize and mitigate new compliance risks proactively as they arise
- Minimization of legal contraventions and associated costs
- Enhancement of the organization's credibility
- Confidence in the organization's sustainability

For these reasons, capital partners and issuers of large contracts increasingly require organizations to provide evidence of an ISO 37301-compliant CMS as a prerequisite of doing business.

The core of every CMS is an obligations register that catalogs the mandatory and voluntary obligations of the organization.

The International Compliance Standard

ISO 37301 is an international standard that helps organizations to establish, develop, implement, maintain and improve an effective CMS. The standard builds upon the principles documented in its predecessor, ISO 19600.

ISO 37301 is a Type A standard. This means regulators and independent experts can certify the CMS of an organization as ISO 37301 compliant.

Certification carries numerous potential benefits. Venture capitalists and other financial partners may limit their searches to CMS-compliant entities. Bidders for public projects may find calls for tenders require a certified CMS. Other organizations may use certification to demonstrate their competence to clients and improve their industry standing.

In addition, organizations operating in high compliance risk industries may be required to maintain certification as a license condition.

PDCA Cycle

ISO 37301 encourages organizations to adopt a plan-do-check-act (PDCA) approach to compliance management. The goal of PDCA is to achieve continuous improvement in management systems.

Performing PDCA sees organizations engage in a perpetual cycle of:

Planning—designing processes to achieve desired outcomes
Doing—implementing processes prepared in the planning phase
Checking—evaluating data collected during the doing phase against expected outcomes
Acting—adjusting established processes to better achieve desired outcomes

The PDCA cycle appears frequently in ISO standards governing management systems. Organizations that adopt PDCA in their CMS can integrate compliance management into the PDCA cycles of other established systems.

Organizational Context

Organizations implementing an ISO 37301-compliant CMS must begin by establishing an obligations register. An obligations register catalogs all of the current mandatory and voluntary obligations of the organization. Each organization must customize the register to provide a comprehensive picture of its obligation status. Having created and populated the register, the organization must conduct a risk assessment. Risk professionals should gauge the risk associated with each entry in the register with the goal of creating the data required to set the organization's risk appetite and propose effective controls.

Performing regular risk assessments allows for a process of continual improvement whereby the CMS is amended and refined to reflect the company's current risk profile.

To complete its assessment of the organization's compliance context, the organization must document any specific compliance expectations of external parties, including partners and holding companies.

Designing the Matrix

Having documented the organizational context, the organization must create and document a matrix of controls for ensuring ongoing compliance with the obligations in the register.

The control matrix comprises policies, functions, processes, roles and tools that achieve standards prescribed in ISO 37301. These standards cover and include:

- **Governance**—officer responsibilities and the promotion of a compliance culture
- **Planning**—procedures for modifying compliance processes to take advantage of opportunities and to respond to emerging risks, regulatory developments, industry events, or changes to the company's strategic plan
- **Support**—compliance training for staff and employment practices to ensure all hires are compatible with the compliance culture
- **Operations**—processes for communicating compliance failures
- **Performance evaluation**—Review of compliance KPIs, records and other data points to assess effectiveness of the system
- **Improvement**—measures designed to ensure compliance failures are addressed appropriately

Sophisticated organizations may choose to create a scalable control matrix that enables risk professionals to tune the intensity of compliance actions according to the risk appetite set by senior officers.

Protected Reporting

Unlike its predecessor, ISO 37301 requires organizations to encourage whistleblowing. Organizations must include formal systems in its control matrix that enable staff to report their concerns easily, that protect reporters from retaliation, and that ensure the confidentiality of reports.

A dedicated international standard governing whistleblowing (ISO 37002) is currently under development. Once published, certification with ISO 37301 is likely to require compliance with ISO 37002.

Compliance Culture

Organizations seeking ISO 37301 certification must establish a standard of conduct for staff that promotes compliance. This standard must be enforced at all levels, from entry level to senior management.

Certified organizations must also consider the effects of cultural diversity and differing views among staff members upon internal communications and make allowances for the impact these elements may have upon compliance.

Reshaping the Future of Compliance

An ISO 37301-compliant CMS represents more than best practice for compliance risk management. It is the yardstick against which the compliance risk mitigation processes of companies will be measured in the future to determine their success as an organization.

The guidance contained in ISO 37301 is scalable to organizations of any size and industry. Organizations without a CMS should consider the risk reduction benefits that come with ISO 37301 certification.

Organizations already aligned with ISO 19600 should update their CMS in accordance with ISO 37301 to achieve best practice.

Your Free Demonstration

If you would like a demonstration of the ISO 37301 Compliance Obligations Register, scan the QR code. →

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance is a legal obligations register and alerting solution that combines regulatory content with technology to empower you to take control of your compliance obligations. We use leading legal and industry experts to provide a practical, plain English interpretation of all the relevant legislative and regulatory materials, so you don't have to. Content is updated regularly, so you can access obligations that reflect the current legislative framework—helping you save significant costs and/or research time. All content is supported with flexible technology options designed to meet your existing and future needs. LexisNexis Regulatory Compliance makes your compliance journey fast and seamless.

Call 800-543-6862

Visit lexisnexis.com/regulatory-compliance

About LexisNexis®

LexisNexis is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries. LexisNexis helps customers to achieve their goals in more than 150 countries, across six continents, with over 10,000 employees.

LexisNexis® | *Regulatory Compliance*