

Business Ethics: Can ISO 37000 Enhance Your Company's Compliance and Ethics?

Compliance and Ethics



On Sept. 1, 2021, the International Standards Organization (ISO) published ISO 37000 — guidance for the governance of organizations (hereinafter, “ISO 37000” or the “Standard”).

ISO is an international organization for standardization based in Geneva, Switzerland comprising a membership of 165 national standards bodies. As you may know, ISO is responsible for developing and publishing over 24,146 standards regarding a wide variety of subject areas from environment, health protection and safety to road vehicles engineering.

ISO 37000 is the product of experts from a wide range of organizations in over 70 countries around the world and is billed as the “first ever international benchmark for good governance.”

The Standard’s stated purpose is to assist “governing bodies” — boards of directors or trustees of organizations of all shapes and sizes — in exercising “good governance” where “decision making within the organization is based on norms, practices, behaviors, organizational ethos, culture, structures, and processes to create and maintain an organization with clear purpose that delivers long term value consistent with the expectations of its stakeholders.”

Its 42 pages are organized around 11 principles of governance:

1. Purpose
2. Value generation
3. Strategy
4. Oversight
5. Accountability
6. Stakeholder engagement
7. Leadership
8. Data and decisions

9. Risk governance
10. Social responsibility
11. Sustainability

The primary focus of the Standard is to promote good governance (the “G” of “ESG”). However, ISO 37000 also requires directors to use their authority to enhance their organizations’ environmental (“E”) and social (“S”) performance.

The Standard claims that “[b]y doing this an organization demonstrates ethical behavior and helps maintain a balance between social, economic, and natural environmental system health and proactively creating sustainable wellbeing.”

As may be apparent from the Standard’s 11 principles of governance, ISO 37000 places expectations on governing bodies that significantly exceed the minimum duties of care and loyalty comprising the business judgment rule and the US Federal Sentencing Guidelines’ mandate that the “organization’s governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.”

The duties the Standard assigns to governing bodies are so voluminous and detailed, I wondered as I read them how any board of directors could satisfy all of them and whether any self-respecting senior management team would tolerate the recommended level of board oversight.

> I wondered as I read them how any board of directors could satisfy all of them and whether any self-respecting senior management team would tolerate the recommended level of board oversight.

But setting that concern aside, the good news for us compliance and ethics professionals is that the Standard is chock full of compliance and ethics board oversight obligations that, if fully executed, hold out the prospects of getting directors in the game in a way that might materially reduce corporate compliance and ethics risk profiles and adequately fund and staff corporate compliance offices.

Here’s a sample of some of ISO 37000’s compliance and ethics requirements:

7.1 Purpose

7.1.3 Key aspects of practices

The governing body should determine and communicate the organizational purpose and values and ensure they are embedded throughout the organization.

7.1.3.2 Determine organizational values

The governing body should be clear about the expected ethical behavior that expresses its organizational values through for example, a code of conduct, and/or code of ethics.

The governing body remains responsible for ensuring that the organizational values are monitored and reviewed, and should assess whether the values remain aligned to and support the organizational purpose.

7.3 Strategy

7.3.3.1 Direct the organization

The governing body should:

- Design and implement an adequate internal control system, including an effective compliance management system and an effective risk management system.
- Ensure that its governance policies clarify the roles of all involved in governing the organization in terms of their authority, accountabilities, performance, and reporting requirements.

7.3.3.2 Monitor and adjust the strategic balance of the organization

The governing body should regulate the strategic balance of the organization directly and indirectly through organizational culture and the deployment of financial resources.

7.3.3.5 Strategically balance the organization

Executive manager and senior management team performance — monitoring, evaluating, and developing individual and team performance including organizational value driven behaviors pertaining to sustainability and social responsibility dimensions among others.

7.4 Oversight

7.4.3.1 Ensure organizational capability

The governing body should:

- Establish and adequately resource systems of internal control, compliance management and risk management to ensure that the organization stays within its risk appetite and appropriately protects the organization’s assets, and stakeholder rights and interests
- [A]ppraise applicable measurement criteria and results against the governing bodies expectation. Such criteria can include:
    - Culture, including local norms
    - Compliance management
    - Risk management processes and performance

There are many more similar mandates peppered throughout the Standard, but I suppose you get the picture. As useful as applying the Standards might be in helping our companies better manage their portfolio of legal and ethical risks, the big question is whether our directors would have any interest in adopting them. Given directors' current significant workload, absent the lash of necessity, this may be unlikely.

> The Standards are worth a read, if for no other reason, to provide corporate counsel and compliance professionals some ideas about recommendations they might make to their directors to improve compliance and ethics program performance.

A quick search I conducted of the US Department of Justices' and Securities and Exchange Commission's websites yielded no mention of the Standards. So, the push, if it will ever come, is not currently in the cards from US enforcement agencies or regulatory authorities. Moreover, it's likely that few corporate directors have ever even heard of the Standards. I checked the National Association of Corporate Directors' website and found that it too made no mention of them.

However, the Standards are worth a read, if for no other reason, to provide corporate counsel and compliance professionals some ideas about recommendations they might make to their directors to improve compliance and ethics program performance.

But if you're successful in getting your board to consider adopting some or all of the Standards, you should be prepared to provide them substantial assistance. Like many ISO standards, ISO 37000 is long on the "what" but short on the "how."

Don't expect your directors to figure out practical methodologies to implement the Standards. That job will likely fall on you and your colleagues in the management team. However, if you're lucky enough to be assigned such a task, take full advantage of it. ISO 37000 just might help your company enhance its compliance and ethics performance and thrive over the long term.

Jim Nortz



Founder & President

Axiom Compliance & Ethics Solutions, LLC