principals and supervisors of a broker-dealer firm). The initial "onboarding" of directors and senior executives, as well as their continuing education, depends upon organizational and industry practices. See NAVEX GLOBAL, 2018 ETHICS & COMPLIANCE TRAINING BENCHMARK REPORT 36 (2018) (72% of surveyed firms provide in person/live training on ethics and compliance to board members, generally in the one- to two-hour range yearly). Programs exist for new public-company directors, some in affiliation with universities. See, e.g., Directors Consortium, Graduate School of Business, Stanford University, http://www.gsb.stanford.edu/exed/directors/. There are numerous continuing education and professional programs for internal-control officers, including annual professional meetings, discussion groups, and other resources. See, e.g., Society of Corporate Compliance and Ethics, http://www.corporatecompliance.org/.

§ 3.07. The Role of the Board of Directors and Executive Management in Promoting an Organizational Culture of Compliance and Risk Management

(a) The board of directors and executive management should promote an organizational culture of compliance and sound risk management.

(b) To promote this culture, among other ways, the directors and executive management should:

(1) approve the values represented in the compliance policies and procedures, the ethical standards in the code of ethics, and the risk culture in the risk-management program;

(2) satisfy themselves that the organization's practices foster these values, standards, and risk culture;

(3) be assured that employees and agents of the organization are willing to adhere to, and their organizational activities reflect, these values, standards, and risk culture; and

(4) communicate, and demonstrate by their actions, adherence to these values, standards, and risk culture throughout the organization, to all its employees and agents, and, if appropriate, to those outside the organization.

Comment:

a. General. As stated in subsection (a), the board of directors and executive management are responsible for promoting an organizational culture of compliance and sound risk management. "Organizational Culture" is defined in § 1.01(oo) to be the "norms, assumptions, perspectives, and

beliefs that guide and govern" the conduct of organizational actors. In so doing, they are supporting a major goal of both the compliance function, as set forth in § 5.02(e), which is "establishing and maintaining a culture of ethics and compliance within the organization," and risk management, as set forth in § 4.06(b)(2), which provides that an element of an effective risk-management program is "creating, promoting, and retaining an appropriate risk culture." "Risk Culture" is defined as "[a]n organization's norms, assumptions, beliefs, understandings, attitudes, and values that shape behaviors, decisions, discussions, and assessments relating to risk." See also § 4.09 (identifying the goals of an organization's risk culture, including in subsection (f) "put[ting] in place appropriate mechanisms to establish, maintain, and promulgate its risk culture throughout the organization"). Under this Principle, together with senior executives, the directors must set a tone—a "tone at the top." See § 1.01(ggg) (defining "tone" as a publicly communicated set of values and norms, expressed in behaviors as well as words) and § 1.01(hhh) (defining "tone at the top" as the tone set by the board of directors and executive management). Because the organization's culture should be the foundation for all its practices and actions, this Principle highlights how, apart from fulfilling their specific compliance and risk-management responsibilities, the board of directors and executive management specially contribute to and support this culture. The Principle is particularly suited for a publicly traded company or other organization of comparable size and operations. Other organizations (or even these) may allocate responsibilities for promoting organizational culture in accordance with their needs and circumstances. However, this Principle strongly recommends that the board of directors and executive management be involved in this effort to promote culture in some way.

b. Approving values, standards, and risk culture. Subsection (b) sets forth several nonexclusive ways in which the directors and senior executives can promote the organizational culture. Subsection (b)(1) recognizes that they must approve the values, standards, and risk culture that are represented in the organizational documents that organizational actors use to guide their conduct. See § 1.01(g) (definition of code of ethics); § 1.01(l) (definition of compliance policies and procedures, which include "an organization's philosophy and general approach to compliance issues"); § 1.01(u) (definition of ethical standards, which are "a set of principles, grounded in concerns of morality or the public good" adopted by the organization and formalized in the code of ethics); § 1.01(xx) (definition of risk culture); § 4.06(b)(2) (specifying that an organization should "creat[e], promot[e], and retain[ ] an effective risk culture"); § 4.09 (specifying the goals

of an organization's risk culture); § 5.36 (describing an organization's commitment to ethical conduct); § 5.37 (discussing features of an organization's code of ethics). In effect, the articulation of the compliance values, ethical standards, and risk culture should result from the collaboration between the board of directors and executive management. With the assistance of internal-control officers, executive management proposes the overall approach of the compliance and risk-management programs, see § 3.14(b)(2) and (4), which the board of directors approves, see § 3.08(b)(2) and (4). In conferring approval, however, the directors should make sure that their own compliance values, ethical standards, and attitudes towards risk are incorporated or reflected in executive management's approach, given their ultimate oversight responsibility for the organizational culture of compliance and risk management.

c. Approving organization's practices. Subsection (b)(2) recognizes that the board of directors and executive management must do more than agree upon the compliance values, ethical standards, and a risk culture to create an organizational culture of compliance and risk management. They should satisfy themselves that the organization's practices, particularly its compensation and incentive practices, foster, and do not undermine, the values, standards, and culture. Otherwise, the compliance policies, the code of ethics, and the risk-management framework will be empty words. To take one example, employees cannot be rewarded or praised for having undertaken successful business operations or other affairs that fell outside the organization's risk limits, were in violation of its compliance program, or ran counter to its ethical standards. The board of directors and executive management will have different responsibilities for the organization's practices, given their respective governance roles. Thus, executive management, which is familiar with and involved in directing the formulation and implementation of many of the organization's central practices, will be more involved than the board of directors with ensuring that the practices foster its compliance values, ethical standards, and risk culture. As part of its oversight of the organization, the board of directors would be expected to ask executive management to explain how the practices further the organization's values, standards, and culture, when executive management is presenting these practices to the board for its review or approval.

d. Overseeing employees' and agents' adherence to organizational culture. Subsection (b)(3) suggests that the board of directors and executive management promote an appropriate organizational culture of compliance and sound risk management only if the activities of the organization's employees and agents reflect its values, standards, and risk culture. See § 4.09(a)

(risk culture "promot[ing] risk-aware behavior and attitudes throughout the organization"). They must thus take steps to ascertain that those becoming employees or agents are willing to adhere to, and in fact demonstrate in their words and conduct, the organizational culture. Again, the board and executive management have different responsibilities for this matter. The board does not generally oversee employee hiring, the engagement of agents, or their respective conduct. It is responsible, however, for selecting the chief executive officer and for approving that officer's recruitment of the other members of executive management. When hiring a chief executive officer, the board should receive assurance that this officer will adhere to and promote the organizational culture. In overseeing the chief executive officer, the board should look for evidence that the officer conducts himself or herself in accordance with the organization's compliance values, ethical standards in its code of ethics, and risk culture. For example, the board should take comfort to learn that the chief executive officer rewarded, rather than retaliated against, an employee who reported on a compliance problem in the organization. Similarly, while the chief executive officer does not typically conduct all the hiring in an organization, engage all of its agents, and oversee their respective conduct, that officer is responsible for selecting the main executives in the organization's managerial team, for approving the engagement of its main agents, for setting the organization's general hiring and contracting policies, and for deciding upon its major activities. The officer should thus ensure that the organization hire, engage, and retain only those whose background, words, and actions show likely adherence to the organization's culture. This executive action reinforces the organization's human-resource responsibilities that are discussed in §§ 5.14-5.17. Executives have less control and influence on the conduct of a third-party agent, engaged for a particular organizational task, than they do on the actions of employees. Nevertheless, they should put in place procedures to ensure that, while the agent acts on the organization's behalf, it does so in accordance with the organization's culture.

e. Communication and demonstration. Subsection (b)(4) provides that the directors and senior executives should communicate, and demonstrate by their conduct, the organization's compliance values, ethical standards, and risk culture. The communication and demonstration should be designed to reach as many employees and agents of the organization as possible and to encourage them to carry out their business or affairs in accordance with the values, standards, and risk culture. They should thus let it be known in the organization that compliant conduct is rewarded and noncompliant behavior is punished. They should also realize that their words and

actions can undermine the organization's values, standards, and culture. For example, if it becomes known throughout the organization that a chief executive officer seeks to identify for probable retribution an employee who reported on problematic organizational practices through a confidential internal-reporting system, this conduct could have a devastating effect on the culture of compliance. Similarly, when a senior executive urges a fellow executive who has questioned improper, but profitable, firm use of client information not to pursue the issue, that executive is clearly demonstrating that profits take priority over the organization's culture.

In addition, the directors and senior executives may also deem it appropriate to publicize the organization's culture more broadly to those outside it, particularly in the communities where its offices and operations are located, and to other stakeholders and to regulators. They should not be expected constantly to engage in this publicizing activity. However, they should understand that their words and actions on compliance, ethics, and risk also have a special impact outside the organization. This subsection thus underscores the importance of "tone at the top," which, as noted above, is subsumed in this Principle.

REPORTERS' NOTE

a. It is well recognized that the board of directors and senior executives have a key role in creating an organizational culture of compliance and risk management. See, e.g., FINANCIAL REPORTING COUNCIL, CORPORATE CULTURE AND THE ROLE OF BOARDS: REPORT OF OBSERVATIONS 12-19 (2016) (discussing ways in which they can shape their organization's culture); REPORT OF THE NACD BLUE RIBBON COMMISSION ON CULTURE AS A CORPORATE ASSET 14-23 (2017) (discussing how boards oversee, and contribute to, an organization's culture); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO 19600 16 (2014) (paragraph, 7.3.2.3, "The development of a compliance culture requires the active, visible, consistent and sustained commitment of the governing body, top management and management towards a common, published standard of behavior that is required throughout every area of the organization."); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT: ALIGNING RISK WITH STRATEGY AND PERFORMANCE, VOL. 1 33 (June 2017) ("It is up to the board of directors and management to define the desired culture of the entity as a whole and of the individuals within it."). Boards and senior executives are often required or encouraged by law to exercise this role. Under the model of an effective compliance and ethics program of the U.S. Sentencing Guidelines, "high-level personnel" (i.e., directors and senior executives) ensure that there is such a program in the organization. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(B) 534 (2016). Organizational scholars explain that an organization's leaders are an important model for the conduct of organizational actors. See, e.g., David M. Mayer et al., *Who Displays Ethical Leadership, and Why Does It Matter? An Examination of Antecedents and*