governance of internal-control functions, it reflects an understanding that organizations should adjust their governance to contextual demands as appropriate.

REPORTERS' NOTE

a. It is recognized that organizations need flexibility in their governance of internal-control functions to reflect their specific circumstances. See generally COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 2 (May 2013) (observing that internal control is flexible and can be adjusted to "the entity's specific needs and circumstances"); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO 19600 5 (2014) (paragraph 4.1, stating that an organization should understand its context in determining its compliance-management system). Small size or limited operations are often determining factors, which require an organization to make accommodations to its governance, such as by outsourcing its internal-control functions or by having a business-line executive also act as a chief compliance officer or a chief risk officer. See, e.g., U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt., application n.2(C)(iii) 536 (2016) (discussing accommodations that small organizations need to make to have an effective compliance and ethics program). Industry-specific requirements, whether in the law or in practice, have an undeniably significant influence upon governance. Large banks, for example, have an increasingly legally mandated structure of governance for compliance, risk management, and internal audit. See, e.g., OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, Standards for Risk Governance Framework, 12 C.F.R. pt. 30, app. D II. (2018) (providing detailed governance requirements on risk management for large insured national banks and other financial firms). While certain nonprofits resemble business firms in the complexity of their operations and governance and may need in-house compliance and risk-management staff, others can handle their internal-control responsibilities with judicious use of an occasional consultant and the assistance of their members. See generally MARILYN E. PHELAN, NONPROFIT ORGANIZATIONS: LAW AND TAXATION § 1.1 (2016) (discussing wide variety of nonprofit organizations).

§ 3.06. Qualifications of Primary Governance Actors for Compliance and Risk Management

(a) The members of the board of directors, executive management, and internal-control officers should:

(1) be independent; and

(2) have the background or experience in compliance and risk management to be able, individually and, when appropriate, collectively, to fulfill their organizational responsibilities over these domains.

(b) To assist them in meeting their obligation under subsection (a)(2), the directors, executive management, and internal-control officers may receive advice and instruction in compliance and risk management, as appropriate and reasonable for those similarly situated in organizations of comparable size and business or affairs, and as tailored to their background, experience, and position in the organization.

Comment:

a. General. Subsection (a) provides that the board of directors, executive management, and internal-control officers should be independent and have the necessary background or experience in compliance and risk management to fulfill their respective organizational responsibilities over these domains. These responsibilities are set forth under § 3.08 (for the board of directors), § 3.14 (for executive management), and §§ 3.15-3.17 (for the primary internal-control officers). The nature of the independence and the level of competence in compliance and risk management differ for individuals in these three groups because of their respective responsibilities. As discussed in Comment *b*, independence varies with one's position in the organization, and the level of competence is expected to be higher when an individual assumes more direct responsibilities over a given subject. For example, directors need not individually be experts or have a background in compliance or risk management. Indeed, this Principle is satisfied if they collectively have sufficient expertise in these subjects. By contrast, senior executives would be expected to be or to become at least minimally competent in compliance and risk management to be able to direct the implementation of those functions in an organization, even if they do not have the level of expertise of a chief compliance officer or a chief risk officer. Moreover, internal-control officers should be professionally competent in compliance, risk management, or internal audit, as may be appropriate, so that they can design their respective internal-control program and manage effectively their respective internal-control department.

This Comment recognizes that the primary governance actors in certain organizations, particularly small ones and nonprofits, may have difficulty completely satisfying this Principle. It may happen that in these organizations no member of the board of directors, senior executive, or internal-control officer has any background in compliance or risk management. Directors may thus have to rely upon an executive, or all the governance actors may have to rely entirely upon the expertise of a third party, in these domains. See § 3.21 (outsourcing an internal-control function). Moreover, the Comment acknowledges that there may be overlapping governance roles for the

primary governance actors in certain organizational forms, such as general partnerships and member-managed limited-liability companies, which will affect their independence. For example, a general partner could not be independent in the same way as most directors on a publicly traded company's board of directors would be.

b. Independence. Subsection (a) identifies three important characteristics or attributes—independence, background, and experience—that enable directors, executive management, and internal-control officers to fulfill their responsibilities properly. The first is "independence," which is defined in § 1.01(aa) to mean "[n]ot … subject to the control … influence or conflict that would prevent an organizational actor from fulfilling his or her role on an organization's behalf." The nature and extent of governance actors' independence depends upon their role in the organization. The independence focus for directors, who generally have full-time executive positions in other organizations, is on whether they are employed by, or have material financial dealings with, the organization if they are responsible for oversight of its internal controls. Independence for the board of directors as a governing body means that its members should collectively have the necessary distance from executive management when supervising internal-control functions. Their independence is sufficient if it enables the directors to pose a credible challenge to executive management on internal-control issues. By contrast, senior executives, such as the chief executive officer and internal-control officers, will not have this kind of independence because they are employees (or, in the case of a third-party service provider, another kind of agent) of the organization. Even if they have other organizational affiliations (e.g., a chief executive officer may be on the board of directors of another organization), independence here means that they act in the interest only of the organization in fulfilling their compliance and risk-management duties. Moreover, independence for internal-control officers suggests that they have the necessary distance from the organization's business or operations that they monitor. See also §§ 3.15-3.17 (recommending that the primary internal-control officers not have other managerial or organizational responsibilities, partly to further the officers' independence).

c. Background or experience. The next two attributes under subsection (a)(2) are related, although not identical. "Background" refers to education and training, while "experience" points to work or other experience, in compliance and risk management. For example, a lawyer who formerly served as a chief compliance officer for a firm may have both background and experience in compliance. This would also be the case, with respect to risk management, for a partner in a

consulting firm who has an MBA and has advised business organizations on risk-management strategies. Background or experience should be suitable for the individual's position in the organization. For example, a director might have no background or experience in compliance and risk management and would have to rely entirely on advice and education on compliance matters from executive management or internal-control officers. A chief executive officer who formerly occupied a similar position in another firm would likely have experience in compliance adequate for the officer's present position. Internal-control officers have often received professional education and training in their respective internal-control subject because compliance, risk management, and internal audit are increasingly recognized as occupations demanding special educational paths and training that prepare one to occupy a compliance, risk-management, or internal-audit professional role. Work or other comparable experience in compliance, risk management, and internal audit also enables individuals to serve competently as internal-control officers. The intent of subsection (a)(2) is to afford flexibility to directors, executive management, and internal-control officers in satisfying the background or experience criterion.

d. Advice, instruction, and continuing education. Subsection (b) identifies ways in which directors, executive management, and internal-control officers may meet their obligation under subsection (a)(2) to have background or experience in compliance and risk management—receiving advice, instruction, and continuing education in the internal-control subject. Again, the nature and the extent of the advice, instruction, and education depends upon the person's position in the organization, as well as upon such factors as the organization's size, legal form, and its industry or sector, and upon the person's background and experience in compliance and risk management. For example, when persons become directors of a publicly traded company, they should be introduced to the major legal or regulatory obligations of the organization, its compliance program and code of ethics, the material risks facing the organization, and its risk-management framework and risk-management program. Depending upon their background and experience, senior executives' or internal-control officers' introduction to some of these matters in these kinds of firms may be unnecessary or can be abbreviated. To take another example, depending upon a nonprofit's size and the nature of its operations, its directors may receive just an occasional report from executive management on a compliance or risk-management issue, or delegate to a committee the responsibility of receiving the necessary advice or instruction to oversee these internal-control functions in the nonprofit.

Directors, executive management, and internal-control officers should also have access to, and may elect to receive, appropriate advice and continuing education in compliance and risk management. Once again, the need for this advice and continuing education depends upon their background, experience, and position in the organization. In particular, internal-control officers may find it useful to receive continuing education in their fields. Programs for this kind of education are readily available to reflect the increasingly professional nature of their occupation.

Organizations should have considerable freedom to decide how they provide this advice, instruction, and continuing education. See § 5.10(b) (discussing how the compliance function provides compliance advice and training). The initial advice and instruction may be part of a new-director or senior-executive orientation, conducted internally, by outside consultants, or in both ways. Similarly, ongoing advice and continuing education on compliance and risk management may occur within the firm, possibly with the assistance of outside counsel and compliance or risk-management professionals, or outside the firm through third-party experts, service providers, organizations, or university programs and institutes.

REPORTERS' NOTE

a. It is well established in the law of organizations, particularly, that of business associations, that members of their governing bodies should be sufficiently independent and competent to be able to perform their oversight duties. Independence has become a legal requirement for the majority of directors of a publicly traded company. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 1003-1005 (2011) (discussing these requirements); NYSE, Inc., Listed Company Manual § 3.03A.01 (2018) ("Listed companies must have a majority of independent directors."); NASDAQ Stock Market Rules § 5605(b)(1) (2018) (same). The New York Stock Exchange's listed-company rules provide that a public-company board must "affirmatively determine that [to be independent] the director has no material relationship with the listed company" and stipulate certain criteria involving conflicts of interest that make a director not independent. See NYSE, Inc., Listed Company Manual § 3.03A.02 (2018) (Independence Tests). See also NASDAQ Stock Market Rules § 5605(a)(2) (2018) (for definition of "Independent Director" and criteria excluding certain directors from meeting this qualification). Competence encompasses a basic ability to understand an organization's affairs, which include its compliance and risk management. This demand for competence is particularly true if a government agency regulates the firm's or organization's internal-control functions. For example, it would be difficult today for one to be a director of a bank or a financial holding company without having a basic understanding of compliance and risk management. See § 3.08, Reporters' Note *a*. Boards and other organizational governing bodies generally have the freedom to attain the necessary expertise in compliance and