Submitted by the Council to the Members of
The American Law Institute
for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019

THE AMERICAN LAW INSTITUTE

Principles of the Law
Compliance, Risk Management, and Enforcement

Tentative Draft No. 1

(April 4, 2019)

SUBJECTS COVERED

CHAPTER 1	Definitions (excluding reserved definitions)
CHAPTER 2	Subject Matter, Objectives, and Interpretation
CHAPTER 3	Governance
CHAPTER 5	Compliance (§§ 5.01-5.08, 5.10-5.17)
APPENDIX	Black Letter of Tentative Draft No. 1

The Executive Office
The American Law Institute
4025 Chestnut Street
Philadelphia, PA 19104-3099
Telephone: (215) 243-1600 • Fax: (215) 243-1636
E-mail: ali@ali.org • Website: http://www.ali.org

As of the date of publication, this Draft has not been considered by the members of The American Law Institute and does not represent the position of the Institute on any of the issues with which it deals. The action, if any, taken by the members with respect to this Draft may be ascertained by consulting the Annual Proceedings of the Institute, which are published following each Annual Meeting.

The American Law Institute

Principles of the Law
Compliance, Risk Management, and Enforcement
Tentative Draft No. 1

Comments and Suggestions Invited

We welcome written comments on this draft. They may be submitted via the website project page or sent via email to PLCERcomments@ali.org. Comments will be forwarded directly to the Reporters, the Director, and the Deputy Director. You may also send comments via standard mail; contact information appears below.

Unless expressed otherwise in the submission, individuals who submit comments authorize The American Law Institute to retain the submitted material in its files and archives, and to copy, distribute, publish, and otherwise make it available to others, with appropriate credit to the author. Comments will be accessible on the website's project page as soon as they are posted by ALI staff. You must be signed in to submit or view comments.

Reporter
Professor Geoffrey P. Miller
New York University School of Law
40 Washington Square South # 411G
Vanderbilt Hall
New York, NY 10012-1005
Email: geoffrey.miller@nyu.edu

Associate Reporters
Professor Jennifer H. Arlen
New York University School of Law
40 Washington Square South # 411D
New York, NY 10012-1005
Email: jennifer.arlen@nyu.edu

Professor James A. Fanto
Brooklyn Law School
250 Joralemon Street
Brooklyn, NY 11201-3798
Email: james.fanto@brooklaw.edu

Professor Claire A. Hill
University of Minnesota Law School
229 19th Avenue South
418 Mondale Hall
Minneapolis, MN 55455-0415
Email: hillx445@umn.edu

Director
Professor Richard L. Revesz
The Executive Office
THE AMERICAN LAW INSTITUTE
4025 Chestnut Street
Philadelphia, PA 19104-3099
Email: director@ALI.org

Deputy Director
Ms. Stephanie A. Middleton
The Executive Office
THE AMERICAN LAW INSTITUTE
4025 Chestnut Street
Philadelphia, PA 19104-3099
Email: smiddleton@ALI.org

Reporters' Conflicts of Interest

The project's Reporters may have been involved in other engagements on issues within the scope of the project; all Reporters are asked to disclose any conflicts of interest, or their appearance, in accord with the Policy Statement and Procedures on Conflicts of Interest with Respect to Institute Projects.

Principles of the Law
Compliance, Risk Management, and Enforcement
Tentative Draft No. 1

REPORTER

GEOFFREY P. MILLER, New York University School of Law, New York, NY

ASSOCIATE REPORTERS

JENNIFER H. ARLEN, New York University School of Law, New York, NY
JAMES A. FANTO, Brooklyn Law School, Brooklyn, NY
CLAIRE A. HILL, University of Minnesota Law School, Minneapolis, MN

ADVISERS

MYTHILI RAMAN, Covington & Burling, Washington, DC
KATHRYN S. REIMANN, Citigroup Inc. (retired), New York, NY
DOUGLAS R. RICHMOND, Aon Professional Services, Overland Park, KS
HILLARY A. SALE, Georgetown University Law Center, Washington, DC
PATTI B. SARIS, U.S. District Court, District of Massachusetts, Boston, MA
JOHN FORD SAVARESE, Wachtell, Lipton, Rosen & Katz, New York, NY
CHARLES V. SENATORE, Fidelity Investments, Boston, MA
KAREN PATTON SEYMOUR, Goldman Sachs & Co., New York, NY
KENNETH S. SIEGEL, Diamond Resorts International Inc., Orlando, FL
NEAL R. SONNETT, The Law Office of Neal R. Sonnett, Miami, FL
LAURA STEIN, The Clorox Company, Oakland, CA
MICHAEL H. ULLMANN, Johnson & Johnson, New Brunswick, NJ
E. NORMAN VEASEY, Gordon, Fournaris & Mammarella, Wilmington, DE
JOHN H. WALSH, Eversheds Sutherland (US), Washington, DC
ROBERT W. WERNER, Green River Hollow Consulting, Hillsdale, NY
BRUCE E. YANNETT, Debevoise & Plimpton, New York, NY
ROBERT ALAN ZAUZMER, U.S. Attorney's Office, Philadelphia, PA
ALLISON ZIEVE, Public Citizen Litigation Group, Washington, DC

LIAISONS

For the American College of Trial Lawyers

ERIC KRAEUTLER, Morgan, Lewis & Bockius, Philadelphia, PA
GRACE E. SPEIGHTS, Morgan, Lewis & Bockius, Washington, DC

MEMBERS CONSULTATIVE GROUP

Principles of the Law, Compliance, Risk Management, and Enforcement
(as of April 04, 2019)

JERRY ANDERSON, Des Moines, IA
JOSÉ F. ANDERSON, Baltimore, MD
CHRISTOPHER EDWARD APPEL, Washington, DC
LARRY CATÁ BACKER, University Park, PA
MARGARET ARMSTRONG BANCROFT, New York, NY
THOMAS C. BAXTER, New York, NY
SHAWN J. BAYERN, Tallahassee, FL
BRIGIDA BENITEZ, Washington, DC
ALAN J. BERKELEY, Washington, DC
BORIS BERSHTEYN, New York, NY
EDWARD K. BILICH, Arlington, VA
HARVEY ERNEST BINES, Boston, MA
JANE BLAND, Houston, TX
RONALD G. BLUM, New York, NY
MATTHEW T. BODIE, Saint Louis, MO
KATHLEEN M. BOOZANG, Newark, NJ
ANDREW S. BOUTROS, Chicago, IL
STEVEN M. BRADFORD, Muscatine, IA
SUSAN E. BROMM, Washington, DC
RUSSELL J. BRUEMMER, Washington, DC
ELLEN M. BUBLICK, Tucson, AZ
JOHN G. BUCHANAN III, Washington, DC
GREGORY P. BUTRUS, Birmingham, AL
IVONNE CABRERA, Downers Grove, IL
FABRIZIO CAFAGGI, Florence, Italy
J. WILLIAM CALLISON, Denver, CO
RUEBEN C. CASAREZ, Houston, TX
RUBEN CASTILLO, Chicago, IL
JONATHAN G. CEDARBAUM, Washington, DC
STEVEN L. CHANENSON, Villanova, PA
JAMES H. CHEEK III, Nashville, TN
ERIC A. CHIAPPINELLI, Lubbock, TX
DONALD EARL CHILDRESS III, Malibu, CA
SYLVIA FUNG CHIN, New York, NY
MARGARET CHON, Seattle, WA
STEPHEN YEE CHOW, Boston, MA
KATHLEEN CLARK, Washington, DC
ANNE E. COHEN, New York, NY
DAVID A. COLLINS, Beverly Hills, MI
PAMELA CRAVEN, New York, NY
ROBERT A. CREAMER, Cambridge, MA
THOMAS L. CUBBAGE III, Washington, DC
CHRISTOPHER SCOTT D'ANGELO, Philadelphia, PA
ALICIA J. DAVIS, Ann Arbor, MI
KIMBERLY A. DEMARCHI, Phoenix, AZ
BRACKETT B. DENNISTON III, Boston, MA
MELANIE DIPIETRO, Greensburg, PA
ANTHONY E. DIRESTA, Washington, DC
ALYSSA A. DIRUSSO, Birmingham, AL
LUCY CLARK DOUGHERTY, Medina, MN
CHRISTINE MICHELLE DUFFY, Parsippany, NJ
SUZANNE M. DUGAN, Washington, DC
STEPHEN S. DUNHAM, University Park, PA
BRIAN J. EGAN, Washington, DC
MITCHELL S. EITEL, New York, NY
E. DONALD ELLIOTT, Washington, DC
J. WILLIAM ELWIN JR., Chicago, IL
ROGER A. FAIRFAX JR., Washington, DC
BORIS FELDMAN, Palo Alto, CA
JEAN K. FITZSIMON, Philadelphia, PA
JOSEPH Z. FLEMING, Miami, FL
ANNE C. FOSTER, Wilmington, DE
VERNON L. FRANCIS, Philadelphia, PA
TAMAR FRANKEL, Boston, MA
MEREDITH FUCHS, Mc Lean, VA
THOMAS P. GALLANIS, Iowa City, IA
BRANDON L. GARRETT, Durham, NC
PHILIP S. GOLDBERG, Washington, DC
M. NORMAN GOLDBERGER, Philadelphia, PA
NORMAN L. GREENE, New York, NY
MICHAEL GREENWALD, Philadelphia, PA
CHARLES E. GRIFFIN, Ridgeland, MS
MICHAEL A. HARRING, Moline, IL
RICHARD E. V. HARRIS, Piedmont, CA
ROBERT M. HART, Bronxville, NY
KATHERINE J. HENRY, Washington, DC
WILLIAM C. HEUER, New York, NY
ERIC L. HIRSCHHORN, Washington, DC
MICHAEL J. HOLSTON, Boston, MA
JOHN E. IOLE, Pittsburgh, PA
KRISTIN N. JOHNSON, New Orleans, LA
RICHARD GIBBS JOHNSON, Cleveland, OH
SUSAN P. JOHNSTON, Mamaroneck, NY
MICHAEL ALEXANDER KAHN, San Francisco, CA
RICHARD B. KATSKEE, Washington, DC
ROBERT R. KEATINGE, Denver, CO
HAROLD H. KIM, Washington, DC
JAMES B. KOBAK JR., New York, NY

DONALD J. KOCHAN, Orange, CA
MICHAEL J. KRAMER, Albion, IN
HILARY K. KRANE, Beaverton, OR
SIMEON M. KRIESBERG, Washington, DC
WILLIAM F. KROENER III, Washington, DC
WILLIAM K. KROGER, Houston, TX
MAUREEN LALLY-GREEN, Pittsburgh, PA
SYBIL H. LANDAU, New York, NY
STEWART M. LANDEFELD, Seattle, WA
PAUL A. LEBEL, Williamsburg, VA
PENINA K. LIEBER, Pittsburgh, PA
CARL D. LIGGIO, Chevy Chase, MD
JONATHAN C. LIPSON, Philadelphia, PA
LYNN M. LOPUCKI, Los Angeles, CA
MARGARET COLGATE LOVE, Washington, DC
ROBERT E. LUTZ, Los Angeles, CA
MYLES V. LYNK, Phoenix, AZ
TIMOTHY D. LYTTON, Atlanta, GA
MEGHAN H. MAGRUDER, Atlanta, GA
PAMELA A. MANN, New York, NY
GARY E. MARCHANT, Phoenix, AZ
COLIN P. MARKS, San Antonio, TX
STEPHEN J. MATHES, Philadelphia, PA
LLOYD H. MAYER, Notre Dame, IN
CATHERINE M. A. MCCAULIFF, Newark, NJ
DON J. MCDERMETT JR., Dallas, TX
PAUL E. MCGREAL, Omaha, NE
JOSEPH MCLAUGHLIN, New York, NY
NANCY A. MCLAUGHLIN, Salt Lake City, UT
KEVIN H. MICHELS, Ewing, NJ
ERICA MOESER, Madison, WI
JONATHAN S. MOTHNER, Stamford, CT
FRED F. MURRAY, Gainesville, FL
DONNA M. NAGY, Bloomington, IN
JOEL W. NOMKIN, Phoenix, AZ
VANCE K. OPPERMAN, Minneapolis, MN
BARAK ORBACH, Tucson, AZ
JOHN E. OSBORN, Chadds Ford, PA
COLIN OWYANG, Rutland, VT
ERIC J. PAN, Washington, DC
JACQUELINE A. PARKER, Stamford, CT
WILLIAM J. PERLSTEIN, New York, NY
JOY LAMBERT PHILLIPS, Gulfport, MS
A. ROBERT PIETRZAK, New York, NY
JACK PIROZZOLO, Boston, MA
ELLEN S. PODGOR, Gulfport, FL
DONALD J. POLDEN, Santa Clara, CA
JEFFREY M. POLLOCK, Princeton, NJ
RAFAEL A. PORRATA-DORIA JR., Bala Cynwyd, PA
JOSEPHINE R. POTUTO, Lincoln, NE
STEVEN A. RAMIREZ, Chicago, IL
BERNARD D. REAMS JR., San Antonio, TX
E. LEE REICHERT III, Denver, CO
HENRY DUPONT RIDGELY, Wilmington, DE
DAN ROBBINS, Calabasas, CA
SUE L. ROBINSON, Wilmington, DE
STEVEN R. RODGERS, Santa Clara, CA
USHA R. RODRIGUES, Athens, GA
BLAKE ROHRBACHER, Wilmington, DE
JEREMY LEDGER ROSS, Seattle, WA
KENNETH ROSS, Midway, UT
VICTORIA P. ROSTOW, Washington, DC
ANJAN SAHNI, New York, NY
MARK E. SCHNEIDER, Chicago, IL
ALEXANDER COCHRAN SCHOCH, Austin, TX
DANIEL SCHWARCZ, Minneapolis, MN
VICTOR E. SCHWARTZ, Washington, DC
VIRGINIA A. SEITZ, Washington, DC
RANDOLPH STUART SERGENT, Baltimore, MD
LEOPOLD Z. SHER, New Orleans, LA
MICHAEL N. SIMKOVIC, Santa Monica, CA
OMARI SCOTT SIMMONS, Winston Salem, NC
MARSHALL L. SMALL, San Francisco, CA
D. GORDON SMITH, Provo, UT
DOUGLAS G. SMITH, Chicago, IL
MARY L. SMITH, Lansing, IL
D. DANIEL SOKOL, Gainesville, FL
PETER Y. SOLMSSEN, Abiquiu, NM
DAVID E. STERNBERG, New York, NY
H. MARK STICHEL, Baltimore, MD
ELIZABETH S. STONG, Brooklyn, NY
ANDREW H. STRUVE, Irvine, CA
GUY MILLER STRUVE, New York, NY
JOHN S. SUMMERS, Philadelphia, PA
KEITH A. SWISHER, Tucson, AZ
SANDRA L. TABOR, Bismarck, ND
LAUREL S. TERRY, Carlisle, PA
PETER D. TROOBOFF, Washington, DC
DANIEL E. TROY, Chevy Chase, MD
FREDERICK TUNG, Boston, MA
THOMAS A. TUPITZA, Erie, PA
E. PETER URBANOWICZ, Sun Valley, ID
BILL WAGNER, Tampa, FL
STEVEN O. WEISE, Los Angeles, CA
CHARLES K. WHITEHEAD, Ithaca, NY
JANE K. WINN, Seattle, WA
PETER A. WINN, Washington, DC
NICHOLAS J. WITTNER, East Lansing, MI
RICHARD J. WOLF, New York, NY
JENNIFER ZACHARY, Kenilworth, NJ
JOSEPH HELDEN ZWICKER, Pittsburgh, PA

The bylaws of The American Law Institute provide that "Publication of any work as representing the Institute's position requires approval by both the membership and the Council."

Each portion of an Institute project is submitted initially for review to the project's Advisers and Members Consultative Group as a Preliminary Draft. As revised, it is then submitted to the Council as a Council Draft. After review by the Council, it is submitted as a Tentative Draft or Discussion Draft for consideration by the membership at an Annual Meeting.

Once it is approved by both the Council and membership, a Tentative Draft represents the most current statement of the Institute's position on the subject and may be cited in opinions or briefs in accordance with Bluebook rule 12.9.4, e.g., Restatement (Second) of Torts § 847A (Am. Law Inst., Tentative Draft No. 17, 1974), until the official text is published. The vote of approval allows for possible further revision of the drafts to reflect the discussion at the Annual Meeting and to make editorial improvements.

The drafting cycle continues in this manner until each segment of the project has been approved by both the Council and the membership. When extensive changes are required, the Reporter may be asked to prepare a Proposed Final Draft of the entire work, or appropriate portions thereof, for review by the Council and membership. Review of this draft is not de novo, and ordinarily is limited to consideration of whether changes previously decided upon have been accurately and adequately carried out.

The typical ALI Section is divided into three parts: black letter, Comment, and Reporter's Notes. In some instances there may also be a separate Statutory Note. Although each of these components is subject to review by the project's Advisers and Members Consultative Group and by the Council and the membership, only the black letter and Comment are regarded as the work of the Institute. The Reporter's and Statutory Notes remain the work of the Reporter.

Principles (excerpt of the Revised Style Manual approved by the ALI Council in January 2015)

Principles are primarily addressed to legislatures, administrative agencies, or private actors. They can, however, be addressed to courts when an area is so new that there is little established law. Principles may suggest best practices for these institutions.

a. The nature of the Institute's Principles projects. The Institute's Corporate Governance Project was conceived as a hybrid, combining traditional Restatement in areas governed primarily by the common law, such as duty of care and duty of fair dealing, with statutory recommendations in areas primarily governed by statute. The project was initially called "Principles of Corporate Governance and Structure: Restatement and Recommendations," but in the course of development the title was changed to "Principles of Corporate Governance: Analysis and Recommendations" and "Restatement" was dropped. Despite this change of title, the Corporate Governance Project combined Restatement with Recommendations and sought to unify a legal field without regard to whether the formulations conformed precisely to present law or whether they could readily be implemented by a court. In such a project, it is essential that the commentary make clear the extent to which the black-letter principles correspond to actual law and, if not, how they might most effectively be implemented as such. These matters were therefore carefully addressed at the beginning of each Comment, as they should be in any comparable "Principles" project.

The "Principles" approach was also followed in Principles of the Law of Family Dissolution: Analysis and Recommendations, the Institute's first project in the field of family law. Rules and practice in this field vary widely from state to state and frequently confer broad discretion on the courts. The project therefore sought to promote greater predictability and fairness by setting out broad principles of sufficient generality to command widespread assent, while leaving many details to the local establishment of "rules of statewide application," as explained in the following provision:

§ 1.01 Rules of Statewide Application

(1) A rule of statewide application is a rule that implements a Principle set forth herein and that governs in all cases presented for decision in the jurisdiction that has adopted it, with such exceptions as the rule itself may provide.

(2) A rule of statewide application may be established by legislative, judicial, or administrative action, in accord with the constitutional provisions and legal traditions that apply to the subject of the rule in the adopting jurisdiction.

Principles of the Law of Family Dissolution: Analysis and Recommendations

Thus, a black-letter principle provided that, in marriages of a certain duration, property originally held separately by the respective spouses should upon dissolution of the marriage be recharacterized as marital, but it left to each State the formula for determining the required duration and extent of the recharacterization:

§ 4.12 Recharacterization of Separate Property as Marital Property at the Dissolution of Long-Term Marriage

(1) In marriages that exceed a minimum duration specified in a rule of statewide application, a portion of the separate property that each spouse held at the time of their marriage should be recharacterized at dissolution as marital property.

(a) The percentage of separate property that is recharacterized as marital property under Paragraph (1) should be determined by the duration of the marriage, according to a formula specified in a rule of statewide application.

(b) The formula should specify a marital duration at which the full value of the separate property held by the spouses at the time of their marriage is recharacterized at dissolution as marital property.

Principles of the Law of Family Dissolution: Analysis and Recommendations

The Comments and Illustrations examined and analyzed the consequences of selecting various possible alternatives.

"Principles" may afford fuller opportunity to promote uniformity across state lines than the Restatement or statutory approaches taken alone. For example, the Institute's Complex Litigation: Statutory Recommendations and Analysis combines broad black-letter principles with the text of a proposed federal statute that would implement those principles.

PROJECT STATUS AT A GLANCE

No portion of this project has previously been submitted for membership approval.

History of Material in This Draft

The Council approved the initiation of this project in October 2015. Earlier versions of Chapter 1 are contained in Council Draft No. 2 (2018); Preliminary Draft No. 4 (2018); Council Draft No. 1 (2018); Preliminary Draft No. 3 (2017); Preliminary Draft No. 2 (2016); and Preliminary Draft No. 1 (2015). Earlier versions of Chapter 2 are contained in Council Draft No. 2 (2018); Preliminary Draft No. 4 (2018); Council Draft No. 1 (2018); Preliminary Draft No. 3 (2017); Preliminary Draft No. 2 (2016); and Preliminary Draft No. 1 (2015). Earlier versions of Chapter 3 are contained in Council Draft No. 2 (2018); Council Draft No. 1 (2018); Preliminary Draft No. 3 (2017); Preliminary Draft No. 2 (2016); and Preliminary Draft No. 1 (2015). Earlier versions of Chapter 5 are contained in Council Draft No. 2 (2018); Council Draft No. 1 (2018); Preliminary Draft No. 3 (2017); Preliminary Draft No. 2 (2016); and Preliminary Draft No. 1 (2015).

Foreword

In 2015, the ALI Council launched Principles of the Law: Compliance, Risk Management, and Enforcement. These topics have emerged as fundamental components of internal controls in complex organizations, both in the United States and around the world. Recent highly publicized settlements of government enforcement actions are visible markers of a significant growth in compliance activities. Other indicators of the importance of these issues are the large increases in hiring in compliance, risk management, and internal audit; enormous attorneys' fees in connection with a foreign corrupt practices investigation; rapid changes at the level of the board of directors with establishment of specialized compliance and risk committees; and attention at the highest levels of government and the private sector to the problem of internal controls, triggered in part by failings in control systems that became evident during the financial crisis of 2007-09.

Corporations, meanwhile, are increasingly adopting their own codes of conduct covering matters as diverse as environmental sustainability, labor rights, human rights, and standards of respect, honest and fair dealing with customers. These company-level norms are often enforced through processes that mirror the formal compliance function. Entities are being called on to encourage ethical and compliant behavior by third parties through systems such as programs of supply chain management, "conflict minerals" disclosures, suspicious activities reports and similar activities.

Principles of Compliance, Risk Management, and Enforcement seeks to provide best practices for a variety of public and private entities but its main audience are large publicly traded corporations. The project is led by Reporter Geoffrey P. Miller of New York University School of Law and three Associate Reporters: Jennifer H. Arlen of New York University School of Law, James A. Fanto of Brooklyn Law School, and Claire A. Hill of University of Minnesota Law School.

This project is coming to the Annual Meeting for the first time, following multiple discussions before the Council, Advisers, and Members Consultative Group. The Reporters will seek approval of Chapter 2, dealing with the overall scope of the project, Chapter 3, on the governance of compliance activities, and portions of Chapter 1 on definitions and Chapter 5 on the performance of the compliance function. Chapters 4 on risk management and Chapter 6 on enforcement, together with the remainder of Chapters 1 and 5, are likely to be before the membership next year.

For the very significant progress on the project so far, I am very grateful to Professors Miller, Arlen, Fanto, and Hill, and to the very dedicated Advisers and Members' Consultative Group.

RICHARD L. REVESZ
Director
The American Law Institute

April 1, 2019

TABLE OF CONTENTS

TOPIC 2. EFFECTIVE COMPLIANCE

TOPIC 3. SPECIFIC COMPLIANCE ACTIVITIES

TOPIC 4. EMPLOYEES, AGENTS, AND COUNTERPARTIES

TOPIC 5. INTERNAL REPORTING

TOPIC 6. THIRD-PARTY SERVICE PROVIDERS

TOPIC 7. INVESTIGATIONS

Principles of the Law: Compliance, Risk Management, and Enforcement

Reporters' Memorandum

This project addresses the need for standards and best practices in compliance, risk management, and enforcement. The project has two parts. The sections on Governance, Compliance and Risk Management relate to internal control (managing the risk that organizations will violate applicable norms); the section on Enforcement relates to external control (enforcing legal requirements through government action). Pending before the membership are parts related to internal control. Chapter 1 contains definitions; Chapter 2 addresses overall scope; Chapter 3 considers the governance of compliance activities; and Chapter 5 deals with the performance of the compliance function. Chapters 2 and 3 have been approved by the Council and are presented in their entirety here. Also pending are parts of Chapter 1 and about half of Chapter 5. The remaining sections will be considered by the Council at a future date.

CHAPTER 1

DEFINITIONS

§ 1.01. Definitions

For purposes of these Principles, the terms set forth herein shall mean the following:

(a) Board of Directors. The individual or group exercising final authority over an organization's internal decisions.

(b) Chief Audit Officer. The head of an organization's internal-audit department.

(c) Chief Compliance Officer. The head of an organization's compliance department.

(d) Chief Executive Officer. The senior-most executive official in an organization.

(e) Chief Legal Officer. The head of an organization's legal department.

(f) Chief Risk Officer. The head of an organization's risk-management department.

(g) Code of Ethics. A written statement that embodies and formalizes the requirements and recommendations of an organization's ethical standards and its code of conduct.

(h) Compliance. Adherence to applicable laws, regulations, rules, or internal requirements.

(i) Compliance Function. The operations, offices, personnel, and activities within an organization that carry out its compliance responsibilities.

(j) Compliance Monitor. An independent third party responsible for assuring compliance with rules or regulations, or with the requirements of agreements settling civil or criminal enforcement actions.

(k) Compliance Officer. An employee working in a professional capacity within an organization's compliance department.

(l) Compliance Policies and Procedures. A statement approved by the board of directors that sets forth an organization's philosophy and general approach to compliance issues.

(m) Compliance Program. A set of specific rules, procedures, authorities, standards, practices, and requirements that implement the compliance policies and procedures within an organization.

(n) Compliance Risk. The risk that an organization will experience financial or reputational losses or legal sanctions or other negative consequences because of its unwillingness or failure to follow laws, regulations, its code of ethics, its ethical standards, or applicable industry codes of conduct, or to cooperate appropriately with regulators.

(o) Deferred Prosecution Agreement. [RESERVED]

(p) Deterrence. [RESERVED]

(q) Duty of Care. The duty to act on an informed and prudent basis with respect to the affairs of an organization.

(r) Duty of Loyalty. The duty not to act in one's own interest, or in the interest of another, to the detriment of the best interests of an organization.

(s) Enforcement Officials. Officials who bring enforcement actions on behalf of a government.

(t) Enterprise Risk Management. [RESERVED]

(u) Ethical Standards. The set of principles, grounded in concerns of morality or the public good, which an organization adopts and declares to be applicable to its employees or agents.

(v) Executive Management. The senior officers of an organization or some subset of such officers.

(w) External Control. A function performed by persons outside an organization that is designed to provide reasonable assurance regarding the achievement of objectives relating to compliance and risk management.

(x) First Line of Defense. An organization's operational managers.

(y) Governance. The process by which decisions relative to compliance and risk management are made within an organization.

(z) Governance Map. A specification assigning responsibility for internal control to persons within an organization.

(aa) Independent. Not part of or subject to the control of any other organization or office and not subject to any influence or conflict that would prevent an organizational actor from fulfilling his or her role on an organization's behalf.

(bb) Informant. A person who reports to an organization's officials about possible wrongful activities by an organization and its employees or agents.

(cc) Inherent Risk. [RESERVED]

(dd) Internal Audit. An internal assurance activity designed to assess whether operations or processes are functioning as designed and whether internal controls are operating effectively.

(ee) Internal-Audit Plan. The policies, procedures, and practices employed by an organization to carry out the task of internal audit.

(ff) Internal-Audit Function. The operations, offices, personnel, and activities within an organization that carry out the task of internal audit.

(gg) Internal Control. A process, implemented by an organization's board of directors, executive management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to compliance and risk management.

(hh) Internal-Control Officer. The chief legal officer, chief risk officer, chief compliance officer, chief audit officer, any of their subordinates, or any other employee charged with carrying out an internal-control function.

(ii) Knowledge. Substantial certainty about a particular fact or state of affairs. Knowledge can be inferred from the circumstances.

(jj) Mandate. A binding obligation imposed by a final judgment or settlement agreement in an enforcement action. [RESERVED]

(kk) Material. Significant, qualitatively or quantitatively, or both, to an organization's reputation, effective functioning, or financial position.

(ll) Misconduct. Any violation of a criminal statute, civil statute, regulation, or mandatory internal rule or standard.

(mm) Nonprosecution Agreement. [RESERVED]

(nn) Organization. A corporation, partnership, limited-liability company, limited-liability partnership, limited-liability limited partnership, professional corporation, business trust, nonprofit corporation, public-benefit corporation, charitable foundation, or other legally constituted entity.

(oo) Organizational Culture. The norms, assumptions, perspectives, and beliefs that guide and govern behavior within an organization.

(pp) Principles. These Principles of the Law, Compliance, Risk Management, and Enforcement.

(qq) Prosecutor. [RESERVED]

(rr) Regulator. [RESERVED]

(ss) Residual Risk. [RESERVED]

(tt) Risk Appetite. [RESERVED]

(uu) Risk-Appetite Statement. [RESERVED]

(vv) Risk Assessment. [RESERVED]

(ww) Risk Capacity. [RESERVED]

(xx) Risk Culture. [RESERVED]

(yy) Risk Limit. [RESERVED]

(zz) Risk Management. [RESERVED]

(aaa) Risk-Management Framework. [RESERVED]

(bbb) Risk-Management Function. [RESERVED]

(ccc) Risk-Management Program. [RESERVED]

(ddd) Risk Tolerance. Acceptable variation in performance, whether exceeding or falling short of the target business objective. [RESERVED]

(eee) Second Line of Defense. The offices and individuals within an organization charged with monitoring the first line of defense to ensure that its functions and processes are properly designed, in place, and operating as intended.

(fff) Third Line of Defense. Internal audit, an independent, objective assurance, and consulting activity designed to add value and improve an organization's operations.

(ggg) Tone. A publicly communicated set of values and norms, expressed in behaviors as well as words.

(hhh) Tone at the Top. The tone set by the board of directors and executive management as to an organization's ethical standards and guiding values.

(iii) Whistleblower. [RESERVED]

CHAPTER 2

SUBJECT MATTER, OBJECTIVES, AND INTERPRETATION

§ 2.01. Subject Matter

These Principles set forth recommendations of best practice for internal control within organizations and external control by regulators, prosecutors, and judges.

Comment:

a. These Principles are concerned with the functions of internal and external control of organizations. Internal control refers to a process, implemented by an organization's board of directors, executive management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to compliance with applicable norms. External control refers to a process, implemented by external public or private entities, designed to ensure that organizations conform to governing norms, or to impose sanctions in cases of noncompliance.

b. These Principles deal with a subject which has evolved rapidly in recent decades. For the most part, this evolution has not been driven by judges or judicial opinions. It has, rather, developed through a variety of sources, including rules and regulations of administrative agencies, agreements settling civil or criminal enforcement actions, best practice guides promulgated by governmental, quasi-governmental, and private parties, and private management decisions by organizations themselves, undertaken either voluntarily or in response to a threat of government action.

For these reasons, unlike some of the Institute's work products, which take the form of Restatements of the Law or statutory proposals, the recommendations of these Principles do not generally summarize the law pertinent to a topic. They are, rather, a set of standards or recommendations that can provide useful guidance about how organizations should structure their internal-control functions and how regulators and prosecutors should respond to these internal-control activities.

c. There is an important international dimension to these Principles. Issues of governance, compliance, risk management, and enforcement are hardly unique to the United States; they confront every country. The recommendations contained herein may appropriately be evaluated in light of practices and norms applicable elsewhere in the world.

REPORTERS' NOTE

a. The concept of internal control is variously defined in different contexts. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: 1. Effectiveness and efficiency of operations. 2. Reliability of financial reporting. 3. Compliance with applicable laws and regulations." COSO, INTERNAL CONTROL – INTEGRATED FRAMEWORK (2013).

Section 13(b)(2)(B) of the Securities Exchange Act of 1934 requires issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that—(i) transactions are executed in accordance with management's general or specific authorization; (ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets; (iii) access to assets is permitted only in accordance with management's general or specific authorization; and (iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences . . . ." 15 U.S.C. § 78m(b)(2)(B).

The Securities and Exchange Commission (SEC) defines the concept of internal control in the context of management's control over financial reporting as "a process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that: (1) [p]ertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant; (2) [p]rovide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and (3) [p]rovide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements." Securities and Exchange Commission, Final Rule on Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, https://www.sec.gov/rules/final/33-8238.htm#P159_33123.

The Department of Justice Criminal Division and the Securities and Exchange Commission Enforcement Division jointly define the concept of internal control over financial reporting under the Foreign Corrupt Practices Act as follows: "the processes used by companies to provide reasonable assurances regarding the reliability of financial reporting and the preparation of financial statements. They include various components, such as: a control environment that covers the tone set by the organization regarding integrity and ethics; risk assessments; control activities

that cover policies and procedures designed to ensure that management directives are carried out (e.g., approvals, authorizations, reconciliations, and segregation of duties); information and communication; and monitoring." Department of Justice Criminal Division and Securities and Exchange Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act, p. 40.

The Department of Justice has been faithful in applying this definition while enforcing the Foreign Corrupt Practices Act. To fulfill the internal-controls term of a recent settlement, the Justice Department required the articulation of a clear and visible compliance policy and executive support of that policy, an extensive risk assessment, criteria for delineating specific compliance duties and ensuring proper training and implementation of the policy by management, an effective system of communication and information gathering from employees to compliance staff and vice versa, and a comprehensive monitoring system of the effectiveness of the compliance program. They have even extended the compliance requirement beyond the above, to agents, business partners, and hires, requiring the inclusion of standard provisions in agreements and contracts that are "reasonably calculated to prevent violations of the anticorruption laws." United States v. Total, S.A., Deferred Prosecution Agreement, No. 13-CR-239, C1-C6 (E.D. Va. May 29, 2013).

b. Although systems of internal control have seen a trend toward increased prominence, the fundamental value of internal controls has long been recognized by regulatory bodies. See Lawrence A. Cunningham, *The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism and Other Ills*, 29 J. CORP. L. 267, 273-274 (2004) (discussing the increased prevalence of internal-control systems within corporations); Statement of Management on Internal Accounting Control, Exchange Act Release No. 15,772, 44 Fed. Reg. 26,702, 26,705 (1979) ("The role of the board of directors in overseeing the establishment and maintenance of a strong control environment, and in overseeing the procedures for evaluating a system of internal accounting control, is particularly important."). It is also important to note the dynamic between regulatory promulgations of valuable compliance mechanisms, and the generally inert response of industry actors, often requiring crises or external enforcement pressures before action is taken.

c. 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"). These Principles do not seek to be detailed frameworks such as the Enterprise Risk-Management Framework by the Committee on Sponsoring Organizations of the Treadway Commission (COSO)—a joint initiative of the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants. (See Reporters' Note 3 to § 4.01 for a listing of some of the major frameworks). Rather, these Principles seek to set forth the principal features of risk-management frameworks and risk-management programs in order to expand on issues particularly related to compliance risk. Risk management was originally developed to deal with financial and business risks, something that is reflected in much of the

broader conceptual apparatus. In particular, concepts such as risk appetite, risk capacity, and risk tolerance embed aggregation, such that more risk in one context may be offset by less risk in another. By contrast, compliance risk, risk arising from the organization's unwillingness or failure to follow laws, regulations, its code of ethics or its ethical standards, or applicable industry codes of conduct, or to cooperate appropriately with regulators, is not appropriately aggregable. That is not to say that no *legal* risks are aggregable. These aggregable legal risks, however, are more akin to business and operational risks, such as risks of changes in law or regulatory regime, of lawsuits being brought against the organization notwithstanding that the organization has acted in good faith, or of adverse governmental action (such as expropriation).

d. There is considerable overlap between risk management and the compliance endeavor, as well as among them and internal audit. Risk is in some respects an overarching concept, insofar as compliance risk is a type of risk. Specifics of compliance are dealt with in the Compliance Chapter; the Chapter on Risk Management discusses special considerations relating to compliance risk *as a type of risk*, and the relationship of compliance risk to risk management generally. The Governance Chapter discusses the responsibilities of the board of directors, executive management, the chief legal officer, the chief risk officer, and the chief compliance officer with respect to risk generally, including compliance risk.

e. For purposes of these Principles, compliance and risk management are both treated as part of internal control. By contrast, in some guidance on risk management, including ENTERPRISE RISK MANAGEMENT: INTEGRATING WITH STRATEGY AND PERFORMANCE, COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, (Sept. 2017), risk management is treated as distinct from internal control, albeit with considerable overlaps. Finally, internal control is sometimes characterized as being part of risk management. See Norman Marks, *Is Risk Management Part of Internal Control or Is It the Other Way Around?,* INTERNAL AUDITOR, May 27, 2013, https://iaonline.theiia.org/is-risk-management-part-of-internal-control-or-is-it-the-other-way-around.

§ 2.02. Objectives

These Principles are intended to promote the following objectives:

(a) fostering compliant, ethical, and risk-aware conduct by organizations and their employees and agents; and

(b) enhancing the effectiveness of internal and external controls.

Comment:

a. A central goal of these Principles is to promote socially desirable conduct by organizations. But organizations, being legal entities, operate only through human beings. These Principles are therefore directed also to the employees and agents of organizations. They provide standards for conduct for these individuals, and also speak to the considerations that enforcement officials, prosecutors, and judges should take into account when deciding on enforcement actions or penalties against an organization's agents or employees.

b. Internal and external controls are beneficial only if they are effective. "Paper" controls that fail to induce compliant conduct accomplish little of value, and may be counterproductive because they can induce those in an organization to be complacent about the effectiveness of controls at deterring illegal or unethical conduct. These Principles are, accordingly, intended to promote internal-control functions that are effective in operation. In some cases, the criterion of effectiveness is explicit in these Principles. An example is § 5.05, which sets forth the elements of an effective compliance function. The criterion of effectiveness, however, is pervasive in these Principles and an implicit goal of all of its recommendations.

c. Cost-effectiveness is an important consideration for internal and external control. Any set of rules and standards governing compliance and enforcement would be self-defeating if the obligations imposed were so onerous that organizations could not operate at all. Accordingly, if the same level of compliant behavior can be achieved through two strategies and one is cheaper than the other, it will usually be appropriate to prefer the cost-effective approach. Moreover, there is an inevitable tradeoff between a compliance function's costs, on the one hand, and its benefits and efficacy, on the other. Although compliance policies are often phrased as adopting a "zero tolerance" approach to violations, no organization can eliminate all misconduct without engaging in prohibitive expenditures. An important goal of these Principles is to facilitate efficient and cost-effective internal-control activities, thus conserving on the resources both of society and of the organizations in question.

REPORTERS' NOTE

a. Effectiveness. The need for effective enforcement is self-evident. For discussion, see, e.g., Anthony G. Hayes, *Making Things Stick: Enforcement and Compliance*, 14 OXF. REV. ECON. POL. 61 (1998); Paul Fenn & Cento G. Veljanovski, *A Positive Economic Theory of Regulatory*

Enforcement, 98 ECON. J. 1055 (1998); Kimberly D. Krawiec, *Cosmetic Compliance and the Failure of Negotiated Governance*, 81 WASH. U. L.Q. 487 (2003).

b. Efficiency. The need for cost considerations, including the cost of compliance, in the design of regulatory strategies is also a ubiquitous theme in the literature on regulation. For an early contribution from the standpoint of economic theory, see George J. Stigler, *The Optimum Enforcement of the Laws*, 78 J. POL. ECON. 526 (1970).

§ 2.03. Characteristics of the Organization

The application of these Principles depends on the facts and circumstances of the organization, which include the following factors, among others:

(a) size;

(b) legal form;

(c) complexity;

(d) geographic scope;

(e) the nature of its business or affairs;

(f) for-profit or not-for-profit status;

(g) history of its compliance violations;

(h) existing obligations arising from settlements of criminal, regulatory, or private enforcement proceedings against it and its employees or agents;

(i) the nature and extent of the regulations applicable to the organization and its business; and

(j) compliance and other risk factors peculiar to its industry or sector.

Comment:

a. These Principles focus primarily on issues of governance, compliance, and risk management for large and/or publicly traded firms. The rationale for this focus is that large organizations tend to face more complex compliance challenges and also tend to have access to resources necessary to address those challenges. The compliance function for large organizations is thus likely to be more extensive than the comparable function for smaller organizations. Larger firms may also have a greater ability to remain current with the most recent thinking and best practices. For these reasons, the large firm presents a model on which smaller firms, nonprofits, religious organizations, and other types of organizations can draw in designing their compliance function, taking into account the fact that substantial modifications will necessarily be required to

adapt to the particular circumstances of the organization. Accordingly, all of the recommendations for internal control contained in these Principles can and should be adapted to the needs of the organization in question.

b. The term "organization" includes corporations, partnerships, limited-liability companies, business trusts, nonprofit corporations, public-benefit corporations, charitable foundations, and other legally constituted entities. These organizations vary greatly in size, ranging from the very small (a few individuals) to the very large (hundreds of thousands of employees). They display significant differences in complexity. They engage in different activities, in different places, posing different risks of violating applicable norms. They are subject to the laws of different countries and jurisdictions. They have different institutional cultures and approaches to institutional ethics.

Given this enormous variation, it is neither possible nor desirable to set forth a set of rules and standards rigidly applicable to all. There is no "one-size-fits-all" rulebook in the field of governance, compliance, risk management, and enforcement. Accordingly, the recommendations and standards set forth in these Principles are general statements of appropriate conduct. In any given case they are subject to modification in light of the facts and circumstances of the particular organization.

One important differentiating factor is the size of the organization. Smaller organizations are unlikely to be equipped to maintain the compliance infrastructure of larger firms. The small size of the organization, however, is not an excuse for avoiding compliance obligations, but rather a reason for fulfilling those obligations through different strategies, policies, and procedures. As stated in the Manual for the Federal Sentencing Guidelines, smaller organizations "may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems." U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. n.2(C)(iii) (U.S. SENTENCING COMM'N 2016).

c. The organization's legal form may also be relevant. For example, public companies face exacting legal and marketplace scrutiny, and accordingly may adopt more formalized approaches to governance, compliance, and risk management than would be appropriate for private firms.

Simple or "shell" organizations, often structured as limited-liability companies or business trusts, may require still a different approach.

d. Complex organizations present greater compliance challenges than simple ones. When an organization operates through numerous subsidiaries or divisions, the challenges of managing an effective compliance program can become daunting. In general, these Principles recommend that complex organizations operate their compliance programs on an enterprise-wide basis in order to reduce the risk that violations "fall through the cracks." However, every organization has its unique structure, and the compliance strategies it undertakes should be adjusted to its particular characteristics.

e. Geographic scope can present special issues for internal control. Organizations doing business in many different countries and many different business cultures will need to design their internal controls in such a way as to take account of this challenge. It may be unrealistic, for example, to expect employees of a division operating in Asia to reach out to the compliance department in the United States if they have a problem; it may be necessary or advisable in such cases to delegate compliance authority to executives "on site," even if the result is some degree of dilution of the organization's ability to manage its internal controls on an enterprise-wide basis.

f. Each business line presents its own set of compliance issues. Companies in the export business face one set of problems; pharmaceutical manufacturers face another; defense contractors face other challenges; and so on. A museum is likely to have different compliance concerns than a not-for-profit university would have. Any general principles of compliance and risk management must take account of the special needs and circumstances of the particular industry or sector involved.

g. The organization's history of compliance violations is a relevant factor. A spotless record may indicate that the organization has an excellent culture of compliance, that it is in an industry presenting a low risk of compliance violations, or that there is some combination of these or other factors. A history of repeated violations may indicate the opposite. Application of these Principles should take into account the individual history and culture of the organization involved. At the same time, the frequency of violations is also a function of the vigor of enforcement: an industry in which enforcement is weak may have few detected violations, but may still present significant compliance problems.

h. In some cases, organizations operate under continuing compliance obligations arising out of the settlement of a civil or criminal enforcement action. The existence of these obligations should be taken into account when applying the recommendations contained in these Principles.

i. Regulatory regimes vary from industry to industry and across states and countries. The application of these Principles will depend in many cases on the nature of the laws and rules to which the organization is subject. Organizations must adhere to legal requirements even if those requirements are at variance with anything in these Principles.

j. Compliance risk varies from industry to industry. Different economic sectors present different risks: for example, the risk of foreign corrupt practices may be low in industries operating primarily within the borders of a single nation; and the risk of antitrust violations may be low when the organization is a small participant in a highly competitive industry. For this and other reasons, these Principles will likely be applied differently across different areas of commerce.

REPORTERS' NOTE

a. Statutes and regulations. The Volcker Rule banning proprietary trading by banking entities explicitly recognizes the need to tailor the internal-control function to the characteristics of the organization. A compliance program must be "appropriate for the types, size, scope, and complexity of activities and business structure of the banking entity." Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Securities and Exchange Commission, Prohibitions and Restrictions on Proprietary Trading and Certain Interests in, and Relationships with, Hedge Funds and Private Equity Funds, 79 Fed. Reg. 5536, 5796 (Jan. 31, 2014).

b. Scholarship and official commentary. Commentators and authoritative sources agree that there is no single specification of the best form of internal controls in all organizations. As the Justice Department and Securities and Exchange Commission put the matter in their Resource Guide to the Foreign Corrupt Practices Act, "the design of a company's internal controls must take into account the operational realities and risks attendant to the company's business, such as: the nature of its products or services; how the products or services get to market; the nature of its work force; the degree of regulation; the extent of its government interaction; and the degree to which it has operations in countries with a high risk of corruption. A company's compliance program should be tailored to these differences." Department of Justice Criminal Division and Securities and Exchange Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act, p. 40.

Other authorities agree about the need for individual tailoring of the compliance function, see, e.g., U.S. Department of Commerce Bureau of Industry and Security Office of Exporter Services Export Management and Compliance Division, Compliance Guidelines: How to Develop an Effective Export Management and Compliance Program and Manual 5 (June 2011) ("Every

organization needs a [compliance program] that uniquely addresses their organization-specific requirements…There is no generic, off-the-shelf, one-size-fits-all [compliance program] that could completely cover the great variety of different industries and business characteristics…How you decide to structure your compliance program will depend on your organization's operations."); Securities and Exchange Commission, Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (2)(B)(3)(d), https://www.sec.gov/rules/final/33-8238.htm#iib3d ("The methods of conducting evaluations of internal control over financial reporting will, and should, vary from company to company. Therefore, the final rules do not specify the method or procedures to be performed in an evaluation."); United States v. Total, S.A., Deferred Prosecution Agreement, No. 13-CR-239, C3 (E.D. Va. May 29, 2013) (noting that the basis for a risk assessment must address the "individual circumstances" of an organization); ETHICS RESOURCE CENTER, BUILDING A CORPORATE REPUTATION OF INTEGRITY 14 (2011), https://rsp.uni.edu/sites/default/files/ERC%20Corporate%20Guide.pdf.

c. The size of the organization can be an important factor in the design of an effective compliance program. As stated in the Compliance Management Review, "in smaller or less complex entities where staffing is limited, a full-time compliance officer may not be necessary. However, management should have clear responsibility for compliance management and compliance staff should be assigned to carry out this function in a manner commensurate with the size of the entity and the nature and risks of its activities." Consumer Financial Protection Bureau, Compliance Management Review 3, https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/052017_cfpb_supervision-and-examination-manual.pdf.

d. As stated in the Federal Sentencing Guidelines Manual, smaller organizations "may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems." U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. n.2(C)(iii) (U.S. SENTENCING COMM'N 2016).

§ 2.04. Interpretation

These Principles should be interpreted in light of the objectives set forth in § 2.02 and the facts and circumstances of the organization listed in § 2.03.

Comment:

a. These Principles should be interpreted in a way that furthers the objectives set forth in § 2.02. For example, as between two possible interpretations that equally serve the goal of promoting compliant and ethical conduct, the preferable interpretation is the one that can be administered effectively at lower overall cost. Moreover, as set forth in § 2.03, these Principles are

designed to provide a general framework that can apply to many kinds of organizations. Because of the wide range of application, the recommendations contained herein should be interpreted in light of the particular facts and circumstances of a given organization and adjusted as appropriate.

§ 2.05. Nonliability

Unless otherwise specifically stated, no recommendation contained in these Principles should be considered as indicating that the law will or should impose liability for conduct that fails to conform to the recommendation.

Comment:

a. These Principles are intended to set forth considerations and suggestions for best practice in the areas of internal and external control. Best practices are evolving standards for managing complex problems. They are not legal requirements and, unless the contrary is explicitly stated or is obvious from the context, should not be considered to indicate that the law will or should impose liability for conduct that fails to conform to the recommendation. Accordingly, these principles alone do not constitute a basis for liability. Whether their adoption as governing norms by an organization or industry group would constitute a basis for liability is outside the scope of this project.

CHAPTER 3

GOVERNANCE

TOPIC 1

GOVERNANCE IN COMPLIANCE AND RISK MANAGEMENT – GENERAL

§ 3.01. Governance in Compliance and Risk Management

Governance is essential to achieving effective compliance and risk management in an organization. Organizations should have flexibility in designing their compliance and risk-management governance.

Comment:

a. As defined in § 1.01(y), governance is "[t]he process by which decisions relative to compliance and risk management are made within an organization." Depending upon the kind of organization, its business or affairs, and other circumstances, compliance and risk management are organizational processes that require certain organizational actors to perform specific tasks. See § 5.01 (noting that compliance includes organizational "operations, offices, personnel, and activities"); § 4.01 (describing risk-management process); § 4.04 (discussing enterprise risk management). Compliance and risk-management programs assign organizational actors their respective responsibilities in these internal-control functions so that the functions are performed efficiently (without unnecessary costs) and comprehensively (leaving no necessary task unassigned). See § 5.06 (specifying compliance-program features); § 4.06 (defining elements of an effective risk-management program). An important part of the programs is the specification of who has decisionmaking authority over, or responsibility for, a particular compliance or risk-management matter or task. See § 5.06(d) (for compliance); § 4.06(b)(5) (for risk management). This specification and the exercise of the authority and responsibility constitute governance. For example, under a larger, for-profit organization's compliance governance, a chief compliance officer may be responsible for designing the compliance program, a chief executive officer decides whether and how to direct its implementation, and the board of directors approves the implementation and periodically reviews the program's effectiveness. Compliance governance may be significantly different in a nonprofit, where, while still being subject to its duty to supervise

the organization, a board of trustees may delegate compliance oversight and implementation to the organization's senior executives, who may in turn use specific staff to perform compliance responsibilities. This Principle reflects the view that organizations should have the flexibility to structure their governance of compliance and risk management as they see fit, within any constraints imposed by law and regulation.

REPORTERS' NOTE

a. As one scholar observes, governance "has to do with the structure of control within an organization. The governance of compliance and risk management in organizations can be complex, involving layers of responsibility and a variety of different offices and positions, with lines of authority projecting in many different ways." See GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 2 (2d ed. 2017). Governance involves specifying these layers and lines of authority or management, while recognizing that, in actual practice, other influences and centers of power may develop. See id. The formal specification of governance is necessary both because it is designed to achieve the most effective compliance and risk management when governance actors are working cohesively and not at cross-purposes, and because it reflects the legal authority of organizational actors. See generally G20/OECD, PRINCIPLES OF CORPORATE GOVERNANCE 9 (2015) ("Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined."); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO 19600 6 (2014) (paragraph 4.4, compliance is supported by principles of good governance).

§ 3.02. Governance Actors

The primary governance actors for compliance and risk management in an organization are its board of directors, executive management, and internal-control officers.

Comment:

a. Depending upon the kind of organization, certain organizational actors govern compliance and risk management in it, even if every actor has a role in these internal-control functions. In a publicly traded company and in an organization of comparable size and operations, such as a large nonprofit, the primary governance actors are typically the board of directors (§ 1.01(a)), executive management (§ 1.01(v)), such as the chief executive officer (§ 1.01(d)), and the internal-control officers, who include the chief audit officer (§ 1.01(b)), the chief compliance officer (§ 1.01(c)), the chief legal officer (§ 1.01(e)), and the chief risk officer (§ 1.01(f)).

Depending upon their position and the organization, they may oversee, direct the implementation of, provide advice for, design, or audit the compliance and risk-management programs. In other words, they make the most important decisions on, and establish the decisionmaking structure for, compliance and risk management in the organization. Within any limitations imposed by law and regulation, an organization should have the flexibility to assign governance responsibilities for compliance and risk management among these parties, or to other employees and agents of the organization. This flexibility is especially necessary if an organization has many or geographically dispersed operations.

REPORTERS' NOTE

a. The governance actors for compliance and risk management are those with the primary legally established decisionmaking authority in an organization, such as a board of directors, senior executives, and internal-control officers. See, e.g., Principles of Corporate Governance: Analysis and Recommendations §§ 3.01 and 3.02 (AM. LAW INST. 1994). They do not include those associated with the organization, such as shareholders of a for-profit corporation or members of a nonprofit, because compliance and risk management, and their governance, are the mission of those directly responsible for the internal control of the organization. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 155 (May 2013). Indeed, the Committee of Sponsoring Organizations of the Treadway Commission describes those primarily responsible for internal control in the following manner:

> The board of directors delegates authority and defines and assigns responsibility to senior management. In turn, senior management delegates authority and defines and assigns responsibility for the overall entity and its subunits. Authority and responsibility are delegated based on demonstrated competence, and roles are defined based on who is responsible for or kept informed of decisions. The board and/or senior management define the degree to which individuals and teams are authorized and encouraged, or limited, to pursue achievement of objectives or address issues as they arise.

See generally COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, supra, at 46. See also id. at 147-152 (describing the internal-control duties of the main governance actors).

§ 3.03. Governance Map for Compliance and Risk Management

It is a best practice for an organization to establish a governance map for compliance and risk management.

Comment:

a. An organization's governance map (§ 1.01(z)) is designed to identify its major compliance and risk-management issues, clearly to assign responsibility for them to organizational actors, and to be part of the compliance and risk-management programs (§ 5.06(d); § 4.06(b)(5)). The chief compliance officer and chief risk officer should help formulate the governance map for their respective internal-control function (§ 3.15(b)(1)(B) and § 3.16(b)(1)(B)). A governance map is a useful tool to assure the person or persons having oversight of compliance and risk management that all compliance and risk-management issues and tasks have been properly assigned to an organizational actor. While such a map may be detailed and elaborate for a publicly traded company with far-flung international operations, it may be simple and informal in a small organization. The map can be in the form of an organizational chart depicting organizational actors with responsibility for compliance and risk management and their relationships. For example, it could identify the responsibilities of compliance officers, the businesses that they oversee, and the executives to whom they report.

REPORTERS' NOTE

a. Depending upon their role, the primary governance actors may design, implement, approve, or review a governance map that sets forth all of the compliance and risk-management responsibilities in the organization. A basic governance map reflects the classic "three lines of defense" for internal control. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 147 (May 2013) (identifying the three lines of defense as (i) management and other front-line personnel, (ii) "business-enabling" internal-control functions, and (iii) internal auditors). Essentially, the map could "delegat[e] to various levels of management the design, implementation, conduct, and assessment of internal control at different levels of the entity…." Id. at 151.

§ 3.04. Coordination of Compliance and Risk Management in Affiliated Organizations

In a group of affiliated organizations, depending upon the structure of that group and legal and practical constraints, the parent organization or another affiliate may find it advisable to coordinate compliance and risk management for the group.

Comment:

a. Organizations, particularly large business firms, may be operated within a group structure of organizations affiliated or related by control or ownership. These affiliates will generally be separate legal entities with their own governance framework and compliance and risk-management programs. In a group structure, compliance problems or the manifestation of risks in one organization could affect the well-being of affiliated organizations in various ways: e.g., the group collectively takes on an excessive amount of a particular kind of risk, even if the level of that risk in any one related organization is not great. Accordingly, if applicable law and practical considerations allow, it may be advisable for one organization in a group to ensure that compliance and risk management are coordinated and group-related compliance and risk-management issues are addressed. See also § 5.04 (discussing enterprise compliance). The parent organization that exercises control over the other affiliates, through its ownership of them and the related power to select some or all of the members of their respective boards of directors, should generally play this role. In other groups, for practical or legal reasons, another affiliate may assume this responsibility, or organizations within the group may coordinate their compliance and risk management. Having an affiliate other than the parent organization act as a coordinator, however, poses a risk of ineffective compliance and risk-management coordination if that affiliate does not have the power fully to gather information from other group affiliates about their compliance and risk management and to ensure that they follow its guidance.

REPORTERS' NOTE

a. Regulators and advisors in the financial sector recognize that large financial businesses can be operated as a group of affiliated firms. They also observe that compliance problems or the manifestation of risk in one or more affiliates can adversely affect the solvency of the entire group, as was seen in certain financial conglomerates during the financial crisis of 2007-2008 with respect to their investments or transactions in mortgage-backed securities. They recommend, therefore, that the parent firm of the group "ensur[e] that there is a clear governance framework appropriate to the structure, business and risks of the group and its entities." See BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS 19 (Oct. 2014) (citing "Principle 5: Governance of group structures"). The recommended group-governance framework, among other things, "addresses risks across the business and legal entity structures," "identif[ies] and address[es] potential intragroup conflicts of interest," and "assess[es] whether there are effective systems in place to facilitate the exchange of information among the various entities, to manage the risks of the separate entities as well as of the group as a whole, and to ensure effective supervision of the group." Id. (paragraph 95). See also BASEL

COMM. ON BANKING SUPERVISION, JOINT FORUM: PRINCIPLES FOR THE SUPERVISION OF FINANCIAL CONGLOMERATES 31 (Sept. 2012) (Principle 21, which "require[s] that an independent, comprehensive and effective risk management framework, accompanied by a robust system of internal controls, effective internal audit and compliance functions, is in place for the financial conglomerate."); id. at 32 (Principle 21(e), "requir[ing] that the board of the head of the financial conglomerate has overall responsibility for the financial conglomerate's group-wide risk management, internal control mechanism, internal audit and compliance functions"). The Board of Governors of the Federal Reserve System echoes this approach to compliance and risk management: "Larger, more complex banking organizations tend to conduct a wide range of business activities that are subject to complex compliance requirements that frequently transcend business lines and legal entities and, accordingly, present risk management and corporate governance challenges." See BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES 2 (Oct. 16, 2008). The Federal Reserve Board mandates that such organizations have "firmwide compliance" that "oversee[s] compliance risk management across the entire organization, both within and across business lines, legal entities, and jurisdictions of operation." Id. at 3.

§ 3.05. Governance Accommodations for Organizational Circumstances

An organization should structure the governance of its internal-control functions of compliance, risk management, and internal audit to reflect its size, legal form, industry-specific requirements, nonprofit status, potential harm caused by a violation or a failure of, or deviation from, an internal-control program, or other circumstances.

Comment:

a. This Principle, which is echoed by other Principles in this Chapter (see, e.g., § 3.20 and § 3.21), underscores that an organization should have the flexibility to adjust the governance of its internal-control functions to reflect its circumstances. A small firm may find it efficient to outsource its internal-audit function and thus its chief audit officer; a registered broker-dealer must have a chief compliance officer, although an outsider may fill that position; and a nonprofit organization's board of trustees may decide to deal with risk management through an ad hoc committee of board members, executives, and consultants. An organization may also give its compliance officers a visible role because the potential harm, both legal and reputational, to the organization from legal violations committed by employees could be devastating. Although Chapter 3 presents Principles that are based upon best practices and, in some cases, the law on the

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

risk management, as in other subjects, in a collective way, i.e., through the entirety of their members. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1003. One or more members may have particular expertise in these subjects. See § 3.09, Reporters' Note *b*. As further shown by the board committees presented in §§ 3.09-3.13, a director may gain expertise in these subjects from being a member of a specialized board committee devoted to them.

The requirement that members of executive management be independent in matters of compliance and risk management arises from their basic fiduciary duties to their organizations. See, e.g., Gantler v. Stephens, 965 A.2d 695, 708-709 (Del. 2009) (holding that officers owe the same fiduciary duties as directors). Their competence in the internal-control functions would presumably be greater than that of directors because they are responsible for directing the implementation of compliance, risk management, and internal audit in their organization. See § 3.14, Reporters' Note *a*. Similarly, internal-control officers should have considerable expertise in their respective internal-control functions, given their responsibilities for designing the compliance program, the risk-management framework and program, and the internal-audit plan. See §§ 3.15-3.17, Reporters' Notes. As for the independence of internal-control officers, issues and conflicts of interest may arise when an internal-control officer also has a business role. See § 3.20, Reporters' Notes *a* and *b*.

b. This Principle's emphasis on background and experience reflects the two common ways in which people gain competency and expertise in a given subject—by education and through experience. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO 19600 15 (2014) (paragraph 7.2.2, "The attainment of competence [in compliance] can be achieved in many ways, including skills and knowledge required through education, training or work experience."). These methods are not always separate: for example, as part of formal training in compliance, a person could do an internship in a compliance department and thus gain work experience in that subject. Internal-control officers may be expected to hold specific educational degrees (e.g., CPA for the chief audit officer). Certification programs and advanced degrees that impart basic knowledge of the field exist in compliance as well. See, e.g., Certified Regulatory and Compliance Professional designation (obtained through academic training at the McDonough School of Business at Georgetown University, in conjunction with the Financial Industry Regulatory Authority, http://www.finra.org/industry/finra-institute-georgetown).

c. This Principle underscores that directors, senior executives, and internal-control officers may satisfy their obligation to become sufficiently expert in compliance and risk management through receiving advice and instruction on these subjects. In addition to past training and education, this advice and instruction can occur before or after a person has assumed the role in question, whether in the form of an initial "boot camp" or continuing advice and education. Law and regulation generally deal indirectly with these issues. For example, members of executive management and internal-control officers may be required to have continuing education as a requirement for maintaining a license in a regulated area. See, e.g., Continuing Education, http://www.finra.org (describing continuing education requirements for, among others, registered

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*

Consequences of Ethical Leadership, 55 ACAD. MGMT. J. 151, 153-154 (2012). If the leaders' words and actions run counter to the organization's compliance policy, code of ethics, and risk culture, this could breed cynicism among its employees, who will regard the policy, code, and risk culture with skepticism. Organizational culture is understood to be the necessary foundation to effective compliance and risk management. See generally David Hess, *Ethical Infrastructures and Evidence-Based Corporate Compliance and Ethics Programs: Policy Implications from the Empirical Evidence*, 12 N.Y.U. J. L. & BUS. 317 (2016) (arguing that a compliance program must be aligned with the organization's culture to have legitimacy in the eyes of the organization's employees). The Board of Governors of the Federal Reserve System states that "[b]oards of directors are responsible for setting an appropriate culture of compliance within their organizations, for establishing clear policies regarding the management of key risks, and for ensuring that these policies are adhered to in practice." See BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES 7 (Oct. 16, 2008).

b. Directors and senior executives can promote and support the organizational culture in many ways. See generally ETHICS & COMPLIANCE INITIATIVE, PRINCIPLES AND PRACTICES OF HIGH-QUALITY ETHICS & COMPLIANCE PROGRAMS: REPORT OF ECI'S BLUE RIBBON PANEL 26-27 (2016) (discussing ways for leaders to "model integrity" and otherwise to build a strong ethical culture). Subsection (b) lists four of them, which represent several significant and general ways that legal and nonlegal sources highlight. See Linda Klebe Trevino, et al., *Legitimating the legitimate: A grounded theory of legitimacy work among Ethics and Compliance Officers* 123 ORGAN. BEHAV. & HUMAN DECISION PROCESSES 186, 195 (2014) (discussing importance of support for compliance by an organization's board and senior executives). More specific responsibilities regarding compliance and risk management are cited and discussed in other Principles, see § 3.08 and § 3.14, and depend upon organizational circumstances. For example, a chief executive officer could introduce the training session on compliance for employees, which would reinforce among them the importance of compliance in the organization.

c. Legal and other authorities recognize that directors and senior executives should collaborate to produce the organization's overall approach towards compliance policies, ethical standards, and risk culture. This generally means that executive management directs the formulation and implementation of compliance policies, a risk-management framework, and a code of ethics for the board's approval. See, e.g., U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(B), supra, at 534 (stating that "high-level personnel" are responsible for ensuring that there is an effective compliance and ethics program); BASEL COMM. ON BANKING SUPERVISION, BCBS NO. 113, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS 9-10 (2005) (Principles 2-4, which stipulate that senior management establishes the compliance policy). While senior executives articulate the values embodied in the compliance policies and the risk culture in the risk-management framework, the board should actively approve, not passively accept, them. See BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS 10 (2014). If directors conclude that the

organization should adopt different compliance values or a different risk culture, they should direct management to implement them. See, e.g., OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations and Insured Federal Branches, 12 C.F.R. part 30, app. D, II.D. (2018) (discussing role of boards and senior executives in adopting strategic risk-management plan).

d. It is well established that an organizational culture of compliance and sound risk management is shown by, and is the foundation for, the firm's practices. That is, if the organization's culture is weak, noncompliance with the law, ethical violations, and failures to follow risk limits generally follow. See David Hess, *Ethical Infrastructures and Evidence-Based Corporate Compliance and Ethics Programs: Policy Implications from the Empirical Evidence*, 12 N.Y.U. J. L. & BUS. 317, 360 (2016) (discussing research showing that a weak ethical culture produces more unethical conduct than the complete absence of such a culture). Compensation practices are often used as an indication of how well an organization's activities are aligned with its culture of compliance and risk management. Certain compensation practices that are seen to reinforce effective compliance and risk management are discussed in § 5.16, Reporters' Note *b* (Compensation). See also BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES, supra, at 7 (stating that the board of a large banking organization should make sure that incentive structures promote compliance); OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations and Insured Federal Branches, 12 C.F.R. part 30, app. D, II.M (2018) (discussing compensation practices); BASEL COMM. ON BANKING SUPERVISION, CORPORATE GOVERNANCE PRINCIPLES FOR BANKS, supra, at 30 (Principle 11, discussing relationship between compensation structure and risk management).

e. Legal authorities and guidelines on compliance and risk-management practices emphasize that the board of directors and senior executives foster organizational culture by selecting employees and agents who are likely to adhere to compliance values, ethical standards, and risk culture. See, e.g., U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(3), supra, at 534 (providing that "substantial authority personnel" should not include those who have "engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program"). The Office of the Comptroller of the Currency provides that, with respect to risk management, the board (or a board risk committee) must "manage talent," which means that it must appoint senior management and internal-control officers who have the skills to carry out their risk-management responsibilities and to require management to place appropriate people in the risk-management program. See OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations and Insured Federal Branches, 12 C.F.R. part 30, app. D, II.L. (2018) (providing the same responsibilities for the chief executive officer). Directors can be held responsible for compliance or ethical failures committed or condoned by an executive whom they oversee when they were on notice that the executive had previously engaged in illegal or unethical conduct. See, e.g., In re Massey Energy Company, 2011 WL 2176479 (Del.

Ch. May 31, 2011) (discussing derivative claims against Massey board for, among other things, their oversight of a chief executive officer who condoned, and engaged in, illegal conduct).

f. Regulators often refer to the importance of the "tone at the top" and urge board members and top executives to exhibit it. See, e.g., Richard G. Ketchum, Chairman and Chief Executive Officer, FINRA, "Remarks From the 2016 FINRA Annual Conference" (May 23, 2016) ("The board, the CEO, business leaders and the CCO all play critical roles in setting the tone at the top and establishing an organization's values and ethical climate."). They are pointing to how words and actions by the members of the highest legal authority and senior executives create and promote the organizational culture. See Gary R. Weaver & Linda Klebe Trevino, *Compliance and Values Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior,* 9 BUS. ETHICS Q. 315 (1999) (supporting this proposition). These words send a strong signal to managers, employees, and other organizational actors that, if they violate the law or organizational values, they will be caught and punished. See generally Donald C. Langevoort, *Cultures of Compliance*, 54 AM. CRIM. L. REV. 933, 966-967 (2017) (underlining the importance of board members and officers in promoting ethical conduct, but emphasizing the individual and institutional pressures that run counter to this promotion). The pronouncements and actions by directors and senior executives may also lead those outside the organization to understand that it is committed to compliance with the law and with extra-legal norms and to a sound risk culture.

TOPIC 2

THE BOARD OF DIRECTORS – GENERAL

§ 3.08. Board of Directors' Oversight of Compliance, Risk Management, and Internal Audit

(a) As part of its supervision of the organization's business or affairs, the board of directors must oversee the organization's compliance, risk-management, and internal-audit functions.

(b) The oversight in subsection (a) should include the following responsibilities:

(1) to be informed of the major legal obligations of, and the main values in the code of ethics for, the organization, its employees, and agents;

(2) to review and approve the organization's compliance program and code of ethics, any material revisions thereto, and their implementation;

(3) to be informed of the material risks to which the organization is or will likely be exposed;

(4) to review and approve the organization's risk-management framework and risk-management program, any material revisions thereto, and their implementation;

(5) to review and approve the internal-audit plan for compliance and risk management, and any material revisions thereto, and be reasonably informed of the results of the internal audit of these internal-control functions;

(6) to be reasonably informed of the staffing and resources allocated by executive management to the internal-control departments of compliance, risk management, and internal audit, and to satisfy itself that the staffing and resources are adequate and that the departments are sufficiently independent and have the appropriate authority to perform their respective internal-control responsibilities;

(7) to approve the appointment, terms of employment, and dismissal of the chief compliance officer, the chief risk officer, and the chief audit officer;

(8) to communicate regularly with these internal-control officers;

(9) to meet at reasonable intervals with executive management and each of the appropriate internal-control officers to review the effectiveness of, inadequacies in, and any necessary changes to the internal-control function headed by that officer;

(10) to confer with executive management, the chief legal officer, and the appropriate internal-control officer or officers:

(A) to address any material violation or failure of the compliance program and code of ethics, material deviation from or failure of the risk-management program, or material failure in the internal audit of compliance and risk management, and

(B) to approve or ratify any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation, failure, or deviation; and

(11) with the assistance of the chief legal officer, the appropriate internal-control officer or officers, outside legal counsel, or outside consultants:

(A) to direct its own investigation of any material violation or failure of the compliance program and code of ethics, material deviation from or failure of the risk-management program, or material failure in the internal audit of compliance and risk management,

(B) to resolve upon any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such violation, failure, or deviation, and

(C) to direct executive management to develop a plan of action for responding to any future such violation, failure, or deviation.

(c) Subject to subsection (a) and if authorized under the law governing the organization, the board of directors, in its discretion, may delegate to a group or committee of its members, to a joint committee of directors and executives, or to executive management the power to perform one or more of the responsibilities set forth in subsection (b).

Comment:

a. General. Under well-established law applicable to most organizations, the board of directors is responsible for the oversight of an organization's business or affairs. Subsection (a) provides that this oversight must include the organization's compliance with laws, regulations, and its code of ethics, identification and management of its risks, and internal audit. See § 5.05(b) (support from and oversight by the organization's board of directors are included as an element of an effective compliance function). The board of directors, however, does not generally direct the implementation of an internal-control program. Rather, executive management, especially the chief executive officer, with the assistance of internal-control officers, proposes compliance and risk-management programs and the internal-audit plan for the board's approval and then, having received it, has the programs and plan put into place. The directors are expected to understand generally the internal-control programs and plan and the reasons for their content, design, and justification, actively to engage with executive management and internal-control officers in learning and asking questions about the programs and plan, and to approve them only in the exercise of their good faith and reasonable judgment. This Principle sets forth an aspirational standard of conduct for the board of directors and is not meant to establish a standard of liability. This Principle also assumes that, within any limitation imposed by law and regulation governing the organization, the board has discretion and flexibility as to how to conduct its oversight of compliance and risk management, as is further emphasized in subsections (b) and (c).

b. Oversight responsibilities; general. Subsection (b) enumerates a nonexclusive list of the key responsibilities that the board of directors should undertake in its oversight of compliance, risk management, and internal audit. Many, if not most, of these characterize board oversight in a

publicly traded company and are in fact mandated by applicable law. This Principle is thus appropriate for a publicly traded company or other organization of comparable size and operations. In other contexts, a board may choose to undertake only certain aspects of these responsibilities or other responsibilities, or it may delegate many of them to a board committee, a committee of directors and executives, or executives, as provided by subsection (c).

c. Oversight responsibilities; compliance. Subsection (b)(1) stipulates that the board should be informed of the major obligations under the law and code of ethics applicable to the organization, its employees, and its agents. Section 3.06 explains some of the ways by which the directors acquire that information. It is expected that senior executives, the chief legal officer, and the chief compliance officer advise the board on these legal and ethical obligations, and on the risks arising from noncompliance with them. See § 1.01(n) (definition of compliance risk). The limitations language ("informed of the *major* legal obligations … and [of] the *main* values") (emphasis added) suggests that the directors should receive the kind of high-level information about significant obligations and risks that is appropriate for those acting in an oversight role.

Subsection (b)(2) provides that the board of directors should review and approve the compliance program and the code of ethics, although it may well delegate this task to a board committee, a committee composed of directors and executives, or senior executives, as provided in subsection (c). The program (which includes the compliance policies and procedures, § 1.01(l)) and code are defined in § 1.01(m) and § 1.01(g) and their features are set forth in § 5.06 and § 5.37, respectively. Under § 3.14, executive management brings before the board the compliance program and the code of ethics, formulated with the assistance of the chief compliance officer under § 3.15, for the board's approval. Because not all organizations have a code of ethics, an organization's ethical standards may be embodied in the compliance policies and procedures or may just be informal guidelines. Since by its terms the compliance program assigns responsibility for compliance to organizational actors, see § 3.03 (discussing the governance map for compliance and risk management), the board of directors also reviews and approves the governance of compliance—the chain of decisionmaking and responsibilities applicable to this internal-control function and its structure in the organization.

As follows from the above discussion, the board of directors is not expected to design the compliance program, the code of ethics, and the structure of the governance of compliance, and need not understand them at the level of detail expected of executive management and the chief

compliance officer. To be able to approve them, however, the directors should have a basic understanding of the ways in which the compliance program identifies and addresses compliance risks and issues and structures the organization's compliance governance. In other words, their "review" presupposes this understanding. The board should also be expected to review and approve major and significant revisions to the compliance program and the code of ethics.

d. Oversight responsibilities; risk management. Subsection (b)(3) clarifies that the board of directors should also be informed and thus have a basic understanding of the material risks (those in addition to legal and compliance risks that are dealt with in subsections (b)(1) and (b)(2)) to which the organization is or will likely be exposed. See § 4.05 (discussing classification of risk). This understanding could come from their background, experience, and education, as explained in § 3.06, with advice and education provided by the chief risk officer under § 3.16, and from meetings with executive management, as provided in § 3.14. Subsection (b)(4) recommends that the directors should also review and approve the organization's risk-management framework, § 1.01(aaa), including its risk-appetite statement, § 1.01(uu), if one is prepared, and the risk-management program that implements this framework, § 1.01(ccc) (definition of a risk-management program) and § 4.06 (identifying program elements). They should similarly review and approve the structure of governance of risk management. Here, again, executive management, with the assistance of the chief risk officer, is responsible for directing the formulation of the organization's risk-management framework and program, and for presenting, explaining, and justifying them to the board of directors. Even so, directors should not passively accept the framework and program as proposed by executive management. Rather, they should understand the risk-management framework and program and satisfy themselves that the kinds and levels of risk, particularly the residual risk, § 1.01(ss), are reasonable in light of the organization's business and affairs and that the framework and program, if implemented, would adequately manage them. The directors should also approve any material revisions to the risk-management framework and program.

e. Oversight responsibilities; internal audit. Subsection (b)(5) underscores that the board of directors should review and approve the internal-audit plan, § 1.01(ee), as it applies to compliance and risk management and the governance of internal audit. In particular, the directors should understand how this plan proposes that the internal auditors check on the effectiveness of the compliance and risk-management functions. Under § 3.17, the chief audit officer designs the

internal-audit plan and structures its governance with the assistance of internal auditors. Because internal audit is the critical "third line of defense" for compliance and risk management (§ 1.01(fff)), the board's oversight of these internal-control functions should include a basic understanding of internal audit's contribution to them. The board should also be informed of the results of the internal audit of compliance and risk management and the modifications to the internal-control functions recommended by the chief audit officer pursuant to § 3.17(b)(8)(D).

f. Oversight of the staffing, resources, independence, and authority of the internal-control departments. Subsection (b)(6) provides that the board of directors should be reasonably informed of the staffing and resources that executive management allocates to the internal-control departments. Because staffing and resources are managerial matters, see § 3.14(b)(6), the board would expect to receive a justification from executive management that they are adequate for the proposed tasks of these departments. The board should also be satisfied that the internal-control departments have the necessary independence and appropriate authority to perform their tasks. Independence of these departments and of the chief internal-control officers is emphasized throughout these Principles. See, e.g., § 5.05, Comment *f* (discussing independence of the compliance function); § 4.06, Comment *e* (discussing independence of the risk-management personnel). In addition, the board would be expected to receive assurance that internal-control officers have the appropriate authority so that organizational actors listen to and are guided by them on internal-control matters.

g. Oversight of the appointment, terms of employment, and dismissal of, and communications with, internal-control officers. Subsections (b)(7) and (b)(8) reflect the two meanings of organizational reporting with respect to the chief compliance officer, the chief risk officer, and the chief audit officer. These officers may be members of executive management who "directly report" to, and would thus be under the direct line of authority of, the chief executive officer, who would then ordinarily propose persons for those positions and decide when to terminate them. Alternatively, they may be lower in the organization's hierarchy and be a direct report to another member of executive management (or to an officer under executive management). In any of these cases, under subsection (b)(7), the board of directors approves the hiring, terms of employment, and dismissal of these internal-control officers. This approval of their engagement, and particularly their dismissal, is designed to provide another layer of oversight to these personnel actions and helps ensure that the officers are not terminated merely for having

raised an important internal-control-related issue in the organization. Although not specifically mentioned by the subsection, "terms of employment" includes these internal-control officers' compensation.

Subsection (b)(8) highlights that these internal-control officers may communicate, in the sense of providing information, directly and regularly with the board of directors (or a designated director or group of directors); this is the other meaning of organizational reporting. This communication would be separate from and independent of that officer's informational reporting to the chief executive officer and other members of executive management. It enables the board to conduct its oversight better by hearing directly from an internal-control officer without the communication being filtered or influenced by other members of executive management. The board itself determines the scope and frequency of any such communication and reporting, but its regularity helps ensure that no unintended negative signal is sent by a meeting between the officer and the board, which signal might occur if this kind of meeting took place only if the board or officer requested it.

h. Review of the effectiveness of internal-control functions. Subsection (b)(9) provides that the board of directors should review at reasonable intervals the effectiveness of compliance, risk management, and internal audit to determine whether the internal-control functions have been properly implemented and are operating effectively and to discuss any necessary changes to them. See § 5.06(o) (providing, as one feature of a compliance program, periodic review and reaffirmation by the board). While the focus of the review is on the compliance program, the risk-management program, and the internal-audit plan, the overall concern is how well the internal-control functions are operating and whether there are inadequacies in them that need to be addressed. For example, if it comes to the board's attention that their company has made frequent large cash payments to foreign accounts without an apparent business reason, the board would be on notice that the company's internal controls are not operating properly, are not effective, and are thus in need of substantial revision. The board determines how frequently each such review should occur. The review of an internal-control function could take place following the assessment of it conducted by executive management with the appropriate internal-control officer, as provided in § 3.14(b)(9). Executive management and the internal-control officer might report on the results of the assessment to the board, especially if the assessment revealed inadequacies in, and recommended modifications to, the compliance program or the risk-management program. A

periodic review of the effectiveness of the internal-control functions also affords the board a good opportunity to learn of any recent significant legal developments, and of any new material risks, facing the organization, and to consider how the compliance and risk-management programs, and the related internal-audit plan, will address them.

i. Decisions on material violations or failures. Under subsection (b)(10), the board of directors confers with executive management, the chief legal officer, and the appropriate internal-control officer or officers about any material violations or failures of, or material deviations from, the internal-control frameworks and approves or ratifies any material remedial and disciplinary measures taken or to be taken, including reporting made or to be made to a regulator, with respect to such violations, failures, or deviations. See § 5.30(c) and Comment *c* (reporting results of internal investigations to the government); § 6.09, Comment *a* (the importance of an organization's self-reporting of misconduct); § 6.15 (on organizational remediation and restitution); § 6.16(e)(4) (enforcement authorities' assessment of an effective compliance program includes "whether the organization promptly reported any detected material misconduct"). This subsection is the counterpart to § 3.14(b)(11)(D), which requires executive management to report on these issues to the board. The material violation or failure of the organization's compliance program or code of ethics, material deviation from or failure of its risk-management program, or material failure of the internal audit should be brought to the attention of the board of directors, which, as the ultimate supervisory body within the organization, should authorize the organization's response to these events (or ratify it if circumstances required executive management to take immediate action), as the following example demonstrates:

> Board of pharmaceutical company receives notice of widespread violations of the law governing the marketing of pharmaceutical products by company sales agents for uses other than those approved by the Food and Drug Administration. Board is expected to approve the company's response to this notice, which would include stopping the illegal activity, enhancing the company's compliance program, and increasing its oversight of the company's marketing.

By the same token, the board should not have to review immaterial violations, failures, or deviations that executive management or the appropriate internal-control officer could address, unless a pattern of these violations, failures, or deviations indicates a potentially serious problem or breakdown in the compliance or risk-management program. The board should also approve the

material remedial or disciplinary measures, which could range from clawbacks of compensation from organizational actors who contributed to the violations, failures, or deviations to recompense to third parties injured as a result. The chief legal officer should be included in the board deliberations because that officer is responsible for legal advice on the organization's response to any material violation, failure, or deviation.

j. Crisis response. Subsection (b)(11) differs from subsection (b)(10) insofar as the latter deals with the approval or ratification by the board of the organization's response to material violations or failures of, or material deviations from, the internal-control programs that executive management generally proposes, whereas, under the former, the board is itself initiating an investigation into the internal-control matter and deciding upon the response to it. See § 5.24 (the organization's decision to conduct an investigation). This subsection thus deals with exceptional circumstances, or a crisis, in compliance and risk management in the organization. This could occur, for example, when the chief executive officer, other senior executives, or directors are themselves implicated in the material violations, failures, or deviations, or a widespread breakdown in compliance or risk management has occurred in the organization that is suggestive of fundamental problems in their governance. These crises often result in civil investigations by regulators and criminal proceedings by federal and state prosecutors. In such circumstances, as provided in subsection (b)(11)(A), the board could enlist the assistance of the organization's internal-control officers, but it could also, or alternatively, seek the help of outside counsel and consultants to ensure that any investigation is independent and thus not tainted by any organizational actors who might want it to be limited in scope. As in the case of subsection (b)(10), under subsection (b)(11)(B) the board can resolve upon any disciplinary or remedial measures to respond to the material violation, failure, or deviation, which could include in these kinds of situations removal of senior executives, significant reduction of their compensation, or a wholesale revamping of the compliance or risk-management program. Failure to respond adequately in these circumstances may lead to externally imposed limits on the board's own oversight of compliance and risk management. See § 6.18(d)(3) (providing for external oversight through a monitor in circumstances where the board of directors, among others, failed to respond to misconduct in the organization); § 6.19 (compliance monitors).

Subsection (b)(11)(C) provides that the board of directors may find it useful to direct executive management to develop a plan of action for future compliance or risk-management crises

(a "crisis plan"), while recognizing that many crises are unexpected and even unforeseeable. Because these events could seriously harm the organization, time is often of the essence in the organization's response to them. Accordingly, the board may find it advantageous to have executive management promulgate policies and procedures that would outline organizational conduct in the event of a crisis. It could direct senior executives, with the assistance of internal-control officers, to prepare the crisis plan, or it could delegate this task to an outside consultant. Among other things, the policies and procedures would define events that trigger the crisis plan (e.g., involvement of senior executives in the violation, revelation of widespread illegal practices in the organization). They would also assign crisis roles (e.g., organizational spokesperson, contact with regulators) to organizational actors, particularly to directors, board committees, and outside consultants and counsel. In addition, the policies and procedures would outline how specific organizational action occurs, including, for instance, the steps for an investigation to take and the status of those accused of involvement in the material violation, failure, or deviation. Those assigned roles in a crisis plan could thus be educated as to their responsibilities in a crisis before one actually occurs. The crisis plan could even provide for a periodic crisis simulation where organizational actors play out their roles in a hypothetical crisis in order to test the effectiveness of the plan and to identify needed improvements to it.

k. Delegation to groups or committees. Subsection (c) provides that, while, under subsection (a), the board of directors is ultimately responsible for the oversight of compliance, risk management, and internal audit, it may decide, if authorized under the law governing the organization, to delegate one or more of the responsibilities listed in subsection (b) (or others) to a group or committee of its members, a committee of directors and executives, or simply senior executives. Indeed, as the practice in publicly traded companies and other large organizations demonstrates and as provided elsewhere in these Principles, see §§ 3.10-3.12, a board committee is often charged with the oversight of an internal-control function (or functions). Subsection (c) approves this delegation because it enables certain directors to become more knowledgeable about specific internal-control functions and promotes more competent and effective oversight of them. This subsection also reflects the view that the board should have flexibility in fulfilling its oversight of internal control.

REPORTERS' NOTE

a. It is well established in the laws governing different kinds of business organizations that the board of directors of a particular organization has oversight responsibility over all the organization's activities. This has been read to include oversight over compliance, risk management, and internal audit, and courts generally defer to the board's business judgment with respect to this oversight. See, e.g., In re Caremark International Inc. Derivative Litigation, 698 A.2d 959, 970 (Del. Ch. 1996) ("a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists"); Stone v. Ritter, 911 A.2d 362 (Del. 2006) (accepting that board's oversight obligation includes the responsibility to ensure that the corporation has an adequate compliance function); In re Citigroup Inc. Shareholder Derivative Litigation, 964 A.2d 106, 124-126 (Del. Ch. 2009) (reasoning that business judgment rule is particularly protective of a board facing a claim of oversight failure with respect to its oversight of business risks); In re Goldman Sachs Group, Inc. Shareholder Litigation, 2011 WL 4826104, at 22 (Del. Ch. Oct. 12, 2011) ("If an actionable duty to monitor business risk exists, it cannot encompass any substantive evaluation by a court of a board's determination of the appropriate amount of risk. Such decisions plainly involve business judgment.") (footnote omitted). See also ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 986 (2011) (discussing this oversight); Stavros Gadinis & Amelia Miazad, "The Hidden Power of Compliance" 15-31 (Feb. 14, 2018 draft) (discussing jurisprudence on a board's oversight of compliance). Under the U.S. Sentencing Guidelines, oversight by an organization's "governing authority" is part of an effective compliance and ethics program. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(A) 534 (2016). See also OFFICE OF INSPECTOR GEN., U.S. DEPT. OF HEALTH & HUMAN SERV., ET AL., PRACTICAL GUIDANCE FOR HEALTH CARE GOVERNING BOARDS ON COMPLIANCE OVERSIGHT 1 (2015) (taking as a given a healthcare board's responsibility for oversight of compliance).

Depending upon the kind of organization involved, regulations may impose this board oversight directly or indirectly. For example, U.S. bank regulators require boards of large banks or bank holding companies to oversee compliance, risk management, and internal audit. See, e.g., Interagency Guidelines Establishing Standards for Safety and Soundness, 12 C.F.R. part 30, app. A, II.B (2018) (regarding the oversight of internal audit); OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 12 C.F.R. part 30, app. D, III. (2018) (regarding the board's oversight of risk-management function); BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES (Oct. 16, 2008) (oversight of compliance in these institutions). Among other things, the regulators echo the guidance of the Basel Committee on Banking Supervision on these matters. See, e.g., BASEL COMM. ON BANKING SUPERVISION, BCBS NO. 113, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS 9 (2005) (Principle 1: the board is responsible "for overseeing the management of the bank's compliance risk"). The

Securities and Exchange Commission similarly requires boards of mutual funds to oversee compliance. See, e.g., 17 C.F.R. § 270.38a-1 (2018) (mandating board approval of the compliance program of a mutual fund as well as those of its advisors and service providers).

b. The above oversight role of the board of directors is so well developed in case law, rules and regulations, and guidance that its essential responsibilities can be set out, as this Principle provides. See generally ETHICS & COMPLIANCE INITIATIVE, PRINCIPLES AND PRACTICES OF HIGH-QUALITY ETHICS & COMPLIANCE PROGRAMS: REPORT OF ECI'S BLUE RIBBON PANEL 20 (2016) (discussing these responsibilities or "leading practices"); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS —GUIDELINES, ISO 19600 10-11 (2014) (paragraphs 5.3.2 and 5.3.3, enumerating the role and responsibilities of the governing body, among others, in compliance). A basic responsibility is that the board of directors should be informed of the major laws and regulations, as well as the major legal risks, affecting an organization and organizational actors. This is the responsibility of each director. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 988 (stating this responsibility for a director of a public corporation). A director may obtain this information in different ways and may reasonably rely upon others who have the professional competence to supply it. See, e.g., DEL. CODE ANN. tit. 8, § 141(e) (2018) (allowing this reliance). The chief legal officer of, or other legal advisor to, the organization is generally the most appropriate person to provide the information about legal risks. See Robert C. Bird & Stephen Kim Park, *The Domains of Corporate Counsel in an Era of Compliance*, 53 AM. BUS. L. J. 203, 209 (2016) (describing the counsel's role). It is also recommended that directors understand the code of ethics and values underlying it. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(A), supra, at 534 (stating that an organization's governing authority "shall be knowledgeable about the content and operation of the compliance and *ethics* program ….") (emphasis added). That the major stock exchanges require a code of business conduct and ethics for listed companies applicable to, among others, directors underscores the need of a director to be informed about the values underlying the code. See, e.g., NYSE, Inc., Listed Company Manual § 303A.10 cmt. (2018) ("such a code can focus the board and management on areas of ethical risk, provide guidance to personnel to help them recognize and deal with ethical issues, provide mechanisms to report unethical conduct, and help to foster a culture of honesty and accountability."). See also DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT § 2 (2010) ("We shall promote the highest ethical values as expressed in our written codes of business conduct ….").

c. That the board of directors specifically reviews and approves the compliance program and code of ethics, as well as material revisions to them (as stated in subsection (b)(2)), is an essential part of its oversight of compliance. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 986, 999; Hillary A. Sale, *Monitoring Caremark's Good Faith*, 32 DEL. J. CORP. L. 719, 733-743 (2007) (discussing, among other things, how board of directors should implement a monitoring system that bring "red flags" of possible misconduct to its attention). Under the U.S. Sentencing Guidelines, the "governing authority" oversees "the implementation and effectiveness of the compliance and ethics program" in an

organization. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(A), supra, at 534. See also BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES, supra at 8 (requiring that a board "should review and approve key elements of the organization's compliance risk management program and oversight framework, including firmwide compliance policies, compliance risk management standards, and roles and responsibilities of committees and functions with compliance oversight responsibilities."); 17 C.F.R. § 270.38a-1(a)(2) (2018) (requiring approval of compliance "policies and procedures" by the board of a registered investment company). This board responsibility receives international support. See generally G20/OECD, PRINCIPLES OF CORPORATE GOVERNANCE 49 (2015) (under VI.D.7, stating board responsibility to ensure "that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.") (bold omitted). Survey data reflects the board's oversight of compliance. See, e.g., KPMG, THE COMPLIANCE JOURNEY: BOOSTING THE VALUE OF COMPLIANCE IN A CHANGING REGULATORY CLIMATE 7 (2017) (survey of U.S. chief compliance officers reveals that 94% of respondents state that their board or a board committee annually reviews and approves the compliance program and 93% state that the board or a committee is informed of compliance risks and mitigation efforts).

d. Similarly, law and regulation, as well as learned authorities, require or recommend that directors be informed of an organization's risks and, as part of their oversight, review and approve its risk-management framework and program. See, e.g., ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 986, 998 (a board's understanding a firm's risk profile and its management of risks), 987 (an individual director's understanding of a firm's kinds of risk). This oversight is part of what is known as enterprise risk management. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT: ALIGNING RISK WITH STRATEGY AND PERFORMANCE, VOL. 1 10 (June 2017) (defined as "[t]he culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.") (italics omitted), 28 ("The board of directors has the primary responsibility for risk oversight in the entity..."). Board risk oversight has traditionally been the responsibility of the board audit committee, as is discussed in § 3.12. See, e.g., NYSE, Inc., Listed Company Manual § 303A.07(b)(iii)(D) cmt. (2018) ("The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken."). After the financial crisis, there has been considerable policy and regulatory focus on a board's oversight responsibilities with respect to an organization's risk management. See, e.g., G20/OECD, PRINCIPLES OF CORPORATE GOVERNANCE, supra, at 50 (2015) (VI.D.7 cmt.: "the board should retain final responsibility for oversight of the company's risk management system"). See also 17 C.F.R. § 229.407(h) (2018) (mandating that all public companies "disclose the extent of the board's role in the risk oversight of the [company]"). Bank regulators have enhanced the board's oversight of

risk management in large banks. See, e.g., OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 12 C.F.R. part 30, app. D, II.D. (2018) (under guidelines of the Office of the Comptroller of the Currency, a board of a bank with consolidated assets equal to or greater than $50 billion, among other things, must approve the chief executive officer's strategic plan for risk management and monitor its implementation). See also 12 U.S.C. § 5365(b)(1)(A)(iii) (2018) (requiring, among other things, the Board of Governors of the Federal Reserve System to promulgate prudential standards for certain bank holding companies and nonbank financial companies, including on risk management). The Federal Reserve's implementing regulation places risk-management oversight on a board risk committee. See 12 C.F.R. § 252.33 (2018).

e. Board oversight of the internal-audit function, which generally occurs through the audit committee, has long been established. See generally ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 986 (discussing this oversight). The New York Stock Exchange directs a board audit committee to "assist board oversight of … (4) the performance of the listed company's internal audit function …." NYSE, Inc., Listed Company Manual § 303A.07(b)(i)(A) (2018). Principle 3A.03 of The American Law Institute's Principles of Corporate Governance acknowledges that the audit committee oversees internal controls. See Principles of Corporate Governance: Analysis and Recommendations § 3A.03 (AM. LAW INST. 1994). Because internal auditors review the implementation of the compliance and risk-management programs, it is also recognized that the board's oversight of the internal-audit process includes how the auditors audit these internal-control functions. Again, the board or its audit committee can oversee the internal audit of internal-control systems. See Interagency Guidelines Establishing Standards for Safety and Soundness, 12 C.F.R. part 30, app. A, II.B (2018) (discussing features of internal-audit system and board oversight of it).

f. It is recognized that an important part of the board's oversight of compliance, risk management, and internal audit is its familiarity and satisfaction with the staffing and resources devoted by executive management to these internal-control functions, as well as its assurance that internal-control personnel have the requisite independence to fulfill their duties. See, e.g., ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1000 ("Boards should also ensure the compliance program has adequate resources and authority to perform its function."). For the board to conclude that an internal-control function is adequate for an organization, it should be satisfied that the function has the appropriate staffing, authority, and resources. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C), supra at 534 (noting that the person or persons with "operational responsibility for the compliance and ethics program" should be given "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority"). Financial regulation and guidance from international financial institutions echo this position. See, e.g., BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES, supra at 7 (referring to the obligation of the board to ensure that "[s]enior management within the corporate

compliance function and senior compliance personnel within individual business lines should have the appropriate authority, independence, and access to personnel and information within the organization, and appropriate resources to conduct their activities effectively."); BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS 10 (2014) (Principle 1, paragraph 42: "The board should ensure that the risk management, compliance and audit functions are properly positioned, staffed and resourced and carry out their responsibilities independently and effectively.").

g. It is well established that the board's oversight of internal-control functions requires it to review them and their effectiveness periodically, as well as their need for modification. See, e.g., ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 999 (discussing a public company board's review of the compliance program and its effectiveness); U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(5)(B), supra, at 535 (a feature of an effective compliance and ethics program is that the organization "evaluate[s] periodically [its] effectiveness…."); BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES, supra, at 7 ("The board should exercise reasonable due diligence to ensure that the compliance program remains effective by at least annually reviewing a report on the effectiveness of the program."); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT: ALIGNING RISK WITH STRATEGY AND PERFORMANCE, supra, at 106-107 (discussing formal and informal reporting to the board about risks, enterprise-risk-management practices, and their performance). The board can determine how to conduct this review, but one alternative is to have it receive reports from and have an annual meeting with the chief compliance officer with, or without, senior executive officers. See, e.g., 17 C.F.R. § 270.38a-1(a)(4)(iii) & (iv) (2018) (stipulating that chief compliance officer of a registered investment company provide an annual report to the board of the investment company and meet annually with its independent directors).

h. Authorities support the practice that the board of directors learns about any significant or material violations or failures of any of the internal-control programs and approves the remedial and disciplinary actions to be taken to remedy them, particularly those involving reporting to a regulator. See OFFICE OF INSPECTOR GEN., U.S. DEPT. OF HEALTH & HUMAN SERV., ET AL., PRACTICAL GUIDANCE FOR HEALTH CARE GOVERNING BOARDS ON COMPLIANCE OVERSIGHT, supra at 10 ("The Board should be assured that there are mechanisms in place to ensure timely reporting of suspected violations and to evaluate and implement remedial measures."); ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 999 (board should ensure that there is an appropriate process "to encourage … timely reporting of significant legal or other compliance matters to the board or an appropriate board committee"); BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES, supra, at 7 ("[t]he board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by senior

management."); 17 C.F.R. § 270.38a-1(a)(4)(iii)(B) (2018) (requiring that a chief compliance officer of a registered investment company address in the annual report to the board each "Material Compliance Matter" that has occurred since the last report). In practice, reports to the board may also focus on the overall results of compliance monitoring. See, e.g., KPMG, THE COMPLIANCE JOURNEY: BOOSTING THE VALUE OF COMPLIANCE IN A CHANGING REGULATORY CLIMATE 25, 27 (2017) (survey of U.S. chief compliance officers reveals that 74% report compliance-monitoring results to a board committee, as well as to senior management, and that 76% report annually to the board on data and root-cause analysis of compliance-investigation results).

i. The National Association of Corporate Directors recommends that a board of a corporation have in place a "crisis management plan" with a designated team to execute the plan. It also recommends that the plan be reviewed on a regular basis for updating and that "worst-case" scenarios be evaluated. See generally REPORT OF THE NACD BLUE RIBBON COMM'N ON RISK GOVERNANCE: BALANCING RISK AND REWARD 40 (2009) (citing 2002 REPORT OF THE NACD BLUE RIBBON COMMISSION ON RISK OVERSIGHT: EXECUTIVE SUMMARY). Having such a plan is considered to be part of enterprise risk management. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT: ALIGNING RISK WITH STRATEGY AND PERFORMANCE, VOL. 1 8 (June 2017) (discussing a crisis-management plan as a way for an organization to manage the impact of an extreme event). See also CAROLE BASRI, CORPORATE COMPLIANCE 637-60 (2017) (discussing the role of corporate compliance in crisis management).

j. The American Law Institute's Principles of Corporate Governance recognize that, generally under corporate law of individual states, a board of a corporation is permitted to delegate to a committee its authority to perform one of its functions or to exercise one of its responsibilities, subject to the board's ultimate responsibility for oversight over the matter. See Principles of Corporate Governance: Analysis and Recommendations § 3.02 and Comment *j* (AM. LAW INST. 1994). See also MODEL BUS. CORP. ACT § 8.25(d) & cmt. (2016) (permitting such delegation and discussing the practice). This assignment of the oversight of compliance, risk management, and internal audit to board committees appears to be the practice today. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 998-1000 (discussing use of committees in risk management and compliance). In particular, the audit committee is often charged with the oversight of many of these functions, which oversight, in certain cases, is legally mandated. See id. at 1015-1019, 1021-1022 (describing committee's responsibilities, which include oversight of internal audit and compliance). Organizations are also reported to use a firm-wide governance committee, on which a chief compliance officer sits, for compliance oversight. See KPMG, THE COMPLIANCE JOURNEY: BOOSTING THE VALUE OF COMPLIANCE IN A CHANGING REGULATORY CLIMATE, supra, at 7.

TOPIC 3

THE BOARD OF DIRECTORS – COMMITTEES

§ 3.09. Delegation of Oversight Responsibilities by the Board of Directors to a Committee or Group of its Members

(a) If the board of directors elects to delegate any of its oversight responsibilities under § 3.08 to a committee or group of its members, this committee or group should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority over them and to any reservation made by the board in the delegation.

(b) The members constituting any such committee or group should:

(1) be independent; and

(2) have the background or experience in compliance and risk management, as the case may be, to be able, individually and, when appropriate, collectively, to fulfill their delegated responsibilities.

(c) Any such committee or group should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's or group's judgment, such engagement is appropriate.

(d) Any such committee or group may elect to have a written charter specifying its purpose, duties, functions, structure, procedures, and member requirements or limitations.

(e) Any such committee or group should regularly report to the board of directors on the exercise of its delegated responsibilities.

Comment:

a. General. This Principle sets forth the terms and conditions governing the delegation by the board of directors of its oversight responsibilities under § 3.08 to a committee or group of its members. It is thus the counterpart to § 3.08(c), which authorizes this delegation. The use of a committee or group of its members to oversee compliance, risk management, and internal audit allows the board to delegate efficiently its oversight over the internal-control functions to its members with backgrounds in these areas. The delegation also enables directors to develop expertise in the functions in an organization. Having a committee or group primarily responsible for an internal-control function should thus promote better oversight of it and is particularly suitable for a publicly traded company or other organization of comparable size and operations.

Section 3.09 deals with the general principles of delegation to committees, while § 3.10 through § 3.12 focus on the compliance and risk-management responsibilities of the board committees responsible for the oversight of a particular internal-control function. As further explained in the Comments to those Principles, the oversight responsibilities of these committees are generally the same as those of the board that are enumerated in § 3.08, albeit tailored for the particular internal-control function that a committee oversees.

The order of presentation of the board committees under Topic 3—the compliance and ethics, risk, and audit committees—reflects the order in which this Chapter presents the internal-control functions and the internal-control officers. This order, which has internal audit following compliance and risk management, is based upon the fact that, because the internal-audit function checks on the operation of the other two internal-control functions, it logically follows them in the presentation. However, this Chapter recognizes that, since in certain organizations the audit committee may be the only board committee responsible for the oversight of all internal-control functions, see § 3.12, Comment *a*, it may be the most significant committee in practice.

b. Terms and conditions of the delegation in general. Subsection (a) suggests that the committee or group to which the board of directors delegates any of its oversight of compliance, risk management, or internal audit assumes full power over the delegated responsibilities in the organization, subject to two qualifications: (i) the board may reserve some of the oversight responsibilities for itself; and (ii) the board's oversight of the internal-control functions is paramount. In other words, the board could decide, at any time, to retake the entire oversight of an internal-control function or the supervision of a given subject matter relating to it. The phrase "full power" in subsection (a) means that executive management and internal-control officers report to the committee in the first instance on matters relating to the internal-control function over which the committee has delegated authority.

c. Independence, background, and experience of committee members. Subsection (b) echoes the language of § 3.06(a) in that it requires the members of a committee with delegated power to have the independence and background or experience to enable them to conduct their oversight appropriately and competently. Thus, the Comments to § 3.06, particularly Comments *b* and *c*, are equally applicable to this subsection. As noted in Comment *b* to that Principle, independence for directors, who generally have full-time executive positions in other organizations, focuses on whether they are employed by, or have material financial dealings with,

the organization if they are responsible for oversight of internal controls. The members of the committee should collectively have the necessary distance from executive management when supervising internal-control functions. In its independence requirement, this Principle reflects the legal mandate for a publicly traded company that the committee having oversight of internal-control functions, the audit committee, be composed of independent directors.

Subsection (b) allows the board considerable flexibility in assembling, in a committee, directors who can collectively oversee a firm's compliance, risk management, or internal audit. Apart from the above requirements, it does not mandate any committee or group composition. Under certain laws and regulations an oversight committee of an internal-control function must include a designated "expert" in the subject, such as a financial expert on the audit committee of the board of a publicly traded company. This Principle supports, but does not mandate, this practice.

d. Resources. Subsection (c) stipulates that a board committee or group be reasonably satisfied that it has adequate resources to conduct its delegated oversight of compliance, risk management, or internal audit. The phrases "reasonably satisfied" and "given the organization's circumstances" emphasize that a committee's desire for resources should always be balanced with such circumstances as the ability of the organization to provide them, in light of the other demands on the organization's funds. The resources could allow the committee or group to engage third-party advisors, including legal counsel, who can assist it in performing its oversight tasks. Compliance, risk management, and internal audit are activities that persons with specialized training and experience often conduct, particularly in large organizations. See § 3.15, § 3.16, and § 3.17 (provisions dealing with, respectively, the chief compliance officer, the chief risk officer, and the chief audit officer). For that reason, in certain circumstances a committee may need an advisor with expertise in the internal-control function who can help the committee to evaluate properly the approach of executive management and the internal-control officer on the internal-control function generally, or on a particular internal-control function issue. The availability of resources ensures that, when appropriate and reasonable, the committee can receive independent advice and information, in addition to that offered by executive management or by executive management's advisors. Alternatively, the committee may need to commission a report or to undertake an investigation on a compliance, risk-management, or internal-audit matter affecting the organization. Engaging a third-party advisor may be necessary to ensure that the report or

investigation is appropriately independent, especially when executive management and internal-control officers were involved in the underlying matter. Board committees in a publicly traded company and a similar large organization may be more likely to engage outside advisors because the oversight of compliance, risk management, and internal audit is more challenging than it would be in a smaller organization and because these committees generally have greater available resources.

e. Charter. Subsection (d) reflects the common practice (and in some cases a legal requirement) that a board committee or group of an organization have a written charter that articulates the committee's or group's purpose, responsibilities, procedures, structure, and composition. The charter could reflect the terms of the delegation from the board by setting forth clearly why the committee has been instituted and what oversight duties it has. It could also specify any qualifications for member service on a committee, as well as any restrictions, such as term limits. This subsection recognizes that it is beneficial for the organization to have a committee's responsibilities spelled out, particularly in cases in which the organization must defend the adequacy of its oversight of a given internal-control function.

f. Committee reporting. Finally, subsection (e) stipulates that, in general, the committee or group should regularly report to the full board of directors on the matters over which it has delegated oversight power. By recommending "regular" reporting by a committee to the board, this subsection underscores that, while this Principle endorses the use of the committee or group for internal-control oversight, the board should be kept apprised of the committee's work. Thus, if the board deems it appropriate or if the committee feels it necessary, the board can itself reassume the oversight of a compliance, risk-management, or internal-audit issue or of an entire internal-control function. However, there may be circumstances in which the committee should not be reporting to the full board (e.g., when certain other board members are the subject matter of the committee's report or investigation).

REPORTERS' NOTE

a. It is well established under the law of many organizations that, pursuant to, and subject to any restriction in, the governing documents of an organization, its board of directors may delegate the oversight of a matter or matters to a committee of its members. See supra § 3.08, Reporters' Note *j* (citing sources). The advantages of the committee for delegated oversight and its limitations are also well established. See Principles of Corporate Governance: Analysis and Recommendations § 3.02(c) and Comment *j* (AM. LAW INST. 1994) ("because of the critical nature

of the oversight function, the board must maintain a continuing presence in and ultimate responsibility for the overall performance of that function"). See also MODEL BUS. CORP. ACT § 8.25(d) (2016) ("A board committee may exercise the powers of the board of directors under Section 8.01, to the extent specified by the board of directors or in the articles of incorporation or bylaws…."); ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 1013 (2011) ("Delegation of a given responsibility to a committee does not relieve the full board of ultimate responsibility for oversight of the company.").

b. It has become common practice to have independent directors on certain oversight committees of publicly traded corporations in order "to improve corporate governance and transparency," ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1012, and to "delegate to a committee matters that require specialized knowledge or experience …," id. It is recommended that such an oversight committee have "appropriate independence," id. at 1014, and that committee members have "experience relevant to committee responsibilities" or "subject matter expertise that will assist the committee in its work," id. at 1015. In certain organizations, applicable law and regulation mandate committee member independence and expertise. The audit committee of a public company must be composed of independent directors, see 15 U.S.C. § 78j-1(m)(3) (2018); 17 C.F.R. § 240.10A-3 (2018); NYSE, Inc., Listed Company Manual § 303A.06 (201), have "financially literate" members, NYSE, Inc., Listed Company Manual § 303A.07(a) cmt. (2018), and disclose whether it has a "financial expert" member, see 15 U.S.C. § 7265 (2018); 17 C.F.R. § 229.407(d)(5) (2018); NYSE, Inc., Listed Company Manual § 303A.07(a) cmt. (2018). Stock-exchange listing rules specify the meaning of financial literacy, see, e.g., NASDAQ Stock Market Rules § 5605(c)(2)(A) (2018) (a basic familiarity with financial statements), and allow it to be acquired "on the job," see NYSE, Inc., Listed Company Manual § 303A.07(a) cmt. (2018). Regulation defines the attributes of a financial expert, see 17 C.F.R. § 229.407(d)(5)(ii)(A)-(E) (2018), and allows the expertise to be acquired through education and experience, see 17 C.F.R. § 229.407(d)(5)(iii)(A)-(D) (2018). This statute and these regulations support the flexibility that the Principle adopts for the background and experience of members of committees overseeing compliance, risk management, and internal audit. Statute and regulation also determine the composition of other important publicly traded-company board committees. See, e.g., 15 U.S.C. § 78j-3 (2018) (mandating compensation-committee-member independence to be effected through stock-exchange listing standards); 17 C.F.R. § 240.10C-1 (2018) (providing guidance to stock exchanges on this committee's composition and practices).

c. It is understood, as a general matter, that board committees should have adequate resources to do their delegated functions. This matter of resources is intertwined with the issue of the committee's responsibilities. If, for example, a committee oversees a firm's compliance program, it may need to engage a compliance expert to advise the committee on the adequacy of this program. Being empowered to engage its own advisors is also indicative of the committee's independence. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S

GUIDEBOOK, supra, at 1014 (identifying authority to engage advisors as part of a committee's independence). Statutes require that certain oversight committees of a publicly traded company be provided with the resources (including the power to engage advisors) to perform their role. See 15 U.S.C. § 78j-1(m)(5) & (6)(B) (2018) (mandating that a listed company allow and fund its audit committee to engage the committee's own independent counsel and other advisers); 15 U.S.C. § 78j-3(c)-(e) (2018) (mandating that the compensation committee of a publicly traded company have the authority, and receive funding, to retain its own compensation consultants as well as legal and other advisors). Another kind of resource is adequate compensation for the members of these committees, given their responsibilities. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1023 (discussing adequate compensation for audit-committee members).

d. It is the recommended practice for a board committee to have a charter that specifies its authority and responsibilities. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1014 (recommending that a committee have a charter or be established by board resolution). In some cases, this charter is mandatory. See NYSE, Inc., Listed Company Manual § 303A.07(b) (2018) (requiring charter for audit committee); NASDAQ Stock Market Rules § 5605(c)(1) (2018) (same); NYSE, Inc., Listed Company Manual § 303A.05(b) (2018) (required charter for compensation committee); NASDAQ Stock Market Rules § 5605(d)(1) (2018) (same).

e. A board committee should regularly report to the board of directors because the latter is ultimately responsible for the oversight of the internal-control functions. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1015 ("Board committees should regularly inform the board of their activities."). Actions taken by a committee should generally be reported at the next board meeting. See Principles of Corporate Governance: Analysis and Recommendations § 3.02(c), Comment *j*, at 93 (AM. LAW INST. 1994) ("This procedure is intended to keep the board apprised of actions taken at what is, in effect, a board level, and also to give the board a means of supervising its committees."). Again, in some cases, this reporting is legally required. See, e.g., NYSE, Inc., Listed Company Manual § 303A.07(b)(iii)(H) (2018) (providing in committee charter for audit committee to report to the board). This committee reporting with respect to compliance, risk management, and internal audit helps the board satisfy its legal duties. See In re Caremark International Inc. Derivative Litigation, 698 A.2d 959, 970 (Del. Ch. 1996) ("But it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.").

§ 3.10. Compliance and Ethics Committee

(a) The board of directors, in its discretion, may elect to delegate to a compliance and ethics committee, or to another committee or committees, part or all of its oversight of compliance and ethics in the organization. This committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should:

(1) be independent; and

(2) have the background or experience in compliance and ethics to be able, individually and, when appropriate, collectively, to fulfill their delegated responsibilities.

(b) The compliance and ethics committee should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's judgment, such engagement is appropriate.

(c) The compliance and ethics committee may elect to operate with a written charter specifying the committee's purpose, responsibilities, functions, structure, procedures, and member requirements or limitations.

(d) The compliance and ethics committee's oversight in subsection (a) should include one or more of the following responsibilities:

(1) to be informed of the major legal obligations of, and the main values in the code of ethics for, the organization, its employees, and agents;

(2) to review and approve the compliance program and the code of ethics, any material revisions thereto, and their implementation;

(3) to be reasonably informed of the staffing and resources allocated by executive management to the compliance department and to satisfy itself that they are adequate and that the department is sufficiently independent and has the appropriate authority to perform its responsibilities;

(4) to approve the appointment, terms of employment, and dismissal of the chief compliance officer;

(5) to communicate regularly with the chief compliance officer;

(6) to meet at reasonable intervals with executive management and the chief compliance officer to review the effectiveness of, inadequacies in, and any necessary changes to the organization's compliance function;

(7) to confer with executive management, the chief compliance officer, and the chief legal officer:

(A) to address any material violation or failure of the compliance program or code of ethics, and

(B) to approve or ratify any material disciplinary or remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation or failure;

(8) to confer with executive management, the chief compliance officer, and the chief legal officer about:

(A) any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and code of ethics in ensuring compliance with them, and

(B) the adequacy of such disclosure or reporting;

(9) to confer with executive management or any other board committee to explore whether the organization's practices, particularly those involving compensation, are adequately aligned with the compliance program and the code of ethics;

(10) to receive and to respond to communications made pursuant to the organization's procedures for confidential internal reporting of a violation or failure of the compliance program and the code of ethics, and to meet at reasonable intervals with the chief legal officer and the chief compliance officer to review the effectiveness of, inadequacies in, and any necessary changes to these procedures;

(11) with the assistance of the chief legal officer, the chief compliance officer, outside legal counsel, or outside consultants, to direct its own investigation of any material violation or failure of the compliance program and the code of ethics,

including any violation or failure communicated under the organization's procedures for confidential internal reporting; and

(12) to report regularly to the board of directors on the responsibilities delegated to it.

Comment:

a. General. This Principle authorizes the creation of a compliance and ethics committee of the board of directors. This kind of board committee may be appropriate for a publicly traded company or other organization of comparable size and operations, or for any size firm that wishes to take advantage of the specialization that comes from having a committee to which the board delegates its oversight of compliance and ethics. This Principle thus offers a basic framework about the committee and its responsibilities that an organization could use as it sees fit. It also recognizes that an organization may elect not have a compliance and ethics committee and may delegate the responsibilities enumerated here to another board committee or committees, a committee of directors and executives, or simply senior executives. This Principle acknowledges that the audit committee has in practice been the board committee overseeing compliance in a publicly traded company.

b. Composition, resources, and charter. Subsection (a) establishes the compliance and ethics committee, its recommended composition, and basic structure. With respect to the independence and background or experience of committee members, it tracks the language in § 3.09(b), and Comment *c* to that Principle applies equally here. Similarly, subsections (b) and (c) track the language of, respectively, § 3.09(c) and (d) about the committee's satisfaction that it has the resources to fulfill its responsibilities and having a charter that, among other things, sets forth the committee's responsibilities. Comments *d* and *e* of § 3.09 explain the purposes of these provisions.

c. Committee responsibilities in general. Subsection (d) sets forth the recommended responsibilities of the compliance and ethics committee for the oversight of compliance and ethics that are, for the most part, the same as those of the board of directors. Subsection (d)(1), (2), and (3) repeat the board's responsibility for being informed about major legal obligations and the organization's main values, its oversight of the compliance program (which includes the compliance policies and procedures) and the code of ethics, and its responsibility to satisfy itself that the compliance department has adequate resources and sufficient independence in the

organization, which are stated, respectively, in § 3.08(b)(1), (2), and (6). Comments *c* and *f* of § 3.08 are applicable here.

d. Committee responsibilities; chief compliance officer's reporting to and communicating with the committee. Subsections (d)(4) and (5) echo the board responsibilities stated in § 3.08(b)(7) and (8) and reflect the two meanings of organizational reporting with respect to the chief compliance officer. These subsections are particularly important for establishing the compliance and ethics committee's primacy over the organization's oversight of compliance and ethics when the board has determined to delegate this responsibility to a board committee. The chief compliance officer may be a member of executive management who "directly reports" to, and would thus be under the line of authority of, the chief executive officer, who would ordinarily propose a person for that position and decide when to terminate that officer. Alternatively, the chief compliance officer may be lower in the organization's hierarchy and be a direct report to another member of executive management (or to an officer below the level of executive management). In any of these cases, under subsection (d)(4), the compliance and ethics committee approves the hiring, terms of employment, and dismissal of this officer. The committee's approval of the engagement, and particularly the dismissal, of the chief compliance officer is designed to provide another layer of oversight of these personnel actions and could help ensure that the officer is not terminated merely for having raised an important compliance- or ethics-related issue in the organization. Subsection (d)(4), moreover, reflects that this committee power over the hiring and dismissal of a chief compliance officer is mandated by law or regulation in certain domains. As provided in this subsection, the committee's oversight extends to the chief compliance officer's terms of employment, which include compensation unless the board compensation committee is responsible for it. See § 5.16, Comment *b* (discussing issues presented by compensation of chief compliance officer).

Subsection (d)(5) highlights that the chief compliance officer may communicate, in the sense of providing or reporting information, directly with the compliance and ethics committee (or to another committee having similar oversight responsibilities). This communication would be separate from and independent of the officer's reporting to the chief executive officer and other members of executive management. It enables the compliance and ethics committee to conduct its oversight of the compliance program better by hearing directly from the chief compliance officer without the communication being filtered or influenced by members of executive management.

The committee determines the scope and frequency of any reporting, but the regularity of such reporting helps ensure that no unintended negative signal is sent by a meeting between the officer and the compliance and ethics committee, which might occur if this kind of meeting took place only at the committee's or officer's request.

e. Committee responsibilities; reviewing the effectiveness of the compliance function, and dealing with a material violation or failure of the compliance program and code of ethics. Under subsection (d)(6), the compliance and ethics committee may be delegated the responsibility of the board of directors, as stated in § 3.08(b)(9) and as explained in Comment *h* to that Principle, to evaluate the effectiveness of the organization's compliance function and to identify and to address inadequacies in it. Subsection (d)(7) tracks § 3.08(b)(10) when it has executive management report to the compliance and ethics committee a material violation or failure of the compliance program or the code of ethics and seek its approval or ratification of disciplinary or remedial action, including reporting to a regulator, that is to be or has been taken as a result. The compliance and ethics committee may wish to refer this matter, particularly discipline, regulatory reporting, and remediation, to the full board of directors for its decision.

f. Committee responsibilities; disclosure and regulatory reporting. While the matters covered by subsection (d)(8) are responsibilities of the board of directors, they are not explicitly addressed in § 3.08 but are included here where there is a more expansive discussion of compliance oversight in the enumeration of the responsibilities of a compliance and ethics committee. This subsection suggests that the board of directors may find it useful to delegate to the compliance and ethics committee, which develops its own expertise on compliance oversight, the task of conferring with executive management and the chief compliance officer to review and approve both mandatory and discretionary disclosures and regulatory reporting about the organization's major legal obligations and ethical standards and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them. An example of a mandatory disclosure would be disclosure on the compliance program or material compliance failures in public filings made to the Securities and Exchange Commission or in any other filings required by law or regulation. The compliance and ethics committee would also likely confer with executive management and the chief compliance officer about significant mandatory reports on the organization's major legal obligations and ethical standards and its compliance program and code of ethics that the organization makes to a regulator. These would be those reports other than routine

communications made in the ordinary course of interaction with regulators. The subsection also includes the committee's oversight of any discretionary disclosure or regulatory reports, which could occur, for example, if executive management believes that it would be in the organization's interest to publicize its compliance program and code of ethics (as portrayed in the following example) or if a regulator asked for, but did not require, a report on the program and code:

> Senior executives of company that provides payment processing services believe that highlighting the company's compliance program and the program's success in addressing legal risks associated with the provision of such services would greatly assist in the company's sales. In consultation with the chief compliance officer and the chief legal officer, the company's compliance and ethics committee would be expected to review with senior executives this disclosure and approve it.

It is recommended that the committee include the chief legal officer in its discussions on this disclosure and reporting because of the risk of litigation relating to them. This subsection is likely to be relevant primarily to a publicly traded company that is a reporting company under the Securities Exchange Act of 1934 or an organization that is in a highly regulated industry. The compliance and ethics committee's review and approval of the above disclosures and regulatory reporting would likely be in addition to those by other board committees and by executive-level compliance committees. See also § 5.06, Comment *g* (discussing organizations making their compliance policies available to the public).

g. Committee responsibilities; meeting with executive management and other committees about organizational practices. Under subsection (d)(9), the compliance and ethics committee may find it useful to meet with executive management or any other board committee to inquire whether organizational practices are adequately aligned with the compliance program and code of ethics, or run counter to them. Given that the risk committee, if one exists, and the audit committee have oversight of the other major internal-control functions, it may be appropriate for the committee to meet periodically with these other committees (if they do not have overlapping membership). These meetings could help the compliance and ethics committee, and thus the organization, ensure that the compliance program and the code of ethics are fully embedded in organizational practices. A particular focus of these meetings could be on the organization's compensation practices because they are critical in aligning the conduct of organizational actors with its compliance program and code of ethics.

h. Committee responsibilities; administering the confidential internal-reporting system. Certain organizations are mandated by law and regulation to establish channels for the confidential internal-reporting of legal and other violations occurring in the organization. See § 5.18 (an organization's procedures for internal reporting); § 6.25 (organizational whistleblower programs). Subsection (d)(10) provides an alternative whereby the compliance and ethics committee is charged by the board of directors or by another committee, such as the audit committee, with receiving and responding to any reports made under the organization's confidential internal-reporting system. This responsibility makes sense because of the committee's oversight of compliance and ethics, which encompasses both being informed about the legal obligations of the organization and organizational actors and about the compliance program's efforts to ensure compliance with these obligations. Subsection (d)(10) also provides that, with the assistance of the chief legal officer and the chief compliance officer, the committee would evaluate the effectiveness of the confidential internal-reporting system and would identify and address inadequacies in it.

i. Committee responsibilities; conducting its own investigation of a material violation or failure. Subsection (d)(11) reflects the committee's responsibility to conduct its own investigation of a material violation or failure of the compliance program and the code of ethics, including any disclosed through the confidential internal-reporting system, rather than relying upon the one conducted by executive management. It thus echoes the board's power set forth in § 3.08(b)(11)(A), and Comment *j* to that Principle explains the reasons for this investigatory responsibility.

j. Committee responsibilities; reporting to the board of directors. Subsection (d)(12) is modeled upon § 3.09(e) in its providing that the compliance and ethics committee should report regularly to the board of directors on the matters as to which the committee has delegated authority. Comment *f* to § 3.09 is applicable here.

REPORTERS' NOTE

a. Organizations are generally not mandated by law or regulation to have a stand-alone compliance and ethics committee of the board of directors. Organizations in highly regulated industries may elect to have a committee dedicated to compliance oversight. See generally PWC STATE OF COMPLIANCE STUDY 2016: LAYING A STRATEGIC FOUNDATION FOR STRONG COMPLIANCE RISK MANAGEMENT 3, 13 (2016) (global survey of 800 executives reveals that 20% of firms have a "separate, stand-alone compliance/ethics committee," while 65% report that the audit committee oversees compliance); SOC'Y OF CORP. COMPLIANCE AND ETHICS & NYSE GOVERNANCE SERV.,

COMPLIANCE AND ETHICS PROGRAM ENVIRONMENT REPORT 28 (2014) (survey of compliance officers in diverse organizations reveals that, when the board has delegated the oversight of compliance and ethics to a committee (51% of respondents), 20% of them report that the delegation is to a compliance committee, whereas 41% report that it is to the audit committee); GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 94-97 (2017) (noting this fact and providing an example of a compliance-committee charter); ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 999-1000 (2011) (noting that some companies establish a compliance committee for compliance oversight). For publicly traded companies listed on the New York Stock Exchange, the audit committee is tasked with assisting the board in its oversight of compliance. See NYSE, Inc., Listed Company Manual § 303A.07(b)(i)(A) (2018). See also ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1018, 1022 (discussing how audit committee meets its oversight responsibilities over compliance). The audit committee may be aided by another committee to fulfill this mission. See id. at 999-1000 (noting how companies have established a compliance or legal-affairs committee to ease the burden of the audit committee). This kind of board compliance committee is recommended in certain sectors, such as banking. See BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS 16 (Oct. 2014) (Principle 3, no. 76, observing that an ethics/compliance committee is increasingly "common"); BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS 12-13 (2005) (Principle 5, referring to possible involvement of a board committee to which the compliance department reports).

b. Because, as noted above, a compliance and ethics committee is not legally required for organizations, nor widespread (although its use appears to be growing), there is little commentary or data on its composition and basic structure. These characteristics can be taken, by analogy, from other prevalent board committees, such as the audit committee. For example, just as the audit committee of a publicly traded company, which is tasked with the oversight of the compliance and ethics program, must be composed of independent directors and have on it a financial expert, see § 3.09, Reporters' Note *b*, a compliance and ethics committee should be composed of independent members who have a background in or familiarity with compliance in such organizations. Again, by analogy with established committees, this committee should have adequate resources to fulfill its responsibilities, which can be laid out in a charter. See § 3.09, Reporters' Notes *d* and *e*.

c. The responsibilities of a compliance and ethics committee are not specified in much detail by practice guidelines. They are thus taken for the most part from those of the board of directors, as enumerated in § 3.08. Practitioners who do address this committee's duties, generally in the context of discussing the audit committee's responsibilities, recommend that it meet regularly, and no less than annually, with the officers who help administer, and check on, an organization's code of ethics and compliance policies, such as the general counsel, chief compliance officer, and chief audit officer. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 1022 (discussing the audit committee's

oversight of compliance). The committee should also receive reports from these officers, who provide the information that will enable it to determine if the compliance program is effective: the "number and type of concerns reported and investigated, any material violations of law and corporate policies, [and] the sanctions imposed…." Id. See also BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, supra, at 12-13 (Principle 5, no. 32: "Although its normal reporting line should be to senior management, the compliance function should also have the right of direct access to the board of directors or to a committee of the board, bypassing normal reporting lines, when this appears necessary. Further, it may be useful for the board or a committee of the board to meet with the head of compliance at least annually, as this will help the board or board committee to assess the extent to which the bank is managing its compliance risk."); SOC'Y OF CORP. COMPLIANCE AND ETHICS & NYSE GOVERNANCE SERV., COMPLIANCE AND ETHICS PROGRAM ENVIRONMENT REPORT, supra, at 29 (survey results of the information reported to a board or board committee on compliance, such as compliance and ethics-program audits, code-of-conduct updates or revisions, and overall program performance); U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C) 534 (2016) ("Individual(s) with operational responsibility [for the compliance and ethics program] shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program.").

An SEC regulation, which specifies the compliance-related oversight of a board of a registered investment company, and Financial Industry Regulatory Authority (FINRA) rules, which do the same for a board of a registered broker-dealer, also serve as sources for the responsibilities of a compliance and ethics committee. See 17 C.F.R. § 270.38a-1 (2018) (for investment companies); FINRA Rule 3130, http://finra.complinet.com (for broker-dealers). The board of a registered investment company (including a majority of the non-interested directors) is required to approve the compliance policies and procedures of the fund and those of its adviser and other service providers, to receive an annual written report from the chief compliance officer on the operation of these policies and procedures, any material changes made to them as a result of an annual review of their effectiveness, and "Material Compliance Matters" (i.e., what the board would reasonably need to know to conduct its oversight, such as violations of the law or compliance policies by the fund or by a service provider and weaknesses in the design or implementation of these policies), and to meet annually with the chief compliance officer. See 17 C.F.R. § 270.38a-1(a)(2) & (4) (2018). See also FINRA Rule 3130(c)(3), supra (specifying report on the compliance program received by the broker-dealer's board and audit committee).

d. An SEC regulation also provides a model for a compliance and ethics committee's authority over the chief compliance officer's hiring, terms of employment, and dismissal. The board of a registered investment company (including a majority of its independent directors) must approve the hiring, compensation, and removal of the company's chief compliance officer. See 17 C.F.R. § 270.38a-1(a)(4)(i) & (ii) (2018). The U.S. Commodity Futures Trading Commission's regulation of futures commission merchants, swap dealers, and major swap participants allows either the board of directors or a senior officer to appoint, to remove, and to determine the

compensation of the chief compliance officer. See 17 C.F.R. § 3.3(a) (2018). See also BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, supra, at 12 (Principle 5, n.27, recommending that the board of directors be informed about the hiring and departure of the chief compliance officer and the reasons for that departure).

e. One legal source of support for having the compliance and ethics committee receive confidential reports of and investigate potential violations of law or of the code of ethics is in SEC regulations providing for a "qualified legal compliance committee" for a publicly traded company, which is composed of one member of the audit committee and otherwise of independent directors and which is authorized to receive confidential reports of material violations of the federal securities laws or breaches of legal duty, to initiate investigations of them, and to recommend appropriate responses and remedial measures to them. See 17 C.F.R. § 205.2(k) (2018). See also U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(7), supra, at 535 (one hallmark of an effective compliance program is that the organization "take reasonable steps to respond appropriately to the criminal conduct…."); see id. cmt. app. n.6, at 537 (response includes remedying the harm from the conduct).

f. There is precedent for an organization's public disclosure and reporting to regulators about its compliance program and code of ethics, other than in situations in which there has been a material violation of them. These serve as a basis for the compliance and ethics committee's responsibilities relating to that disclosure and reporting. Public companies are required to disclose whether they have a code of ethics applicable to certain members of executive management. See 17 C.F.R. § 229.406 (2018). Listed companies have to adopt and to disclose publicly (including through a website) their code of business conduct and ethics, which must address compliance with laws, rules, and regulations. See, e.g., NYSE, Inc., Listed Company Manual § 303A.10 (2018). As for reporting to regulators, regulated organizations must generally expect that their compliance program and any internal reports relating to it are subject to review by the government agencies with jurisdiction over them. The Federal Reserve emphasizes that its examination staff will focus on the compliance program of certain large banks. See BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES 2 (Oct. 16, 2008) (stating its expectations for a compliance-risk-management program at a large banking organization, to be overseen by its examination staff). Reports on the compliance program of a registered investment company prepared by the chief compliance officer are part of its records and are subject to SEC examination. See 17 C.F.R. § 270.38a-1(d) (2018) (describing the records). It is contemplated that FINRA may request comparable reports from broker-dealers. See FINRA Rule 3130.10 (referring to, among other things, FINRA's power to see these reports). Moreover, an organization may be required to report on its compliance activities in the context of a settlement of a government investigation. See, e.g., OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVICES, CORPORATE INTEGRITY AGREEMENTS, http://oig.hhs.gov/compliance/corporate-integrity-agreements (listing this reporting as a feature of a comprehensive corporate-integrity agreement). See also § 6.16 (how enforcement authorities assess the effectiveness of an organization's compliance function).

§ 3.11. Risk Committee

(a) The board of directors, in its discretion, may elect to (or, if required by law, must) delegate to a risk committee, or to another committee or committees, part or all of its oversight of risk management in the organization. This committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should:

(1) be independent; and

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

(b) The risk committee should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's judgment, such engagement is appropriate.

(c) The risk committee may elect to operate with a written charter specifying its purpose, duties, functions, structure, procedures, and member requirements or limitations.

(d) The risk committee's oversight in subsection (a) should include one or more of the following responsibilities:

(1) to be informed of the material risks to which the organization is or will likely be exposed;

(2) to review and approve the organization's risk-management framework and risk-management program, any material revisions thereto, and their implementation;

(3) to be reasonably informed of the staffing and resources allocated by executive management to the risk-management department and to satisfy itself that they are adequate and that the department is sufficiently independent and has the appropriate authority to perform its responsibilities;

(4) to approve the appointment, terms of employment, and dismissal of the chief risk officer;

(5) to communicate regularly with the chief risk officer;

(6) to meet at reasonable intervals with executive management and the chief risk officer to review the effectiveness of, inadequacies in, and any necessary changes to the organization's risk-management function;

(7) to confer with executive management, the chief legal officer, and the chief risk officer:

(A) to address any material deviation from or failure of the risk-management program, and

(B) to approve or ratify any material disciplinary or remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such deviation or failure;

(8) to confer with executive management, the chief legal officer, and the chief risk officer about:

(A) any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the material risks to which the organization is or may be exposed and the effectiveness of the risk-management program in addressing these risks, and

(B) the adequacy of such disclosure or reporting;

(9) to confer with executive management or any other board committee to explore whether the organization's practices, particularly those involving compensation, are adequately aligned with the risk-management framework;

(10) with the assistance of the chief legal officer, the chief risk officer, outside legal counsel, or outside consultants, to direct its own investigation of any material deviation from or failure of the risk-management program; and

(11) to report regularly to the board of directors on the responsibilities delegated to it.

Comment:

a. General. This Principle authorizes the creation of a risk committee of the board of directors. This kind of committee may be appropriate for a publicly traded company or an organization of comparable size and operations, or for any size firm that wishes to take advantage of the specialization that comes from having a risk committee to which the board delegates its risk-management oversight. This Principle thus offers a basic framework for the committee and its

responsibilities that an organization could use as it sees fit. It recognizes that some organizations are required by law to have a risk committee, while others may not have such a committee and may delegate the responsibilities enumerated here to another board committee, such as the audit committee, multiple board committees, a committee of directors and executives, or simply senior executives. It also acknowledges that an organization may have multiple chief risk officers, may conduct risk management through executive-level risk committees, or may have the responsibilities of the chief-risk-officer position performed by another officer or multiple executives. While supporting organizational flexibility, for the ease of exposition this Principle uses the term "chief risk officer" for the executive(s) performing the duties laid out in § 3.16.

b. Composition, resources, and charter. Subsection (a) establishes the risk committee, its recommended composition, and basic structure. With respect to the independence and background or experience of committee members, it tracks the language of § 3.09(b), and Comment *c* to that Principle applies equally here. Background and experience are highlighted in the following example:

> Bank is a global financial institution engaged in diverse financial activities in numerous countries. In designating members of its risk committee, the board should ensure that the members, individually or collectively, are familiar with Bank's major financial activities, the risks associated with them, and the industry-accepted methods of managing its risks.

Similarly, subsections (b) and (c) track the language of, respectively, § 3.09(c) and (d) about the committee's satisfaction that it has the resources to fulfill its responsibilities and its having a charter that, among other things, sets forth the committee's responsibilities. Comments *d* and *e* of § 3.09 explain the purposes of these provisions.

c. Committee responsibilities in general. Subsection (d) sets forth the recommended responsibilities of the risk committee on risk oversight that are, in general, the same as those of the board of directors. Subsection (d)(1), (2), and (3) repeat the board's duty of being informed about material risks, its oversight of the risk-management framework and program, and its responsibility to satisfy itself that the risk-management department has adequate resources and sufficient independence in the organization, which are stated, respectively, in § 3.08(b)(3), (4), and (6). Comments *d* and *f* of § 3.08 are applicable here.

d. Committee responsibilities; chief risk officer's reporting to and communicating with the committee. Subsection (d)(4) and (5) echo the board responsibilities stated in § 3.08(b)(7) and (8)

and reflect the two meanings of organizational reporting with respect to the internal-control officer in question, the chief risk officer. These subsections are particularly important for establishing the risk committee's primacy over the organization's risk oversight when the board has determined to delegate this responsibility to a board committee. The chief risk officer may be a member of executive management who "directly reports" to, and would thus be under the line of authority of, the chief executive officer, who would ordinarily propose a person for that position and decide when to terminate that officer. Alternatively, the chief risk officer may be lower in the organization's hierarchy and be a direct report to another member of executive management (or to an officer under executive management). In any of these cases, under subsection (d)(4), the risk committee approves the hiring, terms of employment, and dismissal of the officer. The committee's approval of the engagement, and particularly the dismissal, of the chief risk officer is designed to provide another layer of oversight of these personnel actions and helps ensure that the officer is not terminated merely for having raised an important risk-related issue in the organization. As provided in this subsection, the committee's oversight extends to the chief risk officer's terms of employment, which include the compensation unless the board compensation committee is responsible for it.

Subsection (d)(5) highlights that the chief risk officer may communicate, in the sense of providing or reporting information, directly with the risk committee (or with another committee having similar oversight responsibilities). This communication would be separate from and independent of that officer's reporting to the chief executive officer and other members of executive management. It enables the risk committee to conduct its oversight of the risk-management program better by hearing directly from the chief risk officer without the communication being filtered or influenced by other executives. The committee determines the scope and frequency of any reporting, but its regularity helps ensure that no unintended negative signal is sent by a meeting between the officer and the risk committee, which might occur if this kind of meeting took place only at the committee's or officer's request.

e. Committee responsibilities; reviewing the effectiveness of the risk-management function; dealing with a material deviation from or failure of the risk-management program. Under subsection (d)(6), the risk committee may be delegated the responsibility of the board of directors, as stated in § 3.08(b)(9) and as explained in Comment *h* to that Principle, to evaluate the effectiveness of the organization's risk-management function and to identify and to address

inadequacies in it. Subsection (d)(7) tracks § 3.08(b)(10) when it has executive management reporting to the risk committee of a material deviation from or failure of the risk-management framework and seeking its approval or ratification of disciplinary or remedial action that will be or has been taken as a result, including reporting to a regulator. The risk committee may wish to refer this matter, particularly discipline, regulatory reporting, and remediation, to the board of directors for its decision.

f. Committee responsibilities; disclosure and regulatory reporting. While the matters covered by subsection (d)(8) are responsibilities of the board of directors, they are not explicitly addressed in § 3.08 but are included here, where there is a more expansive discussion of risk oversight in the enumeration of the responsibilities of a risk committee. This subsection suggests that the board of directors may find it useful to delegate to the risk committee, which develops its own expertise in risk-management oversight, the task of conferring with executive management and the chief risk officer to review and approve both mandatory and discretionary disclosures and regulatory reporting about the organization's material risks and the effectiveness of its risk-management program in addressing them. An example of a mandatory disclosure would be those of the risk-management program and material risk-management failures in public filings made to the Securities and Exchange Commission (SEC) or in any other filings mandated by law or regulation. The risk committee's oversight of this disclosure could help prevent the organization and the directors themselves from incurring liability for the organization's materially inaccurate disclosures about the risk-management program. For example, directors might incur liability under the federal securities laws if they authorized a disclosure in a public filing with the SEC representing that the organization adequately managed its risks when they knew that its actual risk controls were in fact weak. An organization's reporting to government agencies on its risk-management program is typical in certain industries, such as commercial banking. The risk committee would also likely confer with executive management and the chief risk officer about mandatory regulatory reports on the organization's material risks and its risk-management program that the organization makes to a regulator (as occurs in the banking industry). These would be reports other than routine communications made in the ordinary course of interaction with regulators. This subsection also includes the committee's oversight of any discretionary disclosure or regulatory reports, which could occur, for example, if executive management believes that it would be in the organization's interest to publicize its risk-management program

or if a regulator asked for, but did not require, a report on it. It is recommended that the risk committee include the chief legal officer in its discussions on this disclosure and regulatory reporting because of the risk of litigation relating to them. This subsection is likely to be relevant primarily to a publicly traded company that is a reporting company under the Securities Exchange Act of 1934 or an organization that is in a highly regulated industry. The risk committee's review and approval of the disclosures and reporting would likely be in addition to those by other board committees and by an executive-level risk committee.

g. Committee responsibilities; meeting with executive management and other committees about organizational practices. Under subsection (d)(9), the risk committee may find it useful to meet with executive management or any other board committee to inquire whether organizational practices are adequately aligned with the risk-management framework, or run counter to it. Given that the compliance and ethics committee (if one exists) and the audit committee have oversight of the other major internal-control functions, it may be appropriate for the risk committee to meet periodically with these other committees (if they do not have overlapping membership). These interactions could help the risk committee, and thus the organization, ensure that its risk management is fully embedded in its organizational practices. A particular focus of the meetings could be on the organization's compensation practices because they are critical in aligning the conduct of organizational actors with its risk-management framework.

h. Committee responsibilities; conducting its own investigation of a material deviation or failure. Subsection (d)(10) reflects the risk committee's responsibility to conduct its own investigation of a material deviation from or failure of the risk-management program, rather than relying upon one conducted by executive management. It thus echoes the board's responsibility set forth in § 3.08(b)(11)(A), and Comment *j* to that Principle explains the reasons for this investigatory responsibility.

i. Committee responsibilities; reporting to board of directors. Subsection (d)(11) is modeled upon § 3.09(e) in its providing that the risk committee should report regularly to the board of directors on the matters as to which the committee has delegated authority. Comment *f* to § 3.09 is applicable here.

REPORTERS' NOTE

a. Most organizations are not required by law to have a dedicated risk committee, and this committee is not common outside the financial sector. However, the oversight of risk management

has increasingly been seen as an important function of the board of directors in an organization, and therefore deserves a specialized committee. See generally GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 85-87 (2017) (discussing use of risk committees); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT: ALIGNING RISK WITH STRATEGY AND PERFORMANCE, VOL. 1 28 (June 2017) ("Some full boards retain ownership [of risk oversight] while others delegate board-level responsibilities to a committee of the board, such as a risk committee."); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 149 (2013) (describing risk committee formed for, among other reasons, "oversight of risk responses"); ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 998-999 (2011) (discussing enhanced importance of risk-management oversight in a public-company board); G20/OECD, PRINCIPLES OF CORPORATE GOVERNANCE 52 (2015) (recommending the use of a risk-management committee in a publicly traded company). But see REPORT OF THE NACD BLUE RIBBON COMM'N ON RISK GOVERNANCE: BALANCING RISK AND REWARD 12-13 (2009) (recommending against a balkanized approach to risk oversight and recommending that its overall responsibility stay with the full board).

Regulation can encourage a firm to have a board committee responsible for risk oversight. See, e.g., 17 C.F.R. § 229.407(h) (2018) (Item 407(h) of Regulation S-K, which governs disclosure by a public company, requires it to "disclose the extent of the board's role in the risk oversight of the [company], such as how the board administers its oversight function, and the effect that this has on the board's leadership structure."); NYSE, Inc., Listed Company Manual § 303A.07(b)(iii)(D) (2018) (mandating that, in a public company listed on the New York Stock Exchange, the audit committee is tasked with this oversight); id. cmt. (allowing another committee or governance body to conduct risk management, but requiring the audit committee to "discuss guidelines and policies to govern the process by which risk assessment is undertaken."). Certain firms in the financial sector must have a risk committee. Section 165(h) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. 111-203, 124 Stat. 1376 (July 21, 2010), codified at 15 U.S.C. § 5365(h) (2018), directed the Board of Governors of the Federal Reserve System to require that a publicly traded nonbank financial company supervised by it and a publicly traded bank holding company with total consolidated assets not less than $10 billion have a board risk committee composed of independent directors and advised by a risk-management expert. See also 12 C.F.R. § 252.22 (2018) (risk-committee requirement for publicly traded bank holding company having total consolidated assets of not less than $10 billion); 12 C.F.R. § 252.33 (2018) (risk-committee requirement for a large bank holding company having total consolidated assets of not less than $50 billion).

Enhanced risk oversight by the board of directors has been held not to subject the directors to increased liability. See In re Citigroup Inc. Shareholder Derivative Litigation, 964 A.2d 106, 131 (Del. Ch. 2009) ("While it may be tempting to say that directors have the same duties to monitor and oversee business risk, imposing *Caremark*-type duties on directors to monitor

business risk is fundamentally different. Citigroup was in the business of taking on and managing investment and other business risks. To impose oversight liability on directors for failure to monitor 'excessive' risk would involve courts in conducting hindsight evaluations of decisions at the heart of the business judgment of directors. Oversight duties under Delaware law are not designed to subject directors, even expert directors, to personal liability for failure to predict the future and to properly evaluate business risk.") (footnote omitted); In re Goldman Sachs Group, Inc. Shareholder Litigation, 2011 WL 4826104, at *22 (Del. Ch. Oct. 12, 2011) ("If an actionable duty to monitor business risk exists, it cannot encompass any substantive evaluation by a court of a board's determination of the appropriate amount of risk. Such decisions plainly involve business judgment."); id. n.217 ("While a valid claim against a board of directors in a hierarchical corporation for failure to monitor risk undertaken by corporate employees is a theoretical possibility, it would be, appropriately, a difficult cause of action on which to prevail. Assuming excessive risk-taking at some level becomes the misconduct contemplated by *Caremark*, the plaintiff would essentially have to show that the board *consciously* failed to implement any sort of risk monitoring system or, having implemented such a system, *consciously* disregarded red flags signaling that the company's employees were taking facially improper, and not just ex-post ill-advised or even bone-headed, business risks. Such bad-faith indifference would be formidably difficult to prove.").

b. Independence of members of a board committee tasked with risk management is found in audit-committee requirements for a publicly traded company because an audit committee is required to be composed of independent directors. See 15 U.S.C. § 78j-1(m)(3) (2018). A risk committee of both a publicly traded bank holding company with not less than $10 billion in consolidated assets and a large bank holding company with not less than $50 billion in consolidated assets must be chaired by an independent director, 12 C.F.R. § 252.22(d)(2) (2018); 12 C.F.R. § 252.33(a)(4)(ii) (2018), and include on the committee a member with risk-management expertise, see 12 C.F.R. § 252.22(d)(1) (2018); 12 C.F.R. § 252.33(a)(4)(i) (2018). The risk committee acquires risk expertise also from receiving the advice and reports of a chief risk officer or an executive-level risk committee. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 998-999 (describing these methods).

c. A risk committee of a publicly traded bank holding company with consolidated assets of not less than $10 billion and of a large bank holding company with consolidated assets of not less than $50 billion must have a "formal, written charter" approved by the institution's board of directors. See 12 C.F.R. § 252.22(c)(1) (2018); 12 C.F.R. § 252.33(a)(3)(i) (2018).

d. The duties of a risk committee are specified in varying degree of detail by regulation and practice guidelines. The risk committee of a publicly traded bank holding company with not less than $10 billion of total consolidated assets must "approve …and periodically review[ ] the risk-management policies of its global operations and oversee[ ] the operation of its global risk-management framework [a term further defined in the regulation]." See 12 C.F.R. § 252.22(a) (2018). The committee must meet quarterly and document its proceedings. See 12 C.F.R. § 252.22(c)(2) (2018). The risk committee of a large bank holding company with not less than $50

billion in total consolidated assets has the same mandate, although it is broadened to include liquidity risk management, and the same meeting requirements. See 12 C.F.R. § 252.33(a)(1) & (3)(v) (2018). This latter committee receives reports (not less than quarterly) from the company's chief risk officer, see 12 C.F.R. § 252.33(a)(3)(iv) (2018), whom the same regulation places in charge of risk management for the company, 12 C.F.R. § 252.33(b) (2018). Furthermore, under that regulation the chief risk officer must report to the risk committee, as well as to the chief executive officer, see 12 C.F.R. § 252.33(b)(3)(ii) (2018), with the reporting to the former to include information about "risk-management deficiencies and emerging risks," see 12 C.F.R. § 252.33(b)(2)(ii) (2018). The Bank for International Settlements recommends that a board-risk committee meet "periodically" with the audit committee and "other risk-relevant committees to exchange information, to ensure that all risks are identified and to make adjustments to the risk-governance framework." See BASEL COMM. ON BANKING SUPERVISION, CORPORATE GOVERNANCE PRINCIPLES FOR BANKS: GUIDELINES 15 (2014) (Principle 3, no. 74).

e. Regulations applicable to a large bank holding company with consolidated assets not less than $50 billion require that the risk committee of the board ensures that the risk-management department is independent. See 12 C.F.R. § 252.33(a)(2)(ii)(C) (2018) (this is part of the risk-management framework that the risk committee oversees). Having the risk committee approve the hiring and dismissal of the chief risk officer contributes to this independence. The risk committee must also make sure that risk management is integrated into the compensation structure of the firm. See 12 C.F.R. § 252.33(a)(2)(ii)(D) (2018). In particular, the compensation of the chief risk officer must be "consistent with providing an objective assessment of the risks" taken by the firm. See 12 C.F.R. § 252.33(b)(3)(i) (2018).

f. The risk committee of a large bank holding company with consolidated assets not less than $50 billion must regularly report to the full board. See 12 C.F.R. § 252.33(a)(3)(iii) (2018) (providing for this reporting in large banks). This reporting is critical because the identification and management of risks are the ultimate responsibility of the entire board. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK, supra, at 998-999 (discussing generally a board's responsibilities for risk oversight).

§ 3.12. Role of the Audit Committee in Compliance and Risk Management

(a) The board of directors, in its discretion, may elect to delegate to an audit committee, or to another committee or committees, part or all of its oversight of the internal audit of compliance and risk management in the organization. The committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should be:

(1) independent; and

(2) have the background or experience in internal audit to be able, individually and, when appropriate, collectively, to fulfill their delegated responsibilities.

(b) The audit committee should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's judgment, such engagement is appropriate.

(c) The audit committee may elect to operate with a written charter specifying the committee's purpose, responsibilities, functions, structure, procedures, and member requirements or limitations.

(d) The audit committee's oversight in subsection (a) should include one or more of the following responsibilities:

(1) to review and approve the internal-audit plan for compliance and risk management, and any material revisions thereto;

(2) to be reasonably informed of the staffing and resources allocated by executive management to the internal-audit department and to satisfy itself that they are adequate and that the department is sufficiently independent and has the appropriate authority to perform its responsibilities;

(3) to approve the appointment, terms of employment, and dismissal of the chief audit officer;

(4) to communicate regularly with the chief audit officer on the organization's internal-control environment, including its compliance and risk management;

(5) to meet at reasonable intervals with executive management and the chief audit officer to review the effectiveness of, inadequacies in, and any necessary changes to the organization's internal-audit function;

(6) to confer with executive management, the chief legal officer, and the chief audit officer:

(A) to address any material failure in the internal audit of compliance and risk management, and

(B) to approve or ratify any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such failure;

(7) to review, in consultation with the chief audit officer and, if applicable, the external auditor, the results of the internal audit and, if applicable, those of the external audit, as both pertain to compliance and risk management, and, in light of that review:

(A) to consider the effectiveness of and inadequacies in the organization's compliance program, code of ethics, and risk-management framework and program, and any necessary changes to them, and

(B) to evaluate any material violation or failure of the compliance program and the code of ethics, material deviation from or failure of the risk-management framework and program, or material failure in the internal audit of compliance and risk management that the internal or external audit revealed, and the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization as it pertains to compliance and risk management;

(8) to meet with executive management, the chief compliance officer, the chief risk officer, the compliance and ethics committee, the risk committee, or any other board committee that is concerned with compliance and risk management to discuss any conclusions at which it arrived from the processes stated in subsection (d)(7);

(9) with the assistance of the chief legal officer, the chief audit officer, outside legal counsel, or outside consultants, to direct its own investigation of any material failure of the internal audit;

(10) to perform the responsibilities of the compliance and ethics committee and the risk committee, as provided in §§ 3.10 and 3.11, if the board elects to delegate those responsibilities to the audit committee; and

(11) to report regularly to the board of directors on the responsibilities delegated to it.

Comment:

a. General. An audit committee is well established by law and practice as an essential board committee in every publicly traded company and in many organizations of comparable size and operations. The American Law Institute's Principles of Corporate Governance: Analysis and Recommendations deal extensively with the audit committee in a publicly held corporation, clearly establishing its composition, structure, and responsibilities. Those Principles observe that the audit committee contributes to board oversight by reviewing periodically a firm's procedures for producing financial information, its internal controls, and the engagement and independence of the external auditor. Among other powers, as those Principles also recommend, the audit committee oversees the firm's relationship with the external auditor, reviews the annual financial statements and the external audit of them, evaluates, in consultation with the external auditor and chief audit officer (§ 1.01(b)), the adequacy of the firm's internal controls, regularly communicates with the external auditor and the chief audit officer, and approves the hiring and dismissal of that officer.

This Principle is intended only to supplement that earlier work by identifying the responsibilities for the oversight of the internal audit of compliance and risk-management that a board of directors may delegate to its audit committee. These additional responsibilities all arise from the audit committee's established oversight of internal controls, which include compliance and risk management. This Principle sets forth the ways in which the audit committee may conduct this oversight, chiefly involving its review of the results of the internal audit of these internal-control functions performed by the chief audit officer. As in the case of §§ 3.10 and 3.11, this Principle is more appropriate for a publicly traded company or an organization of comparable size and operations than it would be for a smaller organization. However, given an organization's circumstances, including its size, resources, and legal obligations imposed on it, a board of directors may have only an audit committee, which is responsible for oversight of all internal controls, including compliance and risk management, as provided in subsection (d)(10).

b. Composition, resources, and charter. Subsection (a) establishes the board's delegation to the audit committee, and the committee's recommended composition and basic structure. With respect to the independence and background or experience of committee members, it tracks the language in § 3.09(b), and Comment *c* to that Principle applies equally here. Similarly, subsections (b) and (c) track the language of, respectively, § 3.09(c) and (d) about the committee's satisfaction that it has the resources to fulfill its responsibilities and having a charter that, among other things,

sets forth the committee's responsibilities. Comments *d* and *e* of § 3.09 explain the purposes of these provisions.

c. Committee responsibilities in general. Subsection (d) sets forth the recommended responsibilities of the audit committee for the oversight of the internal audit of compliance and risk management that are, for the most part, the same as those of the board of directors. Subsection (d)(1) recommends that the audit committee's responsibilities include the review and approval of the plan for the internal audit of compliance and risk management. The subsection echoes the responsibility of the board of directors set forth in § 3.08(b)(5) and discussed in Comment *e* to that Principle. The internal-audit function (§ 1.01(ff)) is the well-recognized "third line of defense" (§ 1.01(fff)) for compliance and risk management because it audits these internal-control functions in an organization (as well as an organization's other operations and its processes for producing financial statements). Through the internal audit (§ 1.01(dd)), the internal auditors check whether organizational actors are in fact following the compliance program, the code of ethics, the risk-management framework, and the risk-management program, and they identify problems, failures, or deviations in them. Subsection (d)(1) recommends that the audit committee review the internal-audit plan so that the committee understands how the internal auditors will test compliance and risk management in the organization. The committee should also review any revisions to that plan that are made to take into account, among other things, changes in the organization's business or affairs, legal obligations, or risks. Subsection (d)(2) repeats the board's responsibility to satisfy itself that the internal-audit department has adequate resources and sufficient independence in the organization, which is stated in § 3.08(b)(6). Comment *f* of § 3.08 is applicable here.

d. Committee responsibilities; chief audit officer's reporting to and communicating with the committee. Subsections (d)(3) and (4) echo the board responsibilities set forth in § 3.08(b)(7) and (8) and discussed in Comment *g* to that Principle, and they reflect the two meanings of organizational reporting with respect to the chief audit officer. These subsections are particularly important for establishing the audit committee's primacy over the organization's oversight of the internal audit of compliance and risk management when the board has determined to delegate this responsibility to it. The chief audit officer may be a member of executive management who "directly reports" to, and would thus be under the line of authority of, the chief executive officer, who would ordinarily propose a person for that position and decide when to terminate the officer. Alternatively, the chief audit officer may be lower in the organization's hierarchy and be a direct

report to another member of executive management (or to an officer below the level of executive management). In any of these cases, under subsection (d)(3), the audit committee approves the hiring, terms of employment, and dismissal of this officer. The committee's approval of the engagement, and particularly the dismissal, of the chief audit officer is designed to provide another layer of oversight of these personnel actions and helps ensure that the officer is not terminated merely for having raised an important internal-control issue in the organization. Subsection (d)(3), moreover, reflects that this committee power over the hiring and dismissal of a chief audit officer is mandated by law or regulation in certain domains. As provided in this subsection, the committee's oversight extends to the chief audit officer's terms of employment, which include the compensation unless the board compensation committee is responsible for it.

Subsection (d)(4) highlights that the chief audit officer should regularly communicate, in the sense of providing or reporting information, directly with the audit committee about the organization's internal-control environment, particularly its compliance and risk management. The following example shows the benefit of such regular communication:

> In its regular meetings with the chief audit officer, the audit committee of Company hears about pressure put on that officer by senior executives to downplay occasional deviations from risk limits that result from Company transactions. As a result of this communication, the audit committee should question executive management about this pressure and explore whether it is leading to violations of the risk-management program.

This communication would be separate from and independent of the officer's reporting to the chief executive and other members of executive management. It enables the audit committee better to conduct its oversight of the internal-audit function by hearing directly from the chief audit officer without the communication being filtered or influenced by members of executive management. The committee determines the scope and frequency of any communication and reporting, but its regularity helps ensure that no unintended negative signal is sent by a meeting between the executive and the audit committee, which might occur if this kind of meeting took place only at the committee's or officer's request.

e. Committee responsibilities; reviewing the effectiveness of the internal-audit function, and dealing with a material failure of the internal audit. Under subsection (d)(5), the audit committee may be delegated the responsibility of the board of directors, as stated in § 3.08(b)(9) and as explained in Comment *h* to that Principle, to evaluate the effectiveness of the organization's

internal-audit function, and to identify and to address inadequacies in it. The focus of this evaluation here is on its ability to conduct a sufficient audit of compliance and risk management. The audit committee conducts this evaluation with executive management and the chief audit officer. Accordingly, this subsection has a complementary provision in § 3.14(b)(9) and § 3.17(b)(8)(B), which require these organizational actors to meet with the board of directors or the audit committee for this purpose. Subsection (d)(6) tracks § 3.08(b)(10) when it has executive management reporting to the audit committee of a material failure of the internal audit of compliance and risk management and on the committee's approval or ratification of disciplinary or remedial action that will be or has been taken as a result, including reporting to a regulator. The audit committee may wish to refer this matter, particularly discipline, regulatory reporting, and remediation, to the board of directors for its decision.

f. Committee responsibilities; reviewing internal-audit results. Subsection (d)(7) provides that the audit committee should review with the chief audit officer the results of the internal audit of compliance and risk management. See § 3.17(b)(8)(D) and (E) (providing for chief audit officer's meeting on the internal-audit results). If the organization's external auditor covers these internal-control functions in its external audit, the audit committee should review those results as well. See § 5.23(b) and (c) (external auditors' uncovering of compliance violations). The audit committee may decide to conduct these reviews without the chief executive officer and other senior executives being present. The purpose of the review of audit results is twofold. Under subsection (d)(7)(A), which focuses on the effectiveness of and inadequacies in the organization's internal-control programs, the committee is gaining an understanding whether or to what extent organizational actors are following the compliance program, the code of ethics, and the risk-management framework and program and thus whether these programs are achieving their purposes. Under subsection (d)(7)(B), the review of audit results may also alert the committee to material violations or failures of the organization's compliance program or code of ethics, material deviations from or failures of the risk-management framework and program, or material failures in the internal audit of compliance and risk management, and may lead it to evaluate the chief audit officer's identification of the cause or causes for them. The audit committee may conduct this review and consultation as a separate procedure or as part of its review relating to all the results of the internal and external audits.

g. Committee responsibilities; meeting with executive management and other board committees. Subsection (d)(8) provides that the audit committee, when appropriate and if applicable, should communicate with executive management, the compliance and ethics committee, the risk committee, and any other board committees concerned with compliance and risk management its conclusions from the review of audit results and consultation with the chief audit officer described in subsection (d)(7). The purpose of this communication would be for the audit committee to ensure that other organizational actors, particularly board committees with delegated oversight of compliance and risk management, are properly recognizing and addressing the findings from the internal audit and external audit (if applicable) relating to the effectiveness of and problems in these internal-control functions. As a result of its other responsibilities, such as its oversight of internal reporting, the audit committee may also have other information on compliance or risk management to convey to executive management, the chief compliance officer, the chief risk officer, and these committees.

h. Committee responsibilities; conducting its own investigation of material failure of the internal audit. Subsection (d)(9) reflects the audit committee's responsibility to conduct its own investigation of a material failure of the internal audit of compliance and risk management, rather than relying upon one conducted by executive management. It thus echoes the board's responsibility set forth in § 3.08(b)(11)(A), and Comment *j* to that Principle explains the reasons for this investigatory responsibility.

i. Committee responsibilities; serving as the compliance and ethics committee or risk committee. Subsection (d)(10) recognizes that the board of directors may require the audit committee to undertake the responsibilities of a compliance and ethics committee or the risk committee. This recognition reflects that the audit committee in many organizations, such as publicly traded companies, has been expressly given the oversight of compliance and risk and that, as a result, there may be no separate board compliance and ethics committee and risk committee.

j. Committee responsibilities; reporting to board of directors. Subsection (d)(11) is modeled upon § 3.09(e) in its providing that the audit committee should report regularly to the board of directors on the matters as to which the committee has delegated authority. Comment *f* to § 3.09 is applicable here.

REPORTERS' NOTE

a. This Principle draws inspiration from, and is intended only to supplement, the treatment of the audit committee in The American Law Institute's Principles of Corporate Governance. Those Principles provide, among other things, that the audit committee should review the reports of internal auditors and the results of external audits and, in consultation with the external auditor and the chief audit officer, "[c]onsider … the adequacy of the corporation's internal controls." Principles of Corporate Governance: Analysis and Recommendations § 3A.03(e) & (g) 116 (AM. LAW INST. 1994). Although that Principle did not so describe them, see id. Comment *c*, at 119, internal controls are understood today to include compliance and risk management. The Corporate Law Committee of the American Bar Association Business Law Section provides more support for this Principle when it recommends that the audit committee meet with the chief audit officer to discuss, among other things, the internal-audit plan, problems revealed by the internal audit, and proposed corrective actions and their implementation (again, without specifying that the internal audit covers compliance and risk management). See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 1021 (2011). It is well accepted in practice and in theory that the mission of the internal-audit function includes reviewing compliance and risk management in an organization; it is the "third line of defense" for these internal-control functions. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 154 (2013) (describing the broad mandate of internal auditors, as this third line of defense, to cover compliance and risk management, among other organizational operations and systems). As noted in § 3.09, Comment *a*, in many organizations the audit committee alone oversees compliance, risk management, and, presumably, internal audit.

§ 3.13. The Role of the Compensation Committee in Compliance and Risk Management

(a) If the board of directors elects to establish a compensation committee, that committee should consult periodically with any other committee of the board of directors having oversight of compliance and risk management:

(1) to consider its views as to whether the organization's compensation policies and practices under the purview of the compensation committee adequately support or undermine the organization's compliance program, code of ethics, and risk-management framework and program; and

(2) to discuss with it how these policies and practices should be revised to provide this support if the other committee believes that such revision is appropriate.

(b) The compensation committee should also report regularly to the board of directors on the revisions to the organization's compensation policies and practices that result from this consultation.

Comment:

a. General. The compensation committee is established by law and practice as an essential committee of the board of directors in publicly traded companies and other organizations of comparable size and operations. This Principle is thus intended for those firms, not for organizations that do not have this board committee. The compensation committee, the composition, structure, and responsibilities of which are well defined, is generally tasked with overseeing, and recommending to the full board, the terms of employment and the compensation of senior executives, particularly the chief executive officer. This Principle does not discuss this committee in general, but focuses only on certain of its responsibilities relating to compliance and risk management.

These responsibilities include that the committee ensure that compensation for the organizational actors under its mandate (i.e., again, generally senior executives) reflects the extent of their adherence to the organization's compliance program, code of ethics, and risk-management framework and program. The goal here is to ensure that executives take compliance and risk management into account in their decisionmaking because their compensation will adequately and appropriately reflect the extent of their adherence to the compliance and risk-management programs. See § 4.08(b) (recommending that risk-management concerns be taken into account in the design of employee compensation) and Comment *b* (recommending that compensation not encourage excessive risk-taking); § 5.06, Comment *m* (discussing how compensation may incentivize compliance); § 5.07, Comment *b* (discussing compliance risk posed by compensation arrangements); § 5.16(a) (recommending that an employee's compensation reflect compliant conduct); and § 6.02, Comment *c* (discussing importance of an organization's compensation policies in ensuring deterrence of misconduct). To fulfill this responsibility, under subsection (a) the compensation committee should consult periodically with and consider the views of any other board committee with oversight of compliance and risk management, such as the compliance and ethics committee, the risk committee, and the audit committee, as to whether the compensation policies and practices in question adequately support and do not undermine its compliance program, code of ethics, and risk-management framework and program. The use of the word

"consider" suggests that the compensation committee should take into account the views of the other committees in their respective domains (e.g., the risk committee as to how well compensation policies and practices support the risk-management framework and program). If a consulted committee identifies a problem in the alignment of compensation policies and practices with an internal-control function, the compensation committee should discuss with that committee revisions that will address the consulted committee's concerns. The full board of directors could resolve any disagreement between committees on such matters. Under subsection (b), the compensation committee should also regularly report to the board any revisions to the compensation policies and practices that result from its consultation with other board committees.

b. Interaction between the compensation committee and other board committees. This Principle contemplates that the board of directors, or the committees themselves, will structure the consultation between the compensation committee and another board committee as it or they see fit. For example, the meetings could involve just the committee chairpersons. This Principle recommends that the meetings be periodic because this kind of contact among committees (or committee chairpersons) also ensures that compensation policies and practices reflect developments in compliance and risk management in the organization.

c. Committee's limited mandate. This Principle acknowledges that the compensation committee's oversight of compensation policies and practices may be limited to those involving senior executives. As provided in § 3.14, Comment *a*, executive management should ensure that the organization's general and operating-level compensation policies and practices adequately support its compliance program, code of ethics, and risk-management framework and program. If, however, the compensation committee has a broader mandate than executive compensation, the guidance of this Principle would apply in those circumstances as well. For example, the compensation committee, rather than the board committee having oversight over a particular internal-control function, may be tasked with determining or approving the compensation of the internal-control officer responsible for that function. The compensation committee would thus have to ensure that the officer's compensation supports the internal-control function by both incentivizing the officer and supporting the officer's independence from the organization's business or affairs.

REPORTERS' NOTE

a. This Principle reflects the recommended approach for a compensation committee to take compliance and risk management into account in setting the compensation policies and practices under its oversight. This committee in a publicly traded company should consider how well the firm's compensation policies and practices reflect its compliance and risk-management programs because the firm must disclose "risks arising from the [company]'s compensation policies and practices for its employees" if they "are reasonably likely to have a material adverse effect on the [company]." 17 C.F.R. § 229.402(s) (2018). Directors are advised to pay attention to risks in a company's "incentive structure." See, e.g., REPORT OF THE NACD BLUE RIBBON COMM'N ON RISK GOVERNANCE: BALANCING RISK AND REWARD 17 (2009). Federal financial regulators have been mandated to prohibit in large financial firms "incentive-based compensation arrangements … [that] could lead to material financial loss." See 12 U.S.C. § 5641(a)(2) (2018). See also Incentive-Based Compensation Arrangements, Exchange Act Release No. 77,776, 81 Fed. Reg. 37,670 (June 10, 2016) (proposed rulemaking by financial regulators on this subject pursuant to the legislation). Indeed, this Principle takes an approach similar to the one offered in the proposed regulation, which requires a compensation committee of a large financial institution to receive input from the risk and audit committees on "the effectiveness of risk measures and adjustments used to balance risk and reward in incentive-based compensation arrangements." See id. at 37,812 (proposed Federal Reserve rule 12 C.F.R. § 236.10(b)(1) for institutions with consolidated assets greater or equal to $1 billion). Academic literature suggests that organizations can deter, or increase the probability of, crime by their actors through the firms' policies on, among other things, compensation. See Jennifer Arlen, *Corporate criminal liability: theory and evidence,* in RESEARCH HANDBOOK ON THE ECONOMICS OF CRIMINAL LAW 144, 165 (A. Harel & K. Hylton eds., 2012) (discussing how linking compensation to short-term firm benefits can encourage employee crime, whereas linking it to firm long-term benefits deters it); id. at 186 (explaining that compensation policy is a particularly important preventive measure that organizations could use to deter crime by organizational actors). However, survey data suggests that many organizations do not make compliant conduct a factor in employee compensation. See, e.g., KPMG, THE COMPLIANCE JOURNEY: BOOSTING THE VALUE OF COMPLIANCE IN A CHANGING REGULATORY CLIMATE 13 (2017) (survey of U.S. chief compliance officers finds that only 61% of them say that compliant conduct is a factor in compensation decisions).

TOPIC 4

EXECUTIVE MANAGEMENT

§ 3.14. Executive Management of Compliance and Risk Management

(a) As part of its management of the organization's business or affairs, executive management should direct the implementation of effective compliance, risk management, and internal audit in the organization.

(b) Specifically, the responsibilities of executive management under subsection (a) should include the following:

(1) to be informed of the major legal obligations applicable to, and the main values in the code of ethics for, the organization, its employees, and agents;

(2) in collaboration with, among others, the organization's chief compliance officer, to direct the formulation and implementation of the compliance program and the code of ethics, and any material revisions thereto;

(3) to be informed of the material risks to which the organization is or will likely be exposed;

(4) in collaboration with, among others, the organization's chief risk officer, to direct the formulation and implementation of the risk-management framework and risk-management program, and any material revisions thereto;

(5) to provide support to the chief audit officer who implements an internal-audit plan for compliance and risk management, and any material revisions thereto, and to be informed of the results of the internal audit of these internal-control functions;

(6) to ensure that the internal-control departments of compliance, risk management, and internal audit are adequately staffed, have adequate resources, are sufficiently independent, and have the appropriate authority to perform their respective internal-control responsibilities;

(7) subject to the approval of the board of directors, or a board committee, to appoint and dismiss, and to determine the terms of employment of, the chief compliance officer, the chief risk officer, and the chief audit officer;

(8) to communicate regularly with these internal-control officers;

(9) to meet at reasonable intervals with each of these internal-control officers to assess the effectiveness of and to identify inadequacies in the internal-control function headed by that officer, and to authorize, and to direct the implementation of, any necessary changes to it;

(10) to confer with the chief legal officer and the appropriate internal-control officer:

(A) to learn about any material violation or failure of the compliance program or the code of ethics, any material deviation from or failure of the risk-management program, or any material failure of the internal audit of compliance and risk management, and

(B) to resolve upon any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such violation, failure, or deviation; and

(11) accompanied by the appropriate internal-control officer, to meet with the board of directors, or a board committee:

(A) to obtain its approval for the compliance program and the code of ethics, the risk-management framework and risk-management program, and the internal-audit plan for compliance and risk management, and any material revisions thereto,

(B) to report on their implementation,

(C) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the internal-control function headed by the accompanying internal-control officer,

(D) to notify it of any material violation or failure of the compliance program or code of ethics, any material deviation from or failure of the risk-management program, or any material failure of the internal audit of compliance and risk management, and to propose for approval or to identify for ratification any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation, failure, or deviation, and

(E) to confer about any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them, or the material risks to which the organization is or may be exposed and the effectiveness of the risk-management program in addressing them, and the adequacy of such disclosure or reporting.

Comment:

a. General. Executive management is defined in § 1.01(v) as the senior executives of an organization, or even a subset of that group. These generally include the chief executive officer (§ 1.01(d)) and the chief financial officer of the organization, as well as others. The senior executives conduct the high-level management of the organization's business or affairs. This Principle states that their management responsibility includes directing the implementation of effective compliance, risk management, and internal audit in the organization. While the board of directors oversees the internal-control functions, see § 3.08, executive management, assisted by the chief compliance officer, the chief risk officer, and the chief audit officer, proposes the compliance program and code of ethics, the risk-management framework and program, and the related internal-audit plan, as well as the structure of governance of these internal-control functions, for the board's approval. It then proceeds to direct their implementation. This Principle thus emphasizes that the initiative and responsibility for establishing effective compliance, risk management, and internal audit chiefly lie with executive management who must ensure that the the organization's practices, including those involving compensation, are adequately aligned with the internal-control functions. The board may delegate its oversight of executive management on these internal-control functions to one or more of its committees, such as a compliance and ethics committee, a risk committee, and an audit committee, see § 3.10, § 3.11, and § 3.12.

How the senior executives apportion the responsibilities for compliance, risk management, and internal audit in an organization is left to their discretion, although applicable law and practice may dictate the allocation of certain tasks to specific executives. This Principle and its Comments, therefore, refer simply to "executive management" or to "senior executives" without allocating duties to senior-executive positions. This Principle recognizes, however, that, given its paramount

position in organizations, the chief executive officer bears the primary managerial responsibility for establishing effective compliance, risk management, and internal audit, although this officer is likely to direct other executives to assist in fulfilling this responsibility. Moreover, it acknowledges that other senior executives have well-established roles in these internal-control functions. For example, since a chief financial officer is generally responsible for monitoring the financial condition of an organization and for its financial reporting, that officer meets periodically with both the chief audit officer and external auditors to review, among other things, the adequacy of the organization's financial and other internal controls, which review could include an assessment of the effectiveness of its compliance and risk-management programs.

This Principle is designed primarily for a publicly traded company or an organization of comparable size and operations. It thus recognizes that a board of directors of other organizations (or even these) may apportion the responsibilities for compliance, risk management, and internal audit in different ways and may assign to executive management oversight, as well as management, duties with respect to the internal-control functions. It also acknowledges that senior executives may themselves allocate the managerial responsibilities for compliance, risk management, and internal audit in many different ways. However, it strongly recommends that executive management take overall responsibility for directing the implementation of the internal-control functions in an organization.

b. Executive responsibilities in general. The paragraphs of subsection (b) specify the responsibilities that executive management should perform in directing the implementation of compliance and risk management, and the related internal audit. Many, if not most, of them characterize those of senior executives in a publicly traded company, and, in some cases, certain of them are mandated by law or regulation. The responsibilities are modeled upon, albeit different from, those of the board of directors that are laid out in § 3.08. Subsection (b) presumes that the organization has stand-alone compliance, risk-management, and internal-audit departments with officers responsible for them to assist executive management, although it is flexible enough to cover situations in which the departments are combined. Even if the individual departments exist, executive management remains responsible for directing the implementation of effective compliance, risk management, and internal audit.

c. Executive responsibilities; compliance. As stated in subsection (b)(1), executive management should be informed of the major legal and ethical obligations of the organization, its

employees, and agents. The language here is identical to that used in § 3.08(b)(1) for members of the board of directors and thus focuses on the kind of high-level information about significant obligations and compliance risks (§ 1.01(n) (definition)) that is appropriate for those acting in an executive role of this nature. It is likely that, given its managerial position, executive management acquires a more detailed knowledge of an organization's legal and ethical obligations than would directors. As in the case of the board of directors, moreover, § 3.06 explains some of the ways by which executive management acquires that knowledge. It is expected that the chief legal officer and the chief compliance officer (or organizational actors performing these roles) advise senior executives on legal and ethical obligations of the organization and its employees, and on the risks arising from noncompliance with them.

Subsection (b)(2) clarifies that senior executives direct the formulation and implementation of the compliance program (which includes compliance policies and procedures, § 1.01(l)) and the code of ethics, as well as any material revisions to them, in collaboration with the organization's chief compliance officer and the compliance department, which generally means compliance officers and compliance personnel (or those performing these organizational roles). The definitions of the program and the code are found in § 1.01(m) and § 1.01(g), their respective features are provided in § 5.06 and § 5.37, and § 3.15 deals with the chief compliance officer's and compliance personnel's involvement in their design. Because not all organizations have a code of ethics, an organization's ethical standards may be embodied in the compliance policies and procedures or may just be informal guidelines. Since by its terms the compliance program assigns responsibility for compliance to organizational actors, see § 3.03 (governance map for compliance and risk management), it also directs the implementation of the governance of compliance—the chain of decisionmaking and responsibilities applicable to this internal-control function and its structure in the organization. Other organizational actors, such as the chief legal officer, and outside consultants may assist and advise executive management on these matters.

As follows from the above discussion, because executive management is responsible for directing the implementation of the compliance program, the code of ethics, and the structure of the governance of compliance, senior executives should understand them at a greater level of detail than would directors, but likely not to the extent required of the chief compliance officer, who is a specialist in compliance. They should thus have a full understanding of the ways in which the compliance program identifies and addresses compliance risks and issues, and structures the

organization's compliance governance, particularly since they must justify and explain the program to the board of directors.

d. Executive responsibilities; risk management. Similarly, under subsection (b)(3), executive management, like the board, should be informed of and understand the material risks (those in addition to the legal and compliance risks that are dealt with in subsections (b)(1) and (b)(2)) to which the organization is or will likely be exposed. See § 4.05 (discussing classification of risk). This understanding could come from their background, experience, and education, as explained in § 3.06, from the education and advice provided by the chief risk officer, see § 3.16, or from meetings with executive-level risk committees. Since executive management will be justifying and directing the implementation of the risk-management framework and program, its understanding of these risks, particularly the residual risk, see § 1.01(ss) (definition), will likely be more extensive than that held by directors.

As subsection (b)(4) provides, executive management should direct the formulation and implementation of the organization's risk-management framework, § 1.01(aaa), including its risk-appetite statement, § 1.01(uu), if one is prepared, and the risk-management program that implements this framework, § 1.01(ccc) (definition of a risk-management program) and § 4.06 (identifying program elements). It does the same for the structure of governance of risk management. Since risk management is closely interconnected with the management of the business or affairs of an organization, executive management is likely to be more directly involved with it than it would be for compliance. While senior executives are responsible for the risk-management framework and program, for any material revisions to them, and for presenting, explaining, and justifying them to the board of directors, they would likely work closely with the chief risk officer and risk-management personnel, the specialists of risk management, see § 3.16(b)(1), as well as with any executive-level risk committees, to fulfill these responsibilities. Moreover, they should satisfy themselves that the risk-management framework and program adequately manage the kinds and levels of risk incurred by the organization and that such risks, particularly the residual risks, are reasonable in light of the organization's business and affairs.

e. Executive responsibilities; internal audit. Subsection (b)(5) highlights that executive management should provide support to the chief audit officer in the latter's implementation of the internal-audit plan, § 1.01(ee), for compliance and risk management. Senior executives should defer to the chief audit officer and internal-auditors in the design and implementation of the

internal audit plan and its governance. See § 3.17(b)(1)(B). But they should understand how, under this plan, the internal auditors propose to check on the effectiveness of the compliance and risk-management programs, for they must explain this to the board of directors. Executive management will also want to ensure that the chief audit officer has the organizational independence to identify problems (if any) in compliance and risk management that the internal audit reveals and to recommend modifications to the compliance program, the code of ethics, the risk-management framework and program, or to the governance of compliance or risk management. See § 3.17(b)(7)(A).

f. Executive responsibilities; providing adequate staffing and resources for the internal-control departments. Subsection (b)(6) underscores senior executives' responsibility to ensure that the internal-control departments of compliance, risk management, and internal audit have proper staffing and adequate resources, and that they have the independence and authority to perform their duties. See § 5.05(d) (providing that adequate funding, staffing, and other resources are an element of an effective compliance program). Staffing and the allocation of organizational resources are paradigmatic managerial matters. Furthermore, as an organizational practice, executive management has the power to ensure that the internal-control officers and personnel are independent from other organizational actors and have the appropriate authority so that these actors will listen to and be guided by them on internal-control issues.

g. Executive responsibilities; reporting of and communications from internal-control officers. Subsection (b)(7) and (8) reflect the two meanings of organizational reporting with respect to the chief compliance officer, the chief risk officer, and the chief audit officer. These officers may in fact be members of executive management who "directly report" to, and are thus under the direct line of authority of, the chief executive officer, who proposes persons for those positions, decides whether to terminate them, and approves their terms of employment. Alternatively, they may be lower in the organization's hierarchy and be a direct report to other members of executive management (or to officers under executive management). In any of these cases, under subsection (b)(7), executive management, or someone under the direct authority of executive management, approves the hiring, terms of employment, and dismissal of these officers. However, Principles elsewhere foster the independence of the internal-control officers by making these matters also subject to oversight by the board or a board committee. See § 3.08(b)(7), § 3.10(d)(4), § 3.11(d)(4), and § 3.12(d)(3). Moreover, depending upon where these officers stand in the

organizational hierarchy, executive management directly or indirectly determines their compensation.

Subsection (b)(8) highlights that these internal-control officers generally communicate, in the sense of reporting or providing information, with the chief executive officer and other senior executives. This enables executive management to hear directly from them when they are not otherwise members of executive management, without the communication being filtered or influenced by others in the organizational hierarchy. Given executive management's responsibility for compliance, risk management, and internal audit, the reporting should be regular and frequent. The reporting is in addition to the officers' direct reporting to the board or a board committee, as provided in § 3.08(b)(8), § 3.10(d)(5), § 3.11(d)(5), and § 3.12(d)(4).

h. Executive responsibilities; meeting with internal-control officers on effectiveness of the internal-control functions. Subsection (b)(9) provides that executive management should meet at regular intervals with each designated internal-control officer (i) to assess the effectiveness of and to identify inadequacies in the compliance function, the risk-management function, the related internal audit function, and the governance of these internal-control functions, and (ii) to approve, and to help direct the implementation of, any necessary changes to them. See § 5.06(o) (providing, as one feature of a compliance program, its periodic review and reaffirmation by senior executives). Executive management should not passively accept the representations of an internal-control officer made in these meetings. For example, a chief executive officer would not be fulfilling this responsibility if he or she did not read, and then question the chief compliance officer in the meeting about, a report prepared by that officer concerning the organization compliance program. Executive management, accompanied by the appropriate internal-control officer, then reports on the results of the assessment and the proposals for changes to the board of directors, or to one of the board committees. See § 3.08(a)(9), § 3.10(d)(6), § 3.11(d)(6), and § 3.12(d)(5). This assessment also affords executive management a good opportunity to learn of recent significant legal developments or new material risks facing the organization and to understand and to approve how the compliance and risk-management programs will address them. This kind of annual assessment has become the practice in many organizations and is mandated by regulation in certain industries.

i. Executive responsibilities; determinations on organizational responses to a material violation or failure of, or deviation from, an internal-control program. Under subsection (b)(10),

executive management confers with the appropriate internal-control officer to learn about any material violation or failure of, or deviation from, an internal-control program and to resolve upon any material remedial and disciplinary measures to be taken, including any reporting to be made to a regulator, with respect to such violation, failure, or deviation. The chief legal officer should generally be included in the consultation because that officer is responsible for legal advice on the organization's response to the violation, failure, or deviation. This subsection is the necessary counterpart to subsection (b)(11)(D), § 3.08(b)(10), § 3.10(d)(7), § 3.11(d)(7), and § 3.12(d)(6) & (d)(7)(B), which require that executive management report on these issues to the board of directors or to a board committee for approval or ratification. Like the board, executive management should generally focus on a material violation or failure of the organization's compliance program or the code of ethics, a material deviation from or failure of the risk-management program, or a material failure of the internal audit of compliance and risk management—not on immaterial violations, failures, or deviations that the appropriate internal-control officer could address. "Material" here includes a violation, failure, or deviation that might not be financially significant to the organization, but that could cause, or could have caused, reputational or other significant harm to it. See § 1.01(kk). However, because of its managerial position, executive management must be sensitive to how a pattern of minor violations, failures, or deviations could indicate a potentially serious problem or breakdown in the compliance or risk-management program.

Moreover, in all but the most significant of violations, failures, or deviations, which demand immediate reporting to and resolution by the board of directors or a board committee, executive management should in the first instance determine the material remedial or disciplinary measures in response to them, which could include clawbacks of compensation from organizational actors who engaged in the misconduct and recompense to third parties injured as a result of it. See § 5.16(a) (providing that noncompliant conduct should be a factor in employee compensation) and § 5.17 (providing for nonmonetary discipline for compliance violations). In addition, executive management must exert leadership in directing the organization's response to a material violation, failure, or deviation so that it is unified and comprehensive, rather than allowing the response to be made by organizational actors who could work at cross-purposes. Finally, in rare circumstances, executive management may have to authorize an immediate response to a material violation, failure, or deviation, such as the reporting to a regulator about a

major breakdown in the risk-management program, and then seek the board's ratification for this response.

j. Executive responsibilities; reporting to the board of directors. Subsection (b)(11) is the counterpart to § 3.08(b)(2), (4), (5), (9), and (10), and both Principles provide for reporting by executive management to the board of directors on compliance, risk-management, and internal-audit matters. See also § 3.10(d)(2), (6), (7), and (9); § 3.11(d)(2), (6), (7), and (9); § 3.12(d)(1), (5), (6), and (8) (regarding executive management's reporting to board committees responsible for oversight of an internal-control function). This subsection underscores the board's governance supremacy in these domains by proposing that executive management seek its approval for the compliance program and the code of ethics, the risk-management framework and program, and the internal-audit plan, as well as any changes thereto. In subparagraphs (B) and (C), it also directs senior executives to meet with the board to report on the implementation of the internal-control programs and the effectiveness of, inadequacies in, and any necessary changes to the internal-control functions. As a necessary counterpart to subsection (b)(10), under subparagraph (D) executive management should alert the board of directors to any material violation, failure, or deviation of the foregoing internal-control programs and any resulting disciplinary or remedial measures taken or to be taken, including reporting to a regulator made or to be made. The matters covered by subparagraph (E) have no counterpart in § 3.08, but they are addressed in § 3.10(d)(8) and

§ 3.11(d)(8), which provide a more expansive discussion of compliance and risk oversight in enumerating the responsibilities of a compliance and ethics committee and a risk committee. Under subparagraph (E), executive management, together with the chief legal officer and the appropriate internal-control officer, may confer with a board committee to elicit its review and approval of mandatory or discretionary disclosure and regulatory reporting about the organization's compliance or risk-management program. As noted in § 3.10, Comment *f*, and § 3.11, Comment *f*, which discuss the disclosure and reporting in more detail, this subparagraph is likely to be relevant primarily to a large organization that is a reporting company under the Securities Exchange Act of 1934 or that is in a highly regulated industry.

REPORTERS' NOTE

a. It is now well established, and supported by numerous authorities, that senior executives are primarily responsible for directing the formulation and implementation of effective compliance

and risk-management programs, as well as internal audit, as part of the internal control in their organizations. Together with all the employees and agents of an organization, they are its "first line of defense" for these internal-control functions. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 147 (2013) ("Management and other personnel on the front line provide the first line of defense…."); id. at 149-152 (describing senior management's duties on internal control). Among the senior executives, the chief executive officer, or its equivalent, has the primary responsibility for this task and must direct the other officers in its execution. See id. at 149 (the CEO "is responsible for designing, implementing, and conducting an effective system of internal control"); GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 127 (2017) (discussing the chief executive officer's compliance role). Under the U.S. Sentencing Guidelines, "[h]igh-level personnel [who include executive officers] of the organization shall ensure that the organization has an effective compliance and ethics program…." See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(B) 503 (2016). One "hallmark" of an effective compliance program is that senior executives are committed to and enforce it. See Department of Justice Criminal Division and Securities and Exchange Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act, p. 57.(asking "whether senior management has clearly articulated company standards, communicated them in unambiguous terms, adhered to them scrupulously, and disseminated them throughout the organization"). See also Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8988 (Feb. 23, 1998) ("It is incumbent upon a hospital's corporate officers and managers to provide ethical leadership to the organization and to assure that adequate systems are in place to facilitate ethical and legal conduct."); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS —GUIDELINES, ISO 19600 8 (2014) (paragraph 5.1, "top management takes responsibility for ensuring that the commitment to compliance of the organization is fully realized").

b. There is general support for the proposition that executive management proposes compliance and risk-management programs, and the related internal-audit plan for them, to the board of directors for its approval and then directs their implementation. Guidance suggests that senior executives generally delegate the responsibility for the design of these programs to the appropriate internal-control officer and associated personnel, and to others inside or outside the organization with the necessary expertise. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 149 (noting that the chief executive officer "delegat[es] to various levels of management the design, implementation, conduct, and assessment of internal control at different levels of the entity (e.g., processes and controls to be established")); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS —GUIDELINES, supra, at 10 (paragraph 5.3.1, stating that the "governing body and top management should assign responsibility and authority to the compliance function for: a) ensuring that the compliance management system is consistent with this International Standard"); OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured

Federal Savings Associations, and Insured Federal Branches, 12 C.F.R. part 30, app. D, II.D. (2018) (under guidelines of the Office of the Comptroller of the Currency, with the input of, among others, independent risk management, the chief executive officer of a large national bank is tasked with the articulation of a written three-year strategic plan for risk management). In certain regulatory spheres, the chief executive officer is required to meet with a specific internal-control officer so that the officer can certify that the firm has an adequate internal-control framework and program. See FINRA Rule 3130(b) (2018), http://finra.complinet.com (requiring the chief executive officer to certify annually that "the member has in place processes to establish, maintain, review, test and modify written compliance policies and written supervisory procedures reasonably designed to achieve compliance with applicable FINRA [and other applicable] rules" and that the officer has met with the chief compliance officer in the preceding 12 months to discuss these processes).

c. Authorities setting forth the duties of executive management with respect to compliance, risk management, and the related internal audit of these internal-control functions were sources for the responsibilities laid out in this Principle. For example, they provide that, given its position in an organization, executive management must establish the structure of decisionmaking, independence, and authority for compliance, risk management, and internal audit and ensure that these internal-control departments have adequate personnel and resources to accomplish their missions. See, e.g., COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 151 (observing that senior managers "provide direction, for example, on a unit's organizational structure and personnel hiring and training practices, as well as budgeting and other information systems that promote control over the unit's activities"); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS —GUIDELINES, supra, at 11 (paragraph 5.3.3, enumerating "top management's" duties, which include giving the compliance department authority and independence and "adequate and appropriate resources" and implementing the assignment of compliance responsibilities within the organization); BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS 19, 26-27 (2014) (Principle 6, no. 105, support for risk management; Principle 9, nos. 136, 137, independence, authority, stature, and resources of the compliance department; Principle 10, no. 141, same for internal-audit department).

d. There is considerable support—in some cases it is mandated by law—for the proposition that senior executives, particularly the chief executive officer, should meet at least annually with each of the internal-control officers for the purposes of evaluating the effectiveness of the internal-control functions and determining the modifications, if any, that should be made to them. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 151 (stating that the chief executive officer should "[e]valuat[e] internal control deficiencies and the impact on the ongoing and long-term effectiveness of the system of internal control" by meeting regularly with control officers); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS — GUIDELINES, supra, at 25 (paragraph 9.3, "Top management should review the organization's compliance management system, at planned

intervals, to ensure its continuing suitability, adequacy and effectiveness."); Department of Justice Criminal Division and Securities and Exchange Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act, supra, at 62 (emphasizing the importance of a periodic review of a compliance program); Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, supra, 63 Fed. Reg. at 8996 (discussing compliance audits and regular reporting about their results and compliance problems to senior hospital or corporate officers). See also FINRA Rule 3130(b) (requiring that the chief executive officer of a member firm meet with the chief compliance officer at least annually). One method of ensuring that senior executives take seriously the responsibility for regular evaluation of an organization's internal controls is to have them certify annually as to their effectiveness and to identify any serious weaknesses in them. See, e.g., 15 U.S.C. § 7241 (2018); 17 C.F.R. § 240.13a-14 (2018) (quarterly and annual certification by chief executive officer and chief financial officer of a public company that deals with, among other things, the effectiveness of internal controls that would ensure accurate financial reporting by the company); 17 C.F.R. § 3.3(f)(3) (2018) (certification of annual report about the compliance program of a futures commission merchant (among others), including its effectiveness, by either the chief compliance officer or the chief executive officer).

e. Authorities pronouncing on the governance of compliance, risk management, and internal audit in organizations recommend that executive management seek approval from the board of directors for the compliance and risk-management programs and the related internal audit, regularly report to the board on their implementation and effectiveness, and report to it on material failures and violations and recommend remedial measures for them. See, e.g., COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 151 (stating that, on internal controls, "the CEO [is] ultimately accountable to the board of directors"); BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS, supra, at 18 (under Principle 4, no. 93, senior management should keep the board informed about "breaches of risk limits or compliance rules," "internal control failures" and "legal or regulatory concerns"); BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES 8 (Oct. 16, 2008) ("The board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by management."); OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 12 C.F.R. pt. 30, app. D, II.H (2018) (directing banks to "[e]stablish protocols for when and how to inform the board of directors … of a risk limit breach that takes into account the severity of the breach and its impact on the covered bank.").

f. Compliance and risk-management principles provide for external communication by an organization on these subjects, which could be made to regulators, the market, and other interested parties. See, e.g., INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at

18 (paragraph 7.4.3, dealing with external communication on compliance targeting "interested parties" who "can include, but are not limited to, regulatory bodies, customers, contractors, suppliers, investors, emergency services, non-governmental organizations and neighbours."); INT'L STANDARD, RISK MANAGEMENT – PRINCIPLES AND GUIDELINES, ISO 3100 12 (2009) (paragraph 4.3.7, "The organization should develop and implement a plan as to how it will communicate with external stakeholders.").

TOPIC 5

INTERNAL-CONTROL OFFICERS

§ 3.15. Chief Compliance Officer

(a) An organization should elect to have a chief compliance officer ("CCO") who is responsible for the compliance function and, if feasible, does not have other operational responsibilities.

(b) The CCO's responsibilities should include the following:

(1) for the purposes of formulating, implementing, and testing the organization's compliance program and code of ethics:

(A) to be well informed of the legal obligations applicable to, and the values in the code of ethics for, the organization, its employees, and agents,

(B) together with compliance officers and as directed by executive management, to conduct a compliance-risk assessment, and to formulate and implement the compliance program and the code of ethics, and any revisions thereto, in response to that assessment, and

(C) to oversee compliance officers' regular testing and reassessment of the compliance program and the code of ethics for effectiveness and inadequacies;

(2) to manage the compliance department, which includes making recommendations to executive management about its staffing and resources, and to decide upon the hiring, dismissal, compensation, work conditions, placement within the organization, and reporting lines of compliance officers and other compliance personnel;

(3) to oversee communication about the compliance program and the code of ethics throughout the organization and the compliance training conducted for the board of directors, executive management, employees, and agents;

(4) to advise the board of directors, any board committee, executive management, and other organizational actors about whether a course of action, transaction, practice, or other organizational matter complies with the compliance program and the code of ethics, and to oversee compliance officers' provision of compliance advice in the organization;

(5) for the purposes of monitoring compliance with the compliance program and the code of ethics, administering confidential internal reporting and investigating violations:

(A) to initiate and oversee the monitoring done by compliance officers to ensure that the organization, its employees, and agents follow the compliance program and the code of ethics, and, if delegated these responsibilities under the compliance program,

(B) to administer the organization's procedures for confidential internal reporting of violations of the compliance program and the code of ethics, and

(C) in consultation with the chief legal officer, to direct the investigation of any actual or potential violation of the program and the code detected by the monitoring or by the procedures for confidential internal reporting and to report the results of the investigation to the appropriate organizational actor;

(6) to be the organization's liaison with regulators on its compliance program and code of ethics;

(7) to communicate regularly with the board of directors, any board committee responsible for compliance oversight, and executive management about the compliance program and the code of ethics;

(8) to meet at reasonable intervals with executive management to report on the effectiveness of and inadequacies in the compliance function and to recommend any necessary changes;

(9) to confer with executive management:

(A) to notify it of any material violation or failure of the compliance program or the code of ethics, and

(B) to recommend any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such violation or failure; and

(10) to accompany executive management to meet with the board of directors, or a board committee responsible for compliance oversight, or to meet outside the presence of executive management at the request of the board or its committee, or at the CCO's own request, for the following purposes:

(A) to obtain its approval for the compliance program and the code of ethics, and any material revisions thereto,

(B) to report on their implementation,

(C) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the compliance function,

(D) to notify it of any material violation or failure of the compliance program or the code of ethics and to propose for approval or to identify for ratification any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation or failure, and

(E) to confer about any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them, and the adequacy of such disclosure or reporting.

Comment:

a. General. Subsection (a) provides that an organization may elect to have an officer who is responsible for its overall compliance, i.e., the compliance function (§ 1.01(i) (definition), § 5.01 (nature), § 5.02 (goals) and § 5.05 (elements)), which includes the compliance program (§ 1.01(m) (definition, which encompasses the compliance policies and procedures, § 1.01(l)), § 5.06 (features)) and the code of ethics (§ 1.01(g) (definition), § 5.37 (definition and features)). The legal

and ethical obligations imposed today upon many (particularly large) organizations and their employees and agents are numerous and complex. Therefore, organizations may find it useful to have a compliance department that provides appropriate guidance and training to organizational actors on how to satisfy these obligations and that monitors them for compliance and investigates misconduct. The compliance department should have effective management (§ 5.05(c)), which means having an officer (the chief compliance officer or "CCO") with managerial authority over it. Some organizations prefer the title chief ethics and compliance officer or "CECO," which emphasizes the officer's role in promoting compliance with the organization's ethical values and code of ethics. Moreover, a large organization may have numerous "chief" compliance officers who are each responsible for compliance in a division or group or for a specialized kind of compliance and who may even act independently from the CCO. However, even in these situations, there is generally one officer who oversees, and is responsible for, the compliance function in the entire organization. This Principle addresses the responsibilities of that officer.

This Principle does not require that the CCO be a member of executive management (i.e., the senior-most executives in the organization, § 1.01(v)) because it recognizes that organizations should have the flexibility as to where to situate the CCO in the organization's hierarchy. However, making the CCO a member of executive management, which gives that officer a "seat" at the chief executive officer's table, helps underscore the importance of compliance in an organization. This Comment acknowledges that some organizations also use a compliance committee, composed of executives, the chief legal officer, and the CCO, among others, to oversee the compliance program and to ensure that it is followed throughout the firm. Because the CCO has considerable, time-consuming responsibilities in administering the compliance program, it is recommended that this officer not have other operational or business-line responsibilities, particularly in a large organization or in one in a highly regulated industry. Subsection (a) reflects, however, that an organization's circumstances and resources may require that the CCO wear other organizational "hats."

As is suggested above, this Principle provides for a CCO who is most appropriate for a publicly traded company or other organization of comparable size and operations, or for one in a highly regulated industry. In certain domains, law or regulation mandates that an organization have a CCO. This Principle acknowledges that an organization may structure its implementation of the compliance function in many ways, including by delegating the CCO responsibilities listed in it to

other organizational actors without its having a CCO or even by outsourcing some or all of them. See also § 3.20 (multiple responsibilities of internal-control officer) and § 3.21 (outsourcing).

b. CCO responsibilities in general. Subsection (b) specifies the important responsibilities of the CCO. They are primarily based upon the goals and tasks of the compliance program, as set out in § 5.06, which the CCO directs. They also include those responsibilities typically associated with the management of an internal-control department. Because, moreover, the board of directors oversees (§ 3.08(b)(2)), and executive management directs the implementation of (§ 3.14(b)(2)), the organization's compliance program and code of ethics, subsection (b) includes provisions dealing with responsibilities associated with the interaction between the CCO and these organizational actors.

c. CCO responsibilities; formulating, implementing, and testing the compliance program and the code of ethics. Subsection (b)(1)(A) clarifies that a CCO should be informed of the laws and regulations affecting the organization, its employees, and agents, as well as the ethical values in the organization's code of ethics. The CCO's knowledge should be extensive since, as stated in subsection (b)(1)(B), this officer, assisted by compliance officers and directed by executive management, must conduct a compliance risk assessment (§ 1.01(n) (definition of compliance risk); § 5.07 (definition and explanation of this assessment)), and formulate and implement the compliance program, which includes the compliance policies, the governance of compliance, and the code of ethics, all of which presumes the CCO's extensive knowledge of the relevant laws, regulations, and the applicable code. Section 3.06 specifies some of the ways in which the CCO might acquire this knowledge, and regular consultation with the chief legal officer, the primary authority for legal matters in the organization (§ 3.18), is recommended. Subsection (b)(1)(C) also provides that the CCO should oversee the necessary testing and reassessment of the compliance program and the code of ethics conducted by the compliance officers, which is an integral part of a compliance program (§ 5.06(n)) because it can reveal the program's effectiveness and inadequacies. This testing also serves as the basis for the CCO's reporting on these subjects to executive management under subsection (b)(8), and to the board of directors under subsection (b)(10).

d. CCO responsibilities; managing the compliance department. Subsection (b)(2) highlights the CCO's management of the compliance department. In particular, the CCO should be able to recommend to executive management proposed courses of action on the appropriate

staffing and use of resources for the department, and to decide upon the hiring and dismissal, compensation, work conditions, and the appropriate organizational structure of compliance officers (e.g., whether to have them work in a separate compliance department, to embed them in the organization's operations, or to do a combination of both). In other words, executive management makes the overall resource-allocation and staffing decisions, see § 3.14(b)(6) (on executive management's responsibilities for these matters), but the CCO makes those decisions typically associated with department management.

The reporting lines of compliance officers, both to whom they provide information and who has authority over them, vary by organization, with different reporting structures having their own benefits and costs, although the law and regulation governing an organization may impose a particular reporting structure for the CCO and compliance officers. For example, compliance officers who are in a separate reporting line apart from the organization's business or operations may have enhanced independence but may find it more difficult to integrate themselves into that business or those operations so that they can provide compliance advice. Moreover, although the CCO is under the authority of executive management and ultimately the chief executive officer, the CCO should have sufficient independence to ensure that the compliance department operates as an effective part of the organization's internal control. Other Principles recommend that the board of directors or the board compliance and ethics committee approve the hiring, terms of employment, and dismissal of the CCO, which contributes to this independence. See § 3.08(b)(7) and § 3.10(d)(4).

e. CCO responsibilities; overseeing communication and training. Subsection (b)(3) specifies that the CCO is responsible for overseeing the related communication and educational missions, which are critical parts of the compliance program. See § 5.06(g) and (h) (communication and training as features of a compliance program). The CCO must ensure that all organizational actors understand their obligations under the compliance program and the code of ethics, which occurs through regular compliance training, including continuing education with respect to new obligations and amendments to the program and code. See § 5.10 (compliance training and education)

f. CCO responsibilities; advising on compliance. A key part of the compliance program is the provision of advice to organizational actors on their compliance obligations, ideally before they make a decision or resolve upon a particular course of action. See § 5.02, Comment *a*

(recommending this approach), § 5.06(f) (listing this advice-giving as one of the compliance program's tasks), and § 5.08 (discussing compliance advice). Subsection (b)(4) provides that the CCO, as the senior compliance specialist in the organization, should be called upon to advise the board of directors, its committees, executive management, and other executives on compliance matters. An organization that takes compliance seriously seeks the CCO's advice on any major decision. It should also be appropriate for a CCO to offer advice to these organizational actors, if the officer feels that it may promote effective compliance. The CCO also oversees the provision of compliance advice by compliance officers, which involves, among other things, reviewing that advice and having in place a system for the officers to refer difficult compliance matters to the CCO. It should be noted that, when the CCO or a compliance officer provides compliance advice, this does not constitute the kind of legal advice, with all the legal protections for the recipient of that advice, offered by the chief legal officer or other legal officers. See § 3.18(b)(1) and Comment *a*.

g. CCO responsibilities; monitoring, administering procedures for confidential internal reporting, and investigating failures or violations. Critical parts of the compliance program include (i) monitoring to ensure that organizational actors fulfill their compliance obligations (§ 5.06(j)) and to detect failures and violations of the program and the code of ethics, and (ii) investigating these failures and violations (§ 5.06(k)). Subsection (b)(5)(A) makes the CCO responsible for putting into effect the organization's monitoring system or systems, which must be comprehensive. See § 5.09 (elements of compliance monitoring). While monitoring has become a specialized task of compliance officers, the compliance program may give other organizational actors monitoring responsibilities. In addition, today many organizations use automated monitoring systems to flag potential violations of their compliance program. This means that, in overseeing the implementation and operation of a monitoring system, a CCO may need to have the relevant technical expertise or to consult with information-technology specialists within or outside the organization about the monitoring system.

Related to monitoring, a compliance program should have procedures for internal, preferably confidential, reporting of violations or failures of the compliance program and the code of ethics, see § 5.06(i), which procedures are generally under the oversight of a board committee, see § 3.10(d)(10) (recommending that the board compliance and ethics committee have this responsibility). If the organization so elects, under subsection (b)(5)(B), the CCO may be entrusted

with receiving reports made under these procedures. See § 5.18, Comments *a* and *c* (observing that organizations may make the CCO responsible for internal reporting).

Once the monitoring or internal reporting procedures reveal a potential violation or failure of the compliance program or the code of ethics, see § 5.11 ("red flags" revealed by compliance monitoring), under subsection (b)(5)(C) the CCO may be tasked with ensuring that the matter is properly investigated. Organizations vary in how they allocate responsibility for these kinds of investigations. Because the chief legal officer is responsible for advising on any material violation or failure of the compliance program and the code of ethics, see § 3.18(b)(1) and (3), and Comments *c* and *e*, subsection (b)(5)(C) provides that the CCO should consult with that officer in conducting any investigation. The chief legal officer may permit the CCO to oversee initial stages of an investigation, but may then assume control over it once the facts about the violation have been gathered.

Although one element of a compliance program are the procedures for discipline for violations of it, see § 5.06(l), deciding upon and carrying out this discipline are not generally responsibilities of internal-control officers like the CCO, but belong to executive management and other levels of management, although the CCO may make recommendations about disciplinary issues, see subsection (b)(9). Therefore, in accordance with § 5.12 (compliance officer's escalation of a compliance violation within the organization), subsection (b)(5)(C) also provides that the CCO should ensure that the results of any investigation that it oversees are reported to the appropriate organizational actor for discipline and other remedial measures.

h. CCO responsibilities; acting as a liaison with regulators. Subsection (b)(6) provides that, in appropriate circumstances, the CCO may act as the organization's liaison on its compliance matters with regulators who have legal authority over the organization. This may occur when, in certain industries, a regulator is mandated to directly supervise the conduct of the organization, including its compliance program, and when the CCO is thus required to report on the program to the regulator. See, e.g., § 5.03(d) (recommending that, as part of its general compliance activities, an organization display honesty and candor towards regulators, among others). In these circumstances, the regulator may demand or expect direct contact with an organization's CCO. This liaison activity is distinguished from reporting material violations or failures of the compliance program or the code of ethics to regulators, which is covered in subsections (b)(9) and (10).

i. CCO responsibilities; communicating with and reporting to the board and executive management. Subsection (b)(7) provides that, irrespective of the CCO's place in an organization's managerial structure, the CCO should regularly communicate with, and report on the compliance program and compliance matters to, the board of directors or a board committee such as the board executive committee or its compliance and ethics committee, and executive management. This subsection is thus the necessary counterpart to § 3.08(b)(8) (board communicating with internal-control officers), § 3.10(d)(5) (compliance and ethics committee communicating with CCO) and § 3.14(b)(8) (executive management communicating with internal-control officers) and is further explained in Comment *g* to § 3.08, Comment *d* to § 3.10, and Comment *g* to § 3.14. Once again, this reporting is in addition to that associated with a material violation or failure of the compliance program and the code of ethics, which is covered by subsection (b)(10)(D) that allows the CCO to report on such an event to the board or a board committee.

j. CCO responsibilities; meeting with executive management on effectiveness of and inadequacies in the compliance function. Subsection (b)(8) states that the CCO should regularly meet with executive management (usually, the chief executive officer) to report on the effectiveness of and inadequacies in the compliance function and to recommend any necessary changes. See § 3.14(b)(9) (executive management having such meetings with the CCO and other internal-control officers) and § 5.06(o) (providing, as one feature of a compliance program, its periodic review and reaffirmation by senior executives). That kind of report and meeting, which is generally based upon internal testing of the compliance program, see subsection (b)(1)(C), has become an accepted organizational practice, and regulation mandates it for firms in certain industries. While the focus of the meetings is on the operation of the compliance program and the code of ethics, the overall concern is how compliant is the organization, which explains the use of the term, compliance function. Without regular meetings with the CCO, executive management would have difficulty in ensuring that there is an effective compliance function in the organization. In these meetings, the CCO can also inform executive management about any recent significant compliance developments and can seek its approval for the CCO's proposals to address them in the compliance program and the code of ethics. The meetings can be combined with or held separate from those in which the chief audit officer presents the results of the internal audit of the compliance program. See § 3.17(b)(7)(A).

k. CCO responsibilities; meeting with executive management on material violations or failures of the compliance program or the code of ethics. Subsection (b)(9)(A) provides for exceptional reporting when the CCO alerts executive management to any material violation or failure of the compliance program or the code of ethics. See § 3.14(b)(10) (provision dealing with executive management's receiving such report) and Comment *i* (where the purposes of this reporting are explained). Under subsection (b)(9)(B), the CCO may recommend disciplinary and remedial measures, including reporting to a regulator, that executive management may determine to take in response to the violation or failure. In all but the rare case, this determination is for executive management, not for the CCO, to make, with approval by the board of directors. See § 5.12(b) (escalation of compliance issue within an organization to official with the power to address it) and § 5.12(c) (CCO's escalation of compliance issue to a government regulator in unusual circumstances). The chief legal officer should be included in any meetings between executive management and the CCO on these issues (this is provided in § 3.14(b)(10)) because that officer provides legal advice on the organization's response to the material violation or failure. See § 3.18(b)(3) and Comment *e* (role of chief legal officer in the investigation of such violation or failure).

l. CCO responsibilities; meeting with the board of directors. Finally, subsection (b)(10) provides that the CCO should meet with the board of directors, or a board committee such as the compliance and ethics committee, on a number of issues of relevance to the board's oversight of compliance in the organization. The provision presumes that, in these meetings, the CCO accompanies and assists executive management as the organization's specialist in compliance, although it recognizes that, in certain circumstances, the board, its committee, or even the CCO may request a meeting without the presence of executive management. See also § 6.29(b)(1) (whistleblower awards to compliance officers contingent on their reporting first to the organization's governing body). Each of the provisions in this subsection thus has its counterpart in the Principles dealing with the responsibilities of the board (§ 3.08), the compliance and ethics committee (§ 3.10), and executive management (§ 3.14): (i) approving the compliance program (§ 3.08(b)(2), § 3.10(d)(2), and § 3.14(b)(11)(A)), (ii) reporting on its implementation (§ 3.08(b)(2), § 3.10(d)(2), and § 3.14(b)(11)(B)), (iii) reporting on the effectiveness of the compliance function (§ 3.08(b)(9), § 3.10(d)(6), and § 3.14(b)(11)(C)), (iv) reporting on and dealing with a material violation or failure (§ 3.08(b)(10), § 3.10(d)(7), and § 3.14(b)(11)(D)), and

(v) approving mandatory and discretionary disclosures and reporting to regulators regarding the compliance program (§ 3.10(d)(8) and § 3.14(b)(11)(E)).

REPORTERS' NOTE

a. The CCO, who manages the compliance department, has become an established, recommended, and—in certain domains—legally required officer in organizations. See Sean J. Griffith, *Corporate Governance in an Era of Compliance,* 57 WM. & MARY L. REV. 2075, 2101-2102 (2016) (citing survey data on this position in companies); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 153 (2013) (noting the importance of this position). See also CONTROL RISKS, INTERNATIONAL BUSINESS ATTITUDES TO COMPLIANCE: REPORT 2017 11 (2017) (reporting that 47% of U.S. companies surveyed in a global survey have a compliance function led by a dedicated compliance officer). Under the U.S. Sentencing Guidelines, an effective compliance and ethics program has a "[s]pecific individual(s) within the organization … delegated day-to-day operational responsibility for the compliance and ethics program." See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C) 534 (2016). In some sectors, regulations require an organization to have a CCO. See, e.g., Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8989 (Feb. 23, 1998) (noting that one element of a compliance program for hospitals is "[t]he designation of a chief compliance officer … charged with the responsibility of operating and monitoring the compliance program …."); FINRA Rule 3130(a) (2018), http://finra.complinet.com (requiring a broker-dealer that is a member of FINRA to designate one or more principals as CCO(s)); 17 C.F.R. § 275.206(4)-7(c) (2018) (requiring a registered investment adviser to have a CCO); 17 C.F.R. § 270.38a-1(a)(4) (2018) (requiring the same for a registered investment company); 15 U.S.C. 78*o*-8(k)(1) (2018) (requiring each security-based swap dealer and participant to have a CCO); 17 C.F.R. 240.15Fk-1(a) (2018) (implementing rule). See generally John H. Walsh, *Institutional-Based Financial Regulation: A Third Paradigm,* 49 HARV. INT'L L.J. 381, 390-392 (2008) (discussing the advent of the chief compliance officer in broker-dealers and investment advisers). International organizations also recommend that organizations have this position. See BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS 11 (2005) (Principle 5, paragraph 24: "Each bank should have an executive or senior staff member with overall responsibility for co-ordinating the identification and management of the bank's compliance risk and for supervising the activities of other compliance function staff."). International efforts at standardization of compliance reflect that the CCO is a well-established organizational position. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO 19600 10 (2014) (paragraph 5.3.2, "Many organizations have a dedicated person (e.g., a compliance officer) responsible for day-to-day compliance management ….") The title "chief ethics and compliance officer" or "CECO" is used in some organizations. See SOC'Y OF CORP. COMPLIANCE AND ETHICS & NYSE GOVERNANCE SERV., COMPLIANCE AND ETHICS PROGRAM ENVIRONMENT REPORT 10 (2014) (noting that 18% of those surveyed use this title).

b. That organizations are generally free under law and regulation to structure the compliance function and the CCO position as they see fit influenced the drafting of this Principle. Organizations may assist the CCO by instituting an executive-level compliance committee. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 10 (paragraph 5.3.2, "some [organizations] have a cross-functional compliance committee to coordinate compliance across the organization."). They may give their CCO other organizational responsibilities. See, e.g., FINRA Rule 3130.08, supra (providing that "[t]he requirement to designate one or more chief compliance officers does not preclude such persons from holding any other position within the member, including the position of chief executive officer, provided that such persons can discharge the duties of a chief compliance officer in light of his or her other additional responsibilities."). It is recommended that a large organization, with a more extensive compliance program, have a CCO without any operational or other responsibilities. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 153 ("In large and complex organizations, specialized compliance professionals can be helpful in defining and assessing controls for adherence to both external and internal requirements."). The Basel Committee on Banking Supervision states well how circumstances, such as an organization's size, dictate whether the CCO fulfills only compliance duties:

> The independence of the head of compliance and any other staff having compliance responsibilities may be undermined if they are placed in a position where there is a real or potential conflict between their compliance responsibilities and their other responsibilities. It is the preference of the Committee that compliance function staff perform only compliance responsibilities. The Committee recognises, however, that this may not be practicable in smaller banks, smaller business units or in local subsidiaries. In these cases, therefore, compliance function staff may perform non-compliance tasks, provided potential conflicts of interest are avoided.

BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, supra, at 12 (Principle 5, paragraph 28). But see Donald C. Langevoort, *Monitoring: The Behavioral Economics of Corporate Compliance with Law,* 2002 COLUM. BUS. L. REV. 71, 100-103 (2002) (explaining why an organization may not have the most effective compliance function).

Related to the position of the CCO in the organization is the issue to whom this officer reports. Recommended practices and regulations generally deal only with reporting in the sense of providing information, rather than with organizational lines of authority. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 11 (paragraph 5.3.3, requiring that the governing body and top management have a compliance department with "clear and unambiguous support from and direct access to the governing body and top management"). For example, a standard practice, which law or regulation imposes in certain sectors, is for the CCO—or the organizational actor with operational responsibility for the compliance program—to meet with the chief executive officer and the board of directors to report on the effectiveness of the

compliance program and the code of ethics and on any recommended changes to them. In its specification of the features of an effective compliance program, the U.S. Sentencing Guidelines provide that "individual(s) with operational responsibility [for the compliance and ethics program] shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority." See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C), supra, at 534. See also Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, supra, 63 Fed. Reg. at 8993 (requiring that the CCO report to the hospital's governing body, the chief executive officer, and the compliance committee). The requirement of this kind of reporting is common in the financial sector. See, e.g., FINRA Rule 3130(b) & (c), 3130.04-.05, .10, supra (discussing meetings between the CCO and the chief executive officer, the CCO's responsibilities, and the compliance report); 17 C.F.R. § 270.38a-1(a)(4)(iii) (2018) (investment company CCO's annual report to the board of a registered fund); 15 U.S.C. 78*o*-8(k)(3) (2018) (requiring swap dealer CCO's annual report); and 17 C.F.R. 240.15Fk-1(c) (2018) (discussing CCO's annual report that goes to board of directors, audit committee, and senior officer of the firm). See generally John H. Walsh, *Right the First Time: Regulation, Quality, and Preventive Compliance in the Securities Industry*, COLUM. BUS. L. REV. 165, 236 (1997) (discussing generally the value of this reporting).

c. If there is a stand-alone compliance department in the organization, the CCO is expected to manage it as would a typical department manager, subject to the authority of more senior executives, particularly the chief executive officer. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 10 (paragraph 5.3.2, referring to the compliance officer's compliance management). See also COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 149 (observing the primacy of the chief executive officer in the development of internal control). Authorities support the proposition that a CCO must have adequate authority and resources to implement an effective compliance program. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 11 (paragraph 5.3.3, stating that top management should, among other things, "ensure that the compliance function has authority to act independently" and "allocate adequate and appropriate resources" to the compliance function). See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C) supra, at 534 ("To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.").

d. The responsibilities of compliance officers are the subject of codes of best practices and of laws and regulations. In articulating them, this Principle relies upon this background and upon the functions of the compliance program as set forth elsewhere in these Principles. Compliance officers are responsible for the compliance-risk assessment and then the design, implementation, testing, and modification of the compliance program and the code of ethics for the organization to address its compliance risks and to support its values. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 12 (paragraph 5.3.4, listing these and other responsibilities of the compliance department); DELOITTE, COMPLIANCE MODERNIZATION IS NO

LONGER OPTIONAL: HOW EVOLVED IS YOUR APPROACH? 10 (2017) (emphasizing the proactive and predictive side of compliance). Regulations and agency guidance support this multifaceted responsibility. See, e.g., Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, supra, 63 Fed. Reg. at 8993 (listing the CCO's responsibilities as including overseeing and monitoring implementation of the compliance program and periodically revising it); 17 C.F.R. 240.15Fk-1(b)(2) & (4) (2018) (providing that swap dealer CCO must help firm establish, modify as necessary, and administer a compliance program); 17 C.F.R. § 270.38a-1(a)(4) (2018) (noting that an investment-company CCO "administers" the compliance policies and procedures); FINRA Rule 3130.05, supra ("A chief compliance officer is a primary advisor to the member on its overall compliance scheme and the particularized rules, policies and procedures that the member adopts."). Compliance practice in many organizations does not always include regular updating of the compliance program, however. See, e.g., KPMG, THE COMPLIANCE JOURNEY: BOOSTING THE VALUE OF COMPLIANCE IN A CHANGING REGULATORY CLIMATE 16 (2017) (survey of U.S. chief compliance officers finds 31% reporting that "they do not have or do not know if they have regulatory change process to capture changes in laws and regulations.").

It is also well established that the CCO is in charge of the education and training of all organizational actors regarding the compliance obligations, the compliance program, and the code of ethics. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 153 ("The chief legal/compliance officer is responsible for ensuring that legal, regulatory, and other requirements are understood and communicated to those responsible for effecting compliance."); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 12 (paragraph 5.3.4, "providing or organizing on-going training support for employees to ensure that all relevant employees are trained on a regular basis"). See also Todd Haugh, *Nudging Corporate Compliance,* 54 AM. BUS. L. J. 683 (2017) (explaining how compliance officers could use behavioral science to "nudge" employees into compliant conduct). Moreover, as reflected in this Principle, in heavily regulated sectors, where firms have significant reporting responsibilities and are regularly subject to examination, a CCO is likely to be the point person in a firm's interaction with regulators on the compliance program. See, e.g., 17 C.F.R. 240.15Fk-1(c) (2018) (swap dealer CCO's responsibility to prepare a compliance report to be filed with the SEC).

e. A recognized, valued responsibility of the CCO, which is also reflected in this Principle, is to offer advice to senior executives and the board of directors on compliance risks and obligations, the compliance program, and the code of ethics and to supervise compliance officers in their performance of this advisory role for others in the organization. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 12 (paragraph 5.3.4, explaining that one of the tasks of the compliance department is "providing objective advice to the organization on compliance-related matters); FINRA Rule 3130.05, supra (noting that the rule is designed "to foster regular and significant interaction between senior management and the chief compliance officer(s) regarding the member's comprehensive compliance program."); BASEL COMM. ON

BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, supra, at 13 (Principle 7, paragraph 35, noting the advisory function of compliance).

f. There is considerable support for the proposition that a CCO is expected to oversee the compliance program's monitoring, which ensures that organizational actors follow the compliance program and the code of ethics and which detects violations and failures of the program and the code. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(5)(A), supra, at 535 (stating that an effective compliance and ethics program has "monitoring and auditing to detect criminal conduct"); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 12 (paragraph 5.3.4, compliance program "establish[es] … monitoring and measuring compliance performance"); 17 C.F.R. § 240.15Fk-1(b)(2)(ii) (2018) (swap dealer CCO's responsibility for identifying noncompliance through compliance-office review); BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, supra, at 14 (Principle 7, paragraphs 40-41, on monitoring and testing, and CCO's reporting to senior management based on them). Authorities suggest that the CCO could be involved in the identification, investigation, and remediation of material compliance violations or material failures of the compliance program and the code of ethics, without specifying the exact nature of this involvement or the allocation of responsibilities between legal and compliance. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 153 (noting that collaboration between legal/compliance personnel and business management is necessary to "manage adverse outcomes such as regulatory sanctions, legal liability, and failure to adhere to internal compliance policies and procedures"); U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(7) and cmt. appl. n. 6, supra, at 535, 538 (a feature of an effective compliance and ethics program is that, after the organization detects criminal conduct, it takes "reasonable steps to respond appropriately," including "making necessary any modifications" to the compliance and ethics program, without specifying the organizational actors involved in this, other than to say that an organization may use "an outside professional advisor"); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, supra, at 12 (paragraph 5.3.4, compliance "analys[es] performance to identify the need for corrective action").

Certain authorities specifically provide for the CCO's involvement in investigations of compliance violations and in taking remedial action to address them. See BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, supra, at 14 (Principle 7, paragraph 41: "The head of compliance should report on a regular basis to senior management on compliance matters. The reports should refer to the compliance risk assessment that has taken place during the reporting period, including any changes in the compliance risk profile based on relevant measurements such as performance indicators, summarise any identified breaches and/or deficiencies and the corrective measures recommended to address them, and report on corrective measures already taken."); Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, supra, 63 Fed. Reg. at 8994 (one of the tasks of the chief compliance officer is "[i]ndependently investigating and acting on matters related to compliance, including the flexibility to design and coordinate internal

investigations (e.g., responding to reports of problems or suspected violations) and any resulting corrective action with all hospital departments, providers and sub-providers, agents and, if appropriate, independent contractors") (footnote omitted). In some cases, regulation requires a CCO's involvement in dealing with a compliance violation, but the focus here is on reporting of compliance violations and the changes to the compliance program to address them. See, e.g., 17 C.F.R. § 270.38a-1(a)(4)(iii)(B) (2018) (investment company CCO's annual report to the board of a registered fund identifies "Each Material Compliance Matter" that occurred since the last report); 15 U.S.C. § 78*o*-8(k)(2)(F) & (G) (2018) (swap dealer CCO's responsibility for establishing procedures for remediation and closing of noncompliance issues); 17 C.F.R. § 240.15Fk-1(b)(ii) & (iii) (2018) (same), id. (c)(2) (CCO's report identifies "material non-compliance matters," material changes to the compliance program, and additional recommended changes).

§ 3.16. Chief Risk Officer

(a) An organization should elect to have a chief risk officer ("CRO") who is responsible for the risk-management function and, if feasible, does not have other operational responsibilities.

(b) The CRO's responsibilities should include the following:

(1) for the purposes of formulating, implementing, and testing the organization's risk-management framework and risk-management program:

(A) to be well informed of the material risks (other than legal and compliance risks, of which the CRO should be reasonably informed) to which the organization is or will likely be exposed,

(B) together with risk officers and as directed by executive management, to conduct a risk assessment and to formulate and implement the risk-management framework and risk-management program, and any revisions thereto, in response to that assessment, and

(C) to oversee risk officers' regular testing and reassessment of the framework and program;

(2) to manage the risk-management department, which includes making recommendations to executive management about its staffing and resources, and to decide upon the hiring, dismissal, compensation, work conditions, placement within

the organization, and reporting lines of risk officers and other risk-management personnel;

(3) to oversee communication about the risk-management framework and program throughout the organization and the risk-management training conducted for the board of directors, executive management, employees, and agents;

(4) to advise the board of directors, any board committee, executive management, and other organizational actors about whether an organization's course of action, transaction, practices, including those involving employee compensation, or other organizational matters comply and are adequately aligned with the risk-management framework and program, and to oversee risk officers' provision of risk-management advice in the organization;

(5) for the purpose of monitoring compliance with the risk-management program and investigating deviations or failures:

(A) to initiate and oversee the monitoring done by risk officers to ensure that the organization, its employees, and agents follow the risk-management program and to identify and assess new risks, and

(B) if delegated this task under the risk-management program, in consultation with the chief legal officer, to oversee the investigation of any actual or potential deviations from or failures in the program detected by the monitoring and to report the results of the investigation to the appropriate organizational actor;

(6) to be the organization's liaison with regulators on its risk-management program;

(7) to communicate regularly with the board of directors, any board committee responsible for risk oversight, and executive management about the risk-management program;

(8) to meet at reasonable intervals with executive management to report on the effectiveness of and inadequacies in the risk-management function and to recommend any necessary changes;

(9) to confer with executive management:

(A) to notify it of any material deviation from or failure of the risk-management program, and

(B) to recommend any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such deviation or failure; and

(10) to accompany executive management to meet with the board of directors, or a board committee responsible for risk-management oversight, or to meet outside the presence of executive management at the request of the board or its committee, or at the CRO's request, for the following purposes:

(A) to obtain its approval for the risk-management framework and program, and any material revisions thereto,

(B) to report on their implementation,

(C) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the risk-management function,

(D) to notify it of any material deviation from or failure of the risk-management program and to propose for approval or to identify for ratification any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such deviation or failure, and

(E) to confer about any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the material risks to which the organization is or may be exposed and the effectiveness of the risk-management program in addressing them, and the adequacy of such disclosure or reporting.

Comment:

a. General. Subsection (a) provides that an organization may elect to have an officer who is responsible for the risk-management function (§ 1.01(bbb) (definition), § 4.01 (nature of risk management)), the risk-management framework (§ 1.01(aaa) (definition)), which includes, if the organization has one, the risk-appetite statement (§ 1.01(uu) (definition)), and the risk-management program (§ 1.01(ccc) (definition), § 4.06 (identifying elements of an effective program)). It is now well accepted that organizations should manage their risks, which can be

numerous and diverse (§ 4.07 (organizational characteristics affecting their risk-management program); § 4.05 (classification of risk)). Risk management can be furthered by having a specialized department that helps the board of directors and executive management identify, assess, and prioritize the risks facing the organization and organizational actors (§ 1.01(vv) (definition of risk assessment)), decide upon the risks the organization is willing to assume (i.e., the residual risks, § 1.01(ss) (definition)), and then formulate and direct the implementation of a risk-management framework and program for the organization's management of the risks. As explained in § 4.14(c), an organization's tolerance for compliance risks will be low and its treatment of them in the risk-management framework will differ from its management of external and strategy risks. Risk-management activities include establishing appropriate governance of risk management within the organization (§ 4.06(b)(5)), which can be achieved by having an executive (the chief risk officer or "CRO") with authority over it (§ 4.06(b)(8)).

This Principle reflects that organizations have varied governance structures for risk management. An organization may have executives, other than risk officers, engaged in risk management or it may assign the implementation and oversight of risk management to an executive-level risk committee or committees. Moreover, these Principles assume that the identification and "management" of legal and compliance risks are under the authority of the chief compliance officer (§ 3.15) and the chief legal officer (§ 3.18), or those fulfilling their roles. A large organization may also have numerous "chief" risk officers who are each responsible for risk management in a division or group or for a specialized kind of risk management and who may act independently from the CRO. Even in these organizations, there may be an officer who oversees, and is responsible for, the risk-management function in the entire organization. For ease of exposition, this Principle addresses the responsibilities of that officer while recognizing that a specific organization might assign them to several officers, committees, or both.

This Principle does not require that the CRO be a member of executive management (i.e., the senior-most executives in the organization, § 1.01(v)) because it recognizes that organizations should have the flexibility as to where to situate the CRO in the organization's hierarchy. However, as in the case of the chief compliance officer, making the CRO a member of executive management gives that officer a "seat" at the chief executive officer's table and thus underscores the importance of risk management in an organization. Because the CRO has considerable, time-consuming responsibilities in administering the risk-management program, it is recommended that this officer

not have other operational or business-line responsibilities, particularly in a large organization or in one in a highly regulated industry. Subsection (a) reflects, however, that an organization's circumstances and resources may require that the CRO wear other organizational "hats" or be embedded in operations.

As is suggested above, this Principle provides for a CRO who is most appropriate for a publicly traded company or other organization of comparable size and operations, or for one in a highly regulated industry. In certain domains, law or regulation mandates that an organization have a CRO. This Principle acknowledges that an organization may implement its risk-management function in many ways, including by delegating the CRO responsibilities listed here to other organizational actors without its having a CRO or even by outsourcing some or all of them. See also § 3.20 (multiple responsibilities of internal control officer) and § 3.21 (outsourcing).

b. CRO responsibilities in general. Subsection (b) specifies the CRO's important responsibilities, which are similar to those of the chief compliance officer. They are primarily based upon the elements of a risk-management program, as set out in § 4.06. They also include those responsibilities typically associated with the management of an internal-control department. Because, moreover, the board of directors oversees (§ 3.08(b)(4)), and executive management directs the implementation of (§ 3.14(b)(4)), the organization's risk-management program, subsection (b) includes provisions dealing with responsibilities associated with the interaction between the CRO and these organizational actors.

c. CRO responsibilities; formulating, implementing, and testing the risk-management program. Subsection (b)(1)(A) clarifies that a CRO should be well-informed of the actual or potential material risks affecting the organization. The CRO is expected to be only reasonably informed about legal and compliance risks and to rely upon the chief compliance officer and the chief legal officer for an understanding of them. The CRO's knowledge of the remaining risks, which are themselves complex (§ 4.01 and Comments *b, c* and *d*), should be extensive because, as stated in subsection (b)(1)(B), this officer, assisted by risk officers and directed by executive management, must conduct the risk assessment and formulate and implement the risk-appetite statement (if the organization elects to do one), the risk-management framework, and the risk-management program, which includes the governance of risk management, and any revisions to them. All this presumes that the CRO has considerable background and expertise in risk management. See § 3.06 (ways that internal-control officers acquire this expertise). Subsection

(b)(1)(C) also provides that the CRO should oversee risk officers' necessary testing and reassessment of the risk-management framework and program, which are integral parts of a risk-management program (§ 4.06(a)(5) and (8)) because this reassessment can reveal the program's effectiveness and inadequacies. The testing also serves as the basis for the CRO's reporting on these subjects to executive management, under subsection (b)(8), and the board of directors, under subsection (b)(10).

d. CRO responsibilities; managing the risk-management department. Subsection (b)(2) highlights the CRO's management of the risk-management department. In particular, the CRO should be able to recommend to executive management proposed courses of action on typical managerial issues, such as the appropriate staffing of and the use of resources for the department, and to decide upon the hiring and dismissal, compensation, work conditions, and the appropriate organizational structure for risk officers (e.g., whether to have them work in a separate risk-management department, to embed them in the organization's operations, or to do a combination of both). In other words, executive management makes the overall resource-allocation and staffing decisions, see § 3.14(b)(6) (executive management's responsibilities for these matters), but the CRO makes those decisions typically associated with department management. Senior executives may be expected to pay particular attention to these matters, since risk management is tied so closely to the fortunes of an organization's business or affairs. See § 4.07 (identifying the characteristics of an organization affecting its risk-management program).

The reporting lines of risk officers, both to whom they provide information and who has authority over them, vary by organization, with different reporting structures having their own benefits and costs, although law and regulation governing an organization may impose a particular reporting structure for the CRO and risk officers. For example, risk officers who are in a separate reporting line apart from the organization's business or operations may have enhanced independence but may find it more difficult to integrate themselves into that business or those operations so that they can provide useful risk-management advice. Again, because the managing of risks is an integral part of an organization's business or affairs, executive management may elect to integrate risk officers or risk managers closely into the organization's operations. See § 4.06(b)(7) (an element of an effective risk-management program is "[i]ntegrating and embedding risk management throughout the organization"). Moreover, although the CRO is under the authority of executive management and ultimately the chief executive officer, the CRO should

have sufficient independence to ensure that the risk-management department operates as an effective part of the organization's internal control. Other Principles recommend that the board of directors or the board risk committee approve the hiring, terms of employment, and dismissal of the CRO, which contributes to this independence. See § 3.08(b)(7) and § 3.11(d)(4).

e. CRO responsibilities; overseeing communication and training. Subsection (b)(3) specifies that the CRO is responsible for overseeing the related communication and educational missions, which are critical parts of the risk-management program. See § 4.06(b)(1) (communicating risk information throughout the organization). The CRO must ensure that all organizational actors understand their obligations under the risk-management program, which occurs through regular training about risks and risk limits (§ 1.01(yy) (risk limit definition)), including continuing education with respect to new risks, and amendments to the risk-management framework and program.

f. CRO responsibilities; advising on risk management. A key part of the risk-management program is the provision of advice to organizational actors on the organization's risk appetite, acceptable variation in performance, and risk limits, among other things, ideally before they decide or resolve upon a particular course of action. See § 4.06(b)(1) (discussing how the organization communicates about risk). Subsection (b)(4) provides that the CRO, as the senior risk-management specialist in the organization, should be called upon to advise the board of directors, its committees, executive management, and other executives on these matters. An organization that takes risk management seriously seeks the CRO's advice on any major decision (e.g., whether the decision will be in accordance with the organization's risk appetite and tolerance). It should also be appropriate for a CRO to offer advice to these organizational actors, if the officer feels that it may promote effective risk management. The CRO also oversees the provision of risk-management advice by risk officers, which involves, among other things, reviewing that advice and having in place a system for them to refer difficult matters to the CRO.

g. CRO responsibilities; monitoring and investigating deviations and failures. Critical parts of the risk-management program include (i) monitoring to ensure that organizational actors fulfill their obligations under it (§ 4.06(a)(6) and (b)(4) (monitoring generally), § 4.12 and Comments *a-d* (strategies for monitoring risks)) and to detect deviations from and failures of the program and the surfacing of new risks, and (ii) investigating these deviations, failures, and new risks (§ 4.14 (specific risk responses)). Subsection (b)(5)(A) makes the CRO responsible for

putting into effect the organization's monitoring system or systems, which must be comprehensive and continuous. See § 4.06(a)(6) (risk monitoring). While monitoring is a specialized task of risk officers, the risk-management program may assign monitoring responsibilities to other organizational actors, given the pervasiveness of risk in operations and affairs. In addition, organizations use computer software and artificial-intelligence monitoring systems to aid them in flagging potential deviations from or failures of their risk-management programs and the surfacing of new and different risks. This means that, in overseeing the implementation and operation of a monitoring system, a CRO may need to have the relevant technical expertise or to work closely with information-technology specialists within or outside the organization in implementing and maintaining the monitoring system.

The monitoring could identify a new risk, which could be a material enhancement to or a material change in an existing risk. In that case and if appropriate, the CRO may propose modifications to the risk-management framework and program to address it, as is covered by subsection (b)(8). If the monitoring reveals a potential deviation from or failure of the risk-management program, under subsection (b)(5)(B) the CRO may be delegated the responsibility of investigating the matter to identify the cause of the deviation or failure. Organizations vary in how they allocate responsibility for these kinds of investigations. Because the chief legal officer is responsible for advising on the legal implications of any material deviation from or failure of the risk-management program, see § 3.18(a) and (b)(3), and Comment *c* and *e*, subsection (b)(5)(B) provides that the CRO should consult with that officer in conducting any investigation. The chief legal officer may permit the CRO to oversee initial stages of an investigation, but may then assume control over it once the facts about the deviation or failure have been gathered.

Deciding upon and carrying out any discipline of organizational actors as a result of a deviation or failure are not generally tasks of internal-control officers like the CRO, but are the responsibility of executive management and other levels of management, although the CRO may make recommendations about disciplinary issues, see subsection (b)(9). Therefore, subsection (b)(5)(B) also provides that the CRO should ensure that the results of any investigation are reported to the appropriate organizational actor for discipline and other remedial measures.

h. CRO responsibilities; acting as a liaison with regulators. Subsection (b)(6) provides that, in appropriate circumstances, the CRO may act as the organization's liaison on its risk-management matters with regulators who have legal authority over it. This may occur where, in

certain industries, a regulator is mandated to directly supervise the conduct of the organization, including its risk-management program, and where the CRO is thus required to report on the program to the regulator. In these circumstances, the regulator may demand, or expect, direct contact with an organization's CRO. This liaison activity is distinguished from reporting material deviations from or failures of the risk-management program to regulators, which is covered in subsection (b)(9) and (10).

i. CRO responsibilities; communicating with and reporting to the board and executive management. Subsection (b)(7) provides that, irrespective of the CRO's place in an organization's managerial structure, the CRO should regularly communicate with, and report on the risk-management program and matters to, the board of directors or a board committee such as the board executive committee or risk committee, and executive management. This subsection is thus the necessary counterpart to § 3.08(b)(8) (board communicating with internal-control officers), § 3.11(d)(5) (risk committee communicating with CRO), and § 3.14(b)(8) (executive management receiving reports from internal-control officers) and is further explained in the Comment *g* to § 3.08, Comment *d* to § 3.11, and Comment *g* to § 3.14. Once again, this reporting is in addition to that associated with material deviations from or failures of the risk-management program.

j. CRO responsibilities; meeting with executive management on effectiveness of and inadequacies in the risk-management function. Subsection (b)(8) states that the CRO should regularly meet with executive management (usually, the chief executive officer but possibly an executive-level risk committee) to report on the effectiveness of and inadequacies in the risk-management function and to recommend any necessary changes. See § 3.14(b)(9) (executive management's having such meetings with the CRO and other internal-control officers). That kind of report and meeting, which is generally based upon internal testing of the risk-management program, see subsection (b)(1)(C), and upon monitoring by risk officers, see subsection (b)(5)(A), has become an accepted organizational practice, and regulation mandates it for firms in certain industries. While the focus of the meetings is on the operation of the risk-management program, the overall concern is how well the organization is managing its risks, which explains the use of the term, risk-management function. Without regular meetings with the CRO, executive management would have difficulty in ensuring that there is an effective risk-management function in the organization. In these meetings, the CRO can also inform executive management about the appearance or prospect of any new material risk revealed by risk officers' monitoring, see

subsection (b)(5)(A), and about any recent significant risk-management developments and can seek its approval for the CRO's proposals to address them in the risk-management framework and program. The meetings can be combined with or held separate from those where the chief audit officer presents the results of the internal audit of the risk-management framework and program. See § 3.17(b)(7)(A).

k. CRO responsibilities; meeting with executive management on material deviations from or failures of the risk-management program. Subsection (b)(9)(A) provides for exceptional reporting when the CRO alerts executive management to any material deviation from or failure of the risk-management program. See § 3.14(b)(10) (provision dealing with executive management's receiving such report) and Comment *i* (where the purposes of this reporting are explained). Under subsection (b)(9)(B), the CRO may recommend disciplinary and remedial measures, including reporting to a regulator, that executive management may determine to take in response to the deviation or failure. In all but the rare case, executive management, not the CRO, makes this determination (particularly as to disciplinary matters), with approval by the board of directors. The chief legal officer should be included in any meetings between executive management and the CRO on these issues (this is provided in § 3.14(b)(10)) because that officer is responsible for legal advice on the organization's response to the material deviation or failure. See § 3.18(b)(3) and Comment *e* (role of chief legal officer in the investigation of such deviation or failure).

l. CRO responsibilities; meeting with the board of directors. Finally, subsection (b)(10) provides that the CRO should meet with the board of directors, or a board committee such as a risk committee, on a number of issues of relevance to the board's oversight of risk management in the organization. The provision presumes that, in these meetings, the CRO accompanies and assists executive management as the organization's specialist in risk management, although it recognizes that, in certain circumstances, the board, its committee, or even the CRO may request a meeting without the presence of executive management. Each of the provisions in this subsection thus has its counterpart in the Principles dealing with the responsibilities of the board (§ 3.08), the risk committee (§ 3.11), and executive management (§ 3.14): (i) approving the risk-management framework and program (§ 3.08(b)(4), § 3.11(d)(2), and § 3.14(b)(11)(A)), (ii) reporting on their implementation (§ 3.08(b)(4), § 3.11(d)(2), and § 3.14(b)(11)(B)), (iii) reporting on the effectiveness of the risk-management function (§ 3.08(b)(9), § 3.11(d)(6), and § 3.14(b)(11)(C)), (iv) reporting on and dealing with a material deviation or failure (§ 3.08(b)(10), § 3.11(d)(7), and

§ 3.14(b)(11)(D)), and (v) approving mandatory and discretionary disclosures and reporting to regulators regarding the risk-management program (§ 3.11(d)(8) and § 3.14(b)(11)(E)).

REPORTERS' NOTE

a. The CRO has become a standard executive-level position, particularly in large organizations, with the rise of enterprise risk management, a process designed to manage risks across an organization. See GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 151 (2017) (discussing the matter generally and providing data on how common the position has become); COMM. OF SPONSORING ORG. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 150, 152 (2013) (noting that the chief risk officer is a member of senior management); id. at 181-186 (explaining the relationship between internal control and enterprise risk management). In some sectors, such as in financial services, a firm must have a chief risk officer. 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, I.E.3 (2018) ("Chief Risk Executive means an individual who leads an independent risk management unit and is one level below the Chief Executive Officer in a covered bank's organizational structure."); 12 C.F.R. § 252.33(b) (2018) (requiring a bank holding company with total consolidated assets of $50 billion or more to appoint a chief risk officer). International authorities (again in the financial sector) recommend that a large financial institution have this position. See, e.g., BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS 22 (2014) (Principle 6, which recommends that banks have an independent risk-management function under the direction of a CRO).

b. Authorities support the proposition that organizations should be free to structure the CRO role in accordance with their needs, i.e., to have the CRO be a stand-alone position, to have an executive with other organizational responsibilities also perform the CRO role, to have the CRO's duties spread among multiple executives, or to have an executive-management-level risk committee handle them. They suggest that the board of directors must evaluate whether the size of the organization and the complexity of the risks to which it is subject require that there be a CRO who is in charge of the risk-management department and who does not have other operational duties. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 152 ("Depending on the size and complexity of the organization, dedicated risk and control personnel may support functional management to manage different risk types (e.g., operational, financial, quantitative, qualitative) by providing specialized skills and guidance to front-line management and other personnel and evaluating internal control."); BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS, supra, at 23 (paragraph 108: "The CRO, however, should not have management or financial responsibility related to any operational business lines or revenue-generating functions and there should be no

'dual hatting' (ie the chief operating officer, CFO, chief auditor or other senior manager should in principle not also serve as the CRO).") (footnote omitted). Indeed, in certain large financial firms, an executive with business responsibilities is not permitted to act as a CRO. 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, I.E.7(d) (2018) ("No front line unit executive oversees any independent risk management unit.").

Uncertainty about where to situate the CRO in an organization may be related to the multiple roles that the CRO may play: as overseer or as business partner and adviser. This uncertainty may be related to the history of the CRO position. A CRO was first used in a large financial firm as an administrator to prevent the recurrence of large investment losses, and then the CRO position evolved to be that of a partner with the business in its risk taking and management. See generally Anette Mikes, *Chief Risk Officers at Crunch Time: Compliance Champions or Business Partners?* 2 J. RISK MGMT. IN FIN. INST. 7 (2008); Anette Mikes, *Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer, in* ENTERPRISE RISK MANAGEMENT (John Fraser & Betty Simkins eds., 2010).

c. Authorities also recommend that, if there is a CRO in charge of risk management, this executive should have the stature, independence, and resources to accomplish the responsibilities of the position. See BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS, supra, at 23 (paragraph 108, providing: "The CRO should have the organisational stature, authority and the necessary skills to oversee the bank's risk management activities. The CRO should be independent and have duties distinct from other executive functions."); 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.C.2(g) (2018) (responsibility of CRO for risk-management staffing). Having the CRO report to the board of directors, or to a board risk committee, which would also approve the officer's hiring and dismissal, and compensation, enhances this independence and stature. 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, I.E.7(b) (2018) (unrestricted access of CRO to board of directors and its committees); id. (c) (board or risk committee approves hiring, dismissal, and compensation of CRO).

d. CRO responsibilities are increasingly standardized through codes of best practices and regulation and understandably reflect the responsibilities of the risk-management program. A significant responsibility is to assist the board of directors and senior executives in identifying the risks facing the organization and in managing them. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 152 ("The chief risk/control officer is responsible for reporting to senior management and the board on significant risks to the business and whether these risks are managed

within the entity's established tolerance levels, with adequate internal control in place."). More specifically, the CRO helps senior executives formulate a framework and program for managing the organization's risks. See 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, Appendix D, II.C.2(a)-(d) (2018) (setting out these responsibilities); BASEL COMM. ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS, supra, at 23 (paragraph 107, providing: "The CRO is responsible for supporting the board in its development of the bank's risk appetite and RAS [risk appetite statement] and for translating the risk appetite into a risk limits structure."). Similarly, the CRO ensures that the organization has in place policies and procedures for testing the risk-management framework to see whether it is adequate for the organization's risk situation. See, e.g., 12 C.F.R. § 252.33(b)(2)(i)(C) (2018) (from the Board of Governors of the Federal Reserve System's prudential standards for certain bank holding companies). The CRO also oversees the communication to all organizational actors concerning risks and the organization's risk limits and controls. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 152. In addition, the CRO puts into place a system for monitoring organizational actors' compliance with the risk-management program. See, e.g., 12 C.F.R. § 252.33(b)(2)(i)(A) (2018) (monitoring of compliance with risk limits), id. (C) (monitoring of the risk controls).

e. Authorities recommend that the CRO report to executive management, a management risk committee, and, when appropriate, the board of directors about the effectiveness of the risk-management framework and propose necessary modifications to it that arise from changes in the risk environment of the organization. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 152 ("The chief risk/control officer is responsible for reporting to senior management and the board on significant risks to the business and whether these risks are managed within the entity's established tolerance levels, with adequate internal control in place."); 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.C.2(b) (2018) (independent risk management should "determin[e] if actions need to be taken to strengthen risk management or reduce risk given changes in the covered bank's risk profile or other conditions."); INT'L STANDARD, RISK MANAGEMENT—PRINCIPLES AND GUIDELINES, ISO 31000 13 (2009) (paragraphs 4.5 and 4.6, noting the need for monitoring of the risk-management framework and its continual improvement). It is also expected that the CRO alert senior executives, particularly the chief executive officer, the board of directors, or a board risk committee to disagreements over risk matters and deviations from and failures to adhere to the risk-management program by executives and other organizational actors, which disagreements, deviations, and failures risk officers identified through their monitoring. 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.C.2(e) (2018) (reporting about disagreements over risk assessment between risk officers and front-line management and about the latter's failure to adhere to risk guidelines); 12 C.F.R. § 252.33(b)(2)(ii) (2018) ("The chief risk officer is responsible for reporting risk-management deficiencies and emerging risks to the risk committee and resolving risk-management deficiencies in a timely manner."). The organization may have in place a governance structure where the CRO reports only to the board of directors, or one of its committees, if disagreements over risk assessments and failures to adhere to the risk-management program involve senior executives, especially the chief executive officer, or if executives are not holding front-line employees responsible for such adherence. See 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.C.2(f) (2018). The CRO may learn of weaknesses in the risk-management program or failures to comply with it from the chief audit officer. See, e.g., id. at II.C.3 (describing the role of internal audit in evaluating risk management in the organization); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 154 ("The scope of internal auditing is typically expected to include oversight, risk management, and internal control, and assist the organization in maintaining effective control by evaluating its effectiveness and efficiency and by promoting continual improvement.").

§ 3.17. Chief Audit Officer

(a) An organization should have a chief audit officer ("CAO") who is responsible for the internal-audit function and does not have other operational responsibilities.

(b) The CAO's compliance and risk-management responsibilities should include the following:

(1) for the purposes of formulating, implementing, and testing the organization's internal-audit plan:

(A) to be informed of the major legal obligations applicable to, and the main values in the code of ethics for, the organization, its employees, and agents and of the material risks to which the organization is or will be exposed,

(B) together with internal auditors and with the support of executive management, to formulate and implement an internal-audit plan that includes compliance and risk management within its assessment of the organization's internal-control environment, and any revisions to that plan, and

(C) to oversee internal auditors' regular testing and reassessment of the plan;

(2) to manage the internal-audit department, which includes making recommendations to executive management about its staffing and resources, and to decide upon the hiring, dismissal, compensation, work conditions, placement within the organization, and reporting lines of the internal auditors and other internal-audit personnel;

(3) to be the organization's liaison with regulators on its internal audit;

(4) to communicate regularly with the board of directors, the board audit committee, any other board committee responsible for compliance or risk-management oversight, and executive management about the internal-control environment for compliance and risk management;

(5) to meet at reasonable intervals with executive management to report on the effectiveness of and inadequacies in the internal-audit function, including the internal-audit plan for compliance and risk management, and to seek approval for any material modifications;

(6) to confer with executive management:

(A) to notify it of any material failure of the internal audit of compliance and risk management, and

(B) to recommend any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such failure;

(7) to confer with executive management and, when appropriate, the chief compliance officer and the chief risk officer:

(A) to report on the results of the internal audit of compliance and risk management, particularly on the effectiveness of and inadequacies in the compliance function and the risk-management function, and to recommend any necessary changes,

(B) to notify them of any material violation or failure of the compliance program and the code of ethics and of any material deviation from or failure

of the risk-management framework and program that the internal audit revealed,

(C) to identify the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization for compliance or risk management, and

(D) to recommend remedial measures to address such cause or causes; and

(8) to accompany executive management to meet with the board of directors, the board audit committee, or any other board committee responsible for compliance or risk-management oversight, or to meet outside the presence of executive management at the request of the board or its committee, or at the CAO's request, for the following purposes:

(A) to obtain its approval for the internal-audit plan for compliance and risk management, and any material revisions,

(B) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the internal-audit function, including the internal-audit plan for compliance and risk management,

(C) to notify it of any material failure of the internal audit of compliance and risk management, and to propose for approval or to identify for ratification any material disciplinary or remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such failure,

(D) to report on the implementation and the results of the internal audit of compliance and risk management, particularly on the effectiveness of and inadequacies in the compliance function and the risk-management function, and to recommend any necessary changes, and to provide assurance on the internal-control environment of the organization for compliance and risk management, and

(E) to notify it of any material violation or failure of the compliance program and the code of ethics and of any material deviation from or failure of the risk-management framework and program that the internal audit

revealed, to identify the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization for compliance and risk management, and to recommend remedial measures to address such cause or causes.

Comment:

a. General. Subsection (a) provides that an organization may elect to have an officer who is responsible for the internal-audit function (§ 1.01(ff) (definition)) and the internal audit (§ 1.01(dd) (definition)). The chief audit officer ("CAO") (§ 1.01(b) (definition)) is a well-established position in every publicly traded company and in many organizations of comparable size and operations. In certain domains, law and regulation mandate that an organization have this officer. The general duty of the chief audit officer is to evaluate the strength of, and to improve, the organization's internal-control processes.

In dealing extensively with the audit committee in publicly held corporations, The American Law Institute's Principles of Corporate Governance: Analysis and Recommendations treated the committee's oversight of a firm's "senior internal auditing executive." As in the case of § 3.12, which deals with the role of the board audit committee in compliance and risk management, this Principle is intended only to supplement that earlier work by emphasizing that the mandate of the CAO and the internal-audit function should include compliance and risk management. Accordingly, this Principle sets forth the ways in which the CAO ensures that the internal audit covers the compliance function and risk-management function and reports on the internal audit's results with respect to them to the appropriate organizational actors.

This Principle does not require that the CAO be a member of executive management (i.e., the senior-most executives in the organization, § 1.01(v)) because it recognizes that organizations should have the flexibility as to where to situate the CAO in the organization's hierarchy. However, as in the case of the other internal-control officers, making the CAO a member of executive management gives that officer a "seat" at the chief-executive-officer's table and thus underscores the importance of internal audit in an organization. A CAO, however, should not have operational responsibilities, for they could interfere with the CAO's internal-control duties and threaten the officer's independence. Under the CAO's oversight, the internal-audit function acts as an organization's "third line of defense" of internal control, § 1.01(fff), that checks on the performance of the other two "lines of defense," business operations, , and the internal-control

functions of compliance and risk management. These officers should not be put in a conflict-of-interest situation in which they must audit their own activities, which would occur if they had business or other operational responsibilities.

As suggested above, this Principle provides for a CAO who is most appropriate for a publicly traded company or other organization of comparable size and operations, or for one in a highly regulated industry. This Principle acknowledges that an organization may structure its internal-audit function in different ways, including by assigning the CAO's responsibilities to several internal-audit officers or to another internal-control officer, or even, in the case of a small organization, by outsourcing some or all of them. See also § 3.20 (multiple responsibilities of internal-control officer) and § 3.21 (outsourcing).

b. CAO responsibilities in general. Subsection (b) specifies the CAO's important compliance and risk-management responsibilities, which are similar to those of other internal-control officers and which are primarily based upon the internal audit of compliance and risk management. They also include those responsibilities typically associated with the management of an internal-control department. Because the board of directors oversees (§ 3.08(b)(5)), and executive management supports the implementation of (§ 3.14(b)(5)), the organization's internal-audit plan for compliance and risk management, subsection (b) also includes provisions dealing with responsibilities associated with the interaction between the CAO and these organizational actors.

c. CAO responsibilities; formulating, implementing, and testing the internal-audit plan. Subsection (b)(1)(A) clarifies that a CAO should be informed of the significant laws and regulations affecting the organization, its employees, and agents, the ethical values in the organization's code of ethics, and the material risks arising from the organization's affairs. The CAO's knowledge should be extensive—although it does not have to be at the level of a chief compliance officer or a chief risk officer—because, as stated in subsection (b)(1)(B), this officer, with the internal auditors and supported by executive management, must formulate and implement the internal-audit plan that includes compliance and risk management within its assessment of the organization's internal-control environment, and any revisions to that plan. All this presumes that the CAO has background or education in compliance and risk management. See § 3.06 (ways that internal-control officers acquire this expertise). Unlike the chief compliance officer and chief risk officer who collaborate with and are directed by executive management, the CAO works

independently and receives only the support of senior executives in overseeing the implementation of the internal-audit plan. See § 3.14(b)(5) (executive management's support). Subsection (b)(1)(C) also provides that the CAO should oversee the necessary testing and reassessment of the internal-audit plan that internal auditors conduct and that can reveal the plan's effectiveness and inadequacies. This testing also serves as the basis for the CAO's reporting on these subjects to executive management, under subsection (b)(5), and to the board of directors, under subsection (b)(8)(B).

d. CAO responsibilities; managing the internal-audit department. Subsection (b)(2) provides that the CAO should manage the internal-audit department. Like other internal-control officers, the CAO has typical managerial authority over it. In particular, the CAO should be able to recommend to executive management proposed courses of action on standard managerial issues, such as the appropriate staffing of and the use of resources for the department, and to decide upon the hiring and dismissal, compensation, work conditions, and the appropriate organizational structure for internal auditors and other internal-audit personnel. In other words, executive management makes the overall resource-allocation and staffing decisions, see § 3.14(b)(6) (executive management's responsibilities for these matters), but the CAO makes those decisions typically associated with department management.

Internal auditors generally report only to the CAO, which ensures their independence from operational pressures and helps to produce an effective audit. Moreover, although the CAO is under the authority of executive management and ultimately the chief executive officer, the CAO should have unqualified independence to ensure that the internal-audit department operates as an effective part of the organization's internal control. Other Principles recommend that the board of directors or its audit committee approve the hiring, terms of employment, and the dismissal of the CAO, which contributes to this independence. See § 3.08(b)(7) (board's responsibility); § 3.12(d)(3) (audit committee's responsibility). See also The American Law Institute's Principles of Corporate Governance: Analysis and Recommendations § 3A.03(c) (AM. LAW INST. 1994) (board audit committee's authority on this issue).

e. CAO responsibilities; acting as a liaison with regulators. Subsection (b)(3) provides that, in appropriate circumstances, the CAO may act as the organization's liaison on its internal-audit matters with regulators who have legal authority over it. This may occur where, in certain industries, a regulator is mandated to directly supervise the conduct of the organization, including

its internal audit, and where the CAO is thus required to report on the audit to the regulator. In these circumstances, the regulator may demand, or expect, direct contact with an organization's CAO. This liaison activity is distinguished from any reporting to regulators of material failures of the internal audit of compliance and risk management, which reporting may be based upon the CAO's reports to executive management and the board, covered respectively in subsections (b)(6)(B) and (b)(8)(C).

f. CAO responsibilities; communicating with the board and executive management. Subsection (b)(4) provides that, irrespective of the CAO's place in an organization's managerial structure, the CAO should regularly communicate with the board of directors, the board audit committee, any other board committee responsible for the oversight of compliance or risk management, and executive management about the organization's internal-control environment for compliance and risk management. This subsection is thus the necessary counterpart to § 3.08(b)(8) (board communicating with internal-control officers), § 3.12(d)(4) (audit committee communicating with the CAO), and § 3.14(b)(8) (executive management communicating with internal-control officers) and is further explained in Comment *g* to § 3.08, Comment *d* to § 3.12, and Comment *g* to § 3.14. This communication is in addition to the reporting covered in subsections (b)(6), (7) and (8).

g. CAO responsibilities; meeting with executive management on effectiveness and inadequacies of the internal-audit function. Subsection (b)(5) provides that the CAO should report on the effectiveness of and inadequacies in the internal-audit function, including the internal-audit plan for compliance and risk management, and recommend any necessary changes to that function. See § 3.14(b)(9) (executive management's having such meetings with the CAO and other internal-control officers). These kinds of reports and meetings, which are generally based upon internal testing of the internal-audit plan, see subsection (b)(1)(C), enable executive management to fulfill its responsibility for maintaining an effective internal-audit function.

h. CAO duties; meeting with executive management on material failures of the internal audit of compliance and risk management. Subsection (b)(6)(A) provides for exceptional reporting when the CAO alerts executive management to any material failure of the internal audit of compliance and risk management. See § 3.14(b)(10) (provision dealing with executive management's receiving such report) and Comment *i* (where the purposes of this reporting are explained). Under subsection (b)(6)(B), like other internal-control officers, the CAO may

recommend disciplinary and remedial measures, including reporting to a regulator, that executive management may determine to take in response to the failure. In all but the rare case, executive management, not the CAO, makes this determination (particularly as to disciplinary matters), with approval by the board of directors. The chief legal officer should be included in any meetings between executive management and the CAO on these issues (this is provided in § 3.14(b)(10)) because that officer is responsible for legal advice on the organization's response to the material failure. See § 3.18(b)(3) and Comment *e* (role of chief legal officer in the investigation of such failure).

i. CAO duties; meeting with executive management and internal-control officers on results of the internal audit of compliance and risk management. Subsection (b)(7) specifies that the CAO should regularly meet with executive management and, when appropriate, the chief compliance officer and the chief risk officer on the results of the internal audit of compliance and risk management. Under subsection (b)(7)(A), the CAO should report on problems relating to the compliance function and the risk-management function, particularly regarding the effectiveness of and inadequacies in the organization's compliance program, code of ethics, risk-management framework, and risk-management program that the internal audit identified, and recommend any necessary changes to address them. This subsection thus reflects the contribution that the "third line of defense" of the internal-audit function makes to having effective compliance and risk management in an organization. See § 4.06(b)(4) (ongoing review necessary for an effective risk-management program) and § 5.06(n) (regular assessment as an element of a compliance program). The chief compliance officer and the chief risk officer are included in these meetings, which may be combined with their annual meetings with executive management on the effectiveness of their functions, see § 3.15(b)(8) and § 3.16(b)(8), to receive the CAO's feedback directly. Subsection (b)(7)(B) provides for exceptional reporting when the CAO alerts executive management, the chief compliance officer, and the chief risk officer to a material violation or failure of the compliance program or the code of ethics or to a material deviation from or failure of the risk-management framework or program that comes to the attention of the CAO through the internal audit. See § 3.14(b)(10) (provision dealing with executive management's receiving such report) and Comment *i* (purposes of this reporting). In these circumstances, the CAO should not wait for a regular meeting to report on the event. Under subsection (b)(7)(C), the CAO should identify the cause or causes of such violation, failure, or deviation, which could include a systemic weakness

in the internal-control environment for compliance and risk management in the organization, and, under subsection (b)(7)(D), may recommend remedial measures to address them. The chief legal officer is included in any meetings between executive management and the CAO on these issues (§ 3.14(b)(10)) because that officer provides legal advice on the organization's response to the violation, failure, or deviation. See § 3.18(b)(3) and Comment *e* (role of chief legal officer in the investigation of such violation, failure, or deviation). The following is an example of this kind of CAO reporting:

> After having conducted the internal audit of Company, the CAO has determined that the Company's risk-management policies, procedures, and controls are deficient in one of the Company's business lines. The officer should report the deficiencies to executive management and the audit committee, with recommendations for remediation. These recommendations could include that the line of business in question be restricted in its activities until effective policies, procedures, and controls are designed and implemented.

j. CAO responsibilities; meeting with the board of directors. Finally, subsection (b)(8) provides that the CAO should meet with the board of directors, its audit committee, or any board committee responsible for compliance or risk management oversight on a number of issues of relevance to the board's oversight of internal-control functions in the organization. The provision presumes that, in these meetings, the CAO accompanies and assists executive management as the organization's internal-audit specialist, although it recognizes that, in certain circumstances, the board, the audit committee, another board committee, or the CAO may request a meeting without the presence of executive management. Each of the provisions in this subsection thus has its counterpart in the Principles dealing with the responsibilities of the board of directors (§ 3.08), the audit committee (§ 3.12), and executive management (§ 3.14): (i) obtaining approval of the internal-audit plan for compliance and risk management and reporting on its implementation (§ 3.08(b)(5), § 3.12(d)(1), and § 3.14(b)(11)(A) and (B)); (ii) reporting on the effectiveness of and inadequacies in the internal-audit function, with particular emphasis on the internal-audit plan for compliance and risk management (§ 3.08(b)(9), § 3.12(d)(5), and § 3.14(b)(11)(C)); (iii) reporting on any material failure of the internal audit of compliance and risk management and recommended remedial measures (§ 3.08(b)(10), § 3.12(d)(6), and § 3.14(b)(11)(D)); (iv) reporting on the results of the internal audit of compliance and risk management and recommending any necessary changes to these internal-control functions (§ 3.08(b)(5),

§ 3.12(d)(7), and § 3.14(b)(5)); and (v) reporting on any material violation or failure of the compliance program and the code of ethics, and material deviation from or failure of the risk-management framework and program, its cause or causes, again revealed by the internal audit, and recommended remedial measures (§ 3.08(b)(10), § 3.12(d)(7), and § 3.14(b)(11)(D)).

REPORTERS' NOTE

a. The CAO as the head of internal audit is a well-established position in firms today. See GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 130-31 (2017) (discussing the position generally); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 150 (2013) (placing the CAO within senior management). The American Law Institute's Principles of Corporate Governance contemplated that the board audit committee of publicly held firms would have oversight of a "senior internal auditing executive." See Principles of Corporate Governance: Analysis and Recommendations § 3A.03(c), (g) (AM. LAW INST. 1994) (treating the committee's appointment and dismissal of this executive and its review of the adequacy of a company's internal controls with this executive). Although neither law nor regulation requires a public company to have this position, stock-exchange rules mandate that a company have an internal-audit function. See, e.g., NYSE, Inc., Listed Company Manual § 303A.07(b)(iii)(E) & (c) (2018) (specifying required meeting between audit committee and internal auditors and requirement of internal-audit function). It is customary to have an executive in charge of this function. See ABA SECTION OF BUS. LAW, COMM. ON CORP. LAWS, CORPORATE DIRECTOR'S GUIDEBOOK (6th ed. 2011), 66 BUS. LAW. 975, 1021 (2011) (discussing the practice of the audit committee meeting with the "senior internal auditing executive"). The position is legally required in certain large commercial banks. See 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. part 30, app. D, II.L.1. (2018) (requiring the board of a large bank to appoint a "Chief Audit Executive"). See also BASEL COMM. ON BANKING SUPERVISION, THE INTERNAL AUDIT FUNCTION IN BANKS 5 (2012) (Principle 2, paragraph 18; referring to the head of the internal-audit function).

b. If the board of directors elects to have a CAO, rather than to divide the responsibilities of the position among multiple executives or even to outsource it, authorities recommend that the officer not have other operational responsibilities because of the nature of a position involving review of every activity in a firm. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 154 ("Internal auditors do not assume operating responsibilities, nor are they assigned to audit activities with which they were involved recently in connection with prior operating assignments."). They also recommend that this officer have the stature, independence, and resources to accomplish the duties of the position. See BASEL COMM. ON BANKING SUPERVISION, THE INTERNAL AUDIT FUNCTION IN BANKS, supra, at 4-5 (Principle 2, paragraph 12). This independence and stature are

enhanced by having the CAO report to the board of directors, or its audit committee, which would also approve the officer's hiring and dismissal, and compensation. See, e.g., COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 154 ("Internal auditors have functional reporting to the audit committee and/or the board of directors and administrative reporting to the chief executive officer or other members of senior management."); 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, I.E.8(a) & (c) (2018) (setting out the requirements that the audit committee receive the CAO's report and determine the hiring and dismissal of the CAO).

c. Authorities point out that the duties of the CAO as to the audit of compliance and risk management should be essentially the same as those with respect to the audit of the organization's other activities. The internal-audit plan should cover the internal-control functions, including compliance and risk management. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 154 (stating this point generally); Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8996 (Feb. 23, 1998) ("Although many monitoring techniques are available, one effective tool to promote and ensure compliance is the performance of regular, periodic compliance audits by internal or external auditors who have expertise in Federal and State health care statutes, regulations and Federal health care program requirements."); 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.C.3(a) & (b) (2018) (setting out how the internal audit will test risk management); BASEL COMM. ON BANKING SUPERVISION, THE INTERNAL AUDIT FUNCTION IN BANKS, supra, at 12 (Principle 13: "The internal audit function should independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes.") (bold omitted). The CAO ensures that the internal-audit plan is tested and updated to reflect changes in the firm's compliance and risk environment and in light of internal-audit developments. 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.C.3(f) (2018) (testing). In certain sectors, the CAO may be expected to communicate findings about the adequacy of the organization's internal-control functions to regulators. See, e.g., BASEL COMM. ON BANKING SUPERVISION, THE INTERNAL AUDIT FUNCTION IN BANKS, supra, at 15 (Principle 16: "Supervisors should have regular communication with the bank's internal auditors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) monitor the bank's response to weaknesses identified.") (bold omitted).

d. Guidance and regulation emphasize that a key CAO responsibility is to meet with executive management, including the chief compliance officer and the chief risk officer, and with the board of directors, or its audit committee, to report on the results of the internal audit of the compliance and risk-management functions and to offer solutions to any shortcomings or inefficiencies in them that surfaced in the internal audit. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 154 ("The scope of internal auditing is typically expected to include oversight, risk management, and internal control, and assist the organization in maintaining effective control by evaluating its effectiveness and efficiency and by promoting continual improvement. Internal audit communicates findings and interacts directly with management, the audit committee, and/or the board of directors."). The CAO is also expected to identify for these organizational actors material violations or failures of the compliance program or material deviations from or failures of the risk-management program, as well as significant weaknesses in the organization's internal-control environment. See U.S. DEP'T OF JUSTICE, CRIMINAL DIV., FRAUD SECTION, EVALUATION OF CORPORATION COMPLIANCE PROGRAMS 6 (2017) ("What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?"). Here authorities suggest that the CAO should try to determine the cause or causes of the violation, failure, deviation, or weakness and the effectiveness of any solution. See 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.C.3(c) (2018) (requiring internal auditors to "identify [to the audit committee] the root cause of any material issues" and evaluate how effective is the response of the business line and risk management to resolving the issues); BASEL COMM. ON BANKING SUPERVISION, THE INTERNAL AUDIT FUNCTION IN BANKS, supra, at 12 (Principle 12, paragraph 59: "Therefore, the internal audit function should inform senior management of all significant findings so that timely corrective actions can be taken. Subsequently, the internal audit function should follow up with senior management on the outcome of these corrective measures. The head of the internal audit function should report to the board, or its audit committee, the status of findings that have not (yet) been rectified by senior management.").

§ 3.18. Compliance and Risk-Management Responsibilities of Chief Legal Officer

(a) An organization should have a chief legal officer ("CLO") who is primarily responsible for all legal advice to organizational actors.

(b) The CLO should have the following compliance and risk-management responsibilities:

(1) to provide advice on a regular basis and as requested to the board of directors, any board committee, executive management, and internal-control officers with respect to the legal obligations of the organization, its employees, and agents, the risks arising from noncompliance with them, and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them;

(2) to advise the board of directors, any board committee, executive management, and the appropriate internal-control officer about:

(A) any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them, and the material risks to which the organization is or may be exposed and the effectiveness of the risk-management framework and program in addressing them, and

(B) the adequacy of such disclosure or reporting; and

(3) unless otherwise directed by the board:

(A) to advise the board of directors, any board committee, executive management, and the appropriate internal-control officer on, and to conduct the investigation of, any material violation or failure of the compliance program or the code of ethics, any material deviation from or failure of the risk-management program, or any material failure of the internal audit, and

(B) to advise them on any remedial or disciplinary measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation, failure, or deviation.

Comment:

a. General. Subsection (a) reflects that the CLO, as general counsel, is a well-established position in publicly traded companies and other organizations of comparable size and operations, or those whose circumstances require internal legal expertise. The CLO is the paramount authority on legal matters and, as stated in subsection (a), is primarily responsible for providing all legal advice to organizational actors. Because this Principle focuses only on the CLO's specific

contributions to compliance and risk management, it expressly does not deal with the breadth of a general counsel's role in an organization, which goes well beyond the CLO's responsibilities with respect to these internal-control functions and which is outside the mandate of these Principles. See § 5.22 (discussing legal services of attorneys in compliance). It also does not address the applicability of the attorney–client privilege or work-product doctrine to the CLO's provision of advice or conduct of an investigation that this Principle sets forth. See § 5.27 and Comments (privileges in internal investigations); § 6.14 (an organization's waiver of the attorney–client privilege and work-product protection). Moreover, in situating the CLO under the topic of internal-control officers, this Principle underscores that it is focusing here only on the CLO's compliance and risk-management responsibilities, not on the many possible activities of an organization's lawyer and that lawyer's relationships with the client organization. For example, a CLO may be, as general counsel, a member of executive management while also having the enumerated internal-control responsibilities.

b. CLO's compliance and risk-management responsibilities; in general. Subsection (b) identifies ways in which the CLO should contribute to the organization's compliance and risk-management functions. While this list is not exhaustive, it highlights key responsibilities that follow from the CLO's position and expertise set forth in subsection (a) and that make the CLO an important participant in an organization's compliance and risk management. In setting forth the CLO's responsibilities, subsection (b) does not address the nuances and complexities in the interactions between the CLO and other organizational actors. For example, a CLO may determine that a particular course of action is legal, but executive management, on the advice of both the CLO and the chief compliance officer, may decide that the organization should not engage in it because it runs counter to the organization's culture.

c. CLO's compliance and risk-management responsibilities; providing legal advice. Subsection (b)(1) states that, as the paramount legal authority in the organization, the CLO should regularly provide advice to a wide range of organizational actors about their and the organization's legal obligations, the risks of not fulfilling them, and the effectiveness of the compliance program and the code of ethics (if the latter addresses in any way legal obligations) in ensuring compliance with them. See, e.g., § 3.08(b)(1) (providing that members of the board of directors should be informed about the legal obligations of the organization and organizational actors); § 3.14(b)(1) (similar responsibility of executive management). Since an important goal of the compliance

program is to ensure that the organization, its employees, and agents comply with their legal obligations, the chief compliance officer should consult with the CLO about, among other things, the design of the compliance program to deal with those obligations, any modifications to it to address new legal developments, and its effectiveness. See § 5.13(b) (providing for the chief compliance officer's receiving guidance from the CLO in the event of "legal uncertainty"). Similarly, executive management and the board of directors (or the board compliance and ethics committee) would also seek the CLO's advice when they approve, or review the effectiveness of and inadequacies in, this program and any significant modifications to it.

In a related fashion, the CLO advises the chief risk officer, executive management, and the board (or its risk committee), among others, about the compliance and legal risks facing the organization, its employees, and agents that the organization's risk-management program should address. See § 5.08(b) (providing that a legal officer may offer compliance advice). Accordingly, the CLO would be expected to contribute to the design of this program.

d. CLO's compliance and risk-management responsibilities; advising on disclosure and regulatory reporting. An important role of the CLO is to anticipate, and, if necessary, to defend the organization in, litigation brought against it, including by regulatory enforcement officials and prosecutors. As provided in subsection (b)(2), the CLO should counsel the appropriate organizational actors, particularly executive management, the board of directors, or a board committee, when there is any mandatory or discretionary public disclosure or reporting to a regulator about the organization's compliance and risk-management programs. This subsection is a counterpart to § 3.10(d)(8) and § 3.11(d)(8), which discuss the context of such disclosure and regulatory reporting, and recommend that the board compliance and ethics committee and risk committee seek out the advice of the CLO in these circumstances, and to § 3.14(b)(11)(E), which underlines executive management's responsibility for the disclosure and reporting. Simply put, the CLO advises as to the legality of and legal consequences arising from the disclosure and reporting.

e. CLO's compliance and risk-management responsibilities; advising on and investigating material violations, failures, or deviations. Subsection (b)(3) reflects that the CLO is expected to be called upon and actively involved when there has occurred a material violation or failure of the compliance program or the code of ethics, a material deviation from or failure of the risk-management program, or a material failure of the internal audit of compliance and risk management, which may trigger remedial or disciplinary measures that could include reporting to

a regulator. In these cases, the CLO generally takes charge of and conducts any internal investigation and the legal defense of the organization, including protecting the attorney–client privilege and, if necessary, engaging outside counsel, for the investigation of the violation, failure, or deviation. See § 5.26(b) (providing that a lawyer should lead or participate in investigations posing a material threat to the organization's financial condition or strategic plan). The CLO assumes paramount authority over litigation on these compliance and risk-management matters, just as the officer would for other litigation against the organization, and advises on disciplinary and remedial measures. At its discretion (e.g., if the CLO is implicated in the misconduct), the board of directors may direct the CLO not to be involved in a particular investigation. In such cases, another officer or outside counsel would assume the advisory and investigatory role.

f. CLO serving as, or exercising direct authority over, the chief compliance officer. This Principle does not address or reflect options that certain organizations have elected: to have the CLO also serve as the chief compliance officer, or to have the chief compliance officer be in the direct reporting line of the CLO. These options have been justified on the following grounds, among others: because the CLO is the paramount authority on legal matters in the organization, the officer has the expertise to serve as the chief compliance officer or to exercise organizational authority over that position. Moreover, this combination or linking of the two positions is also justified on historical grounds because compliance was part of and grew out of the legal department. The trend today—which this Principle supports if an organization's circumstances allow—is to separate the CLO and chief-compliance-officer positions and to have the chief compliance officer be under the direct authority of the chief executive officer or the board of directors. In some domains, law and regulation mandate this separation and reporting. Among other reasons, the separation of these positions is based on the fact that the CLO's duty of loyalty to the organization can conflict with the role of the chief compliance officer as the organization's liaison with regulators. This separation also avoids the issue of whether the CLO can assert attorney-client privilege with respect to communications made while acting as the chief compliance officer. See Comment *a*, supra.

If an organization elects to have its CLO also serve as a chief compliance officer, the CLO would be expected to undertake the chief compliance officer's responsibilities and to manage the compliance department, as specified in § 3.15. Moreover, if it decides to place the chief compliance officer under the direct authority of the CLO in its management structure, the chief compliance

officer should still communicate regularly with other organizational actors, as provided by the Principles. See § 3.08(b)(8) (communication of chief compliance officer with the board of directors);

§ 3.10(d)(5) (chief compliance officer's communication with the board compliance and ethics committee). In this case, an organizational actor superior to the CLO should also approve the hiring, terms of employment, and dismissal of this officer. See § 3.08(b)(7) (requiring board approval for these actions); § 3.10(d)(4) (approval of the board compliance and ethics committee for the same).

REPORTERS' NOTE

a. The literature on the role of the general counsel in organizations is a rich one, see, e.g., Ben W. Heineman, Jr., et al., *Lawyers as Professionals and as Citizens: Key Roles and Responsibilities in the 21st Century,* Center on the Legal Profession, Harvard Law School 22-35 (2015), https://clp.law.harvard.edu (discussing the complex roles of the lawyer in corporate law departments); E. Norman Veasey & Christine T. Di Guglielmo, *The Tensions, Stresses, and Professional Responsibilities of the Lawyer for the Corporation,* 62 BUS. LAW. 1, 5-8 (2006) (presenting an overview of the modern general counsel), as is the literature on the involvement of the CLO in compliance, particularly as a chief compliance officer, see SEC. INDUS. ASS'N, COMPLIANCE & LEGAL DIV., WHITE PAPER ON THE ROLE OF COMPLIANCE 1 (2005) (recounting how, prior to the early 1960s, legal departments generally had responsibility for compliance in the brokerage industry). Also well documented, and debated, has been the ongoing relationship between the CLO and the chief compliance officer, when the latter has become a stand-alone position with its own department. See Robert C. Bird & Stephen Kim Park, *The Domains of Corporate Counsel in an Era of Compliance,* 53 AM. BUS. L.J. 203 (2016) (discussing the debate over the CLO's role in compliance with the emergence of stand-alone chief compliance officers and identifying the CLO's contributions to compliance); Michele DeStefano, *Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 10 HASTINGS BUS. L.J. 71 (2014) (comprehensively covering the relationship of compliance and legal departments, regulators' pressures to separate the two, and the intellectual debates on the merits of the separation); Sean J. Griffith, *Corporate Governance in an Era of Compliance,* 57 WM. & MARY L. REV. 2075, 2101-2102 (2016) (discussing the movement of compliance into its own department with a chief compliance officer reporting directly to the chief executive officer, although presenting survey data showing continuing organizational links between that officer and the legal department). See also CONTROL RISKS, INTERNATIONAL BUSINESS ATTITUDES TO COMPLIANCE: REPORT 2017 21 (2017) (reporting that, in their survey, larger companies allocate compliance to a specialist compliance team, given that the general counsel has too many other responsibilities). There is survey data available about the chief compliance officer's reporting line, with some data indicating that direct reporting to the general counsel is becoming less prevalent in business firms

today. See, e.g., LRN, THE 2015 ETHICS AND COMPLIANCE EFFECTIVENESS REPORT 7 (2015) (showing that, collectively, chief compliance officers report more often to others, such as the audit committee and the chief executive officer, rather than to the general counsel, although the latter remains the largest single reporting line); SOC'Y OF CORP. COMPLIANCE AND ETHICS & NYSE GOVERNANCE SERV., COMPLIANCE AND ETHICS PROGRAM ENVIRONMENT REPORT 11 (2014) (data on chief compliance officer reporting).

b. Authorities explain that the CLO and legal personnel provide legal advice to organizational actors, including compliance personnel, regarding legal obligations imposed upon the organization and the organizational actors, as well as legal risks from noncompliance. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 153 (2013) ("Counsel from legal professionals is key to defining effective controls for compliance with regulations and managing the possibility of lawsuits."); N.Y. CITY BAR, REPORT OF THE TASK FORCE ON THE LAWYER'S ROLE IN CORPORATE GOVERNANCE 98 (Nov. 2006) ("A strong General Counsel is an important participant in a good corporate governance process[,]… is a key advisor to senior management. … [and] is uniquely positioned to bring relevant matters to the Board of Directors."). It has been argued that, in its advisory role with the board of directors and senior executives, the CLO occupies a unique position to promote an ethical organizational culture. See Robert C. Bird & Stephen K. Park, *The Domains of Corporate Counsel in an Era of Compliance,* 53 AM. BUS. L.J. 203 (2016).

c. There is support for the proposition that good practice requires the CLO to be involved in any public disclosure and reporting to regulators on compliance and risk-management matters, other than on minor and routine disclosure. See N.Y. CITY BAR, REPORT OF THE TASK FORCE ON THE LAWYER'S ROLE IN CORPORATE GOVERNANCE, supra*,* at 98 (observing that the general counsel often participates in "the preparation of SEC disclosure and other regulatory filings."). Some argue that the CLO has an important role in a firm's competitive position by its creative interaction with regulators. See, e.g., Constance E. Bagley, et al., *Who Let the Lawyers Out?: Reconstructing the role of the Chief Legal Officer and the Corporate Client in a Globalizing World*, 18 U. PA. J. BUS. L. 419, 471-476 (2016) (discussing examples of these interactions).

d. It is also well accepted that the CLO generally assumes responsibility for undertaking the organization's investigation and legal defense when a legal violation or a material failure of the organization's rules has occurred, unless the CLO decides to call upon the assistance of outside counsel. See N.Y. CITY BAR, REPORT OF THE TASK FORCE ON THE LAWYER'S ROLE IN CORPORATE GOVERNANCE, supra*,* at 154-155 (discussing these issues). Indeed, under law and regulation, the CLO of a public company who receives from another lawyer a report of a material violation of the securities law or a breach of fiduciary duty by the company, an officer, director, or agent is required to investigate and take reasonable steps to ensure that the company has adopted an appropriate response to the matter. See 15 U.S.C. § 7245 (2018); 17 C.F.R. § 205.3(b)(1) & (2) (2018). See also U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(7), supra, at 535 (2016) (a feature of an effective compliance and ethics program is that, under it, after the detection of criminal conduct the organization "take[s] reasonable steps to respond appropriately to the criminal conduct….").

The steps may include "restitution" to victims and "other forms of remediation," "self-reporting and cooperation with authorities," id., cmt. app. n.6, supra, at 538, actions typically taken with the CLO's advice.

§ 3.19. Compliance and Risk-Management Responsibilities of the Human-Resources Officer

(a) An organization may elect to have a human-resources officer ("HRO") who is responsible for the human-resources function and, if feasible, does not have other operational responsibilities.

(b) The HRO's compliance and risk-management responsibilities should include the following:

(1) in collaboration with the chief compliance officer, chief legal officer, and chief risk officer and directed by executive management, to formulate policies and procedures that support the compliance program, the code of ethics, and the risk-management framework and program of the organization, for:

(A) the hiring, retention, compensation, performance evaluation, and promotion of employees, including conducting background checks and related personnel testing, and

(B) the status of employees under investigation and the discipline of employees, including their suspension or termination;

(2) to advise executive management, the chief compliance officer, chief legal officer, and chief risk officer on the implications of personnel decisions resulting from employees' violations of the compliance program and the code of ethics and their deviations from the risk-management program;

(3) to administer the organization's policies and procedures for nonretaliation against employees who use the organization's procedures for confidential internal reporting and to report any evidence of retaliation to the appropriate organizational actor; and

(4) to report to the chief compliance officer and the chief legal officer any actual or potential violation of employment-related law and regulation and of the organization's code of ethics and, if delegated this task, in consultation with the chief

legal officer, to oversee the investigation of such violation and to report the results of the investigation to the appropriate organizational actor.

Comment:

a. General. Subsection (a) provides that an organization may elect to have a human-resources officer ("HRO") who is responsible for its human-resources function and who also has important compliance and risk-management responsibilities. Since human resources is a subject ancillary to the focus of these Principles, this Principle is intended only to ensure that compliance and risk management are included within the mandate of the HRO, and it does not specify all the responsibilities of this position nor treat the human resources function in any detail. The subsection does not require the HRO to be a member of executive management (i.e., the senior-most executives in the organization, § 1.01(v)), because it recognizes that organizations should have flexibility as to where to situate this position in the organization's hierarchy. Whether the HRO has operational responsibilities is also a matter for the organization to resolve. Moreover, this Principle acknowledges that an organization may implement the human-resources function in many ways, including by delegating HRO responsibilities to other organizational actors without having an HRO or even by outsourcing some or all of these responsibilities. See also § 3.20 (multiple responsibilities of internal control officer) and § 3.21 (outsourcing). In fact, this Principle may be most appropriate for a publicly traded company or other organization of comparable size and operations that has the resources to support a human-resources department.

b. HRO responsibilities in general. Subsection (b) specifies the HRO's important compliance- and risk-management-related responsibilities. They are primarily based upon the organization's compliance and risk-management activities that are associated with the human-resources function.

c. HRO responsibilities; formulating and implementing personnel policies. Subsection (b)(1) provides that, advised by the chief legal officer, the chief compliance officer, and the chief risk officer and directed by senior executives, the HRO should be responsible for formulating, and then implementing under the direction of executive management, personnel policies and procedures on a number of compliance and risk-management matters. Under subsection (b)(1)(A) these policies and procedures could include screening new employees or "checking" on existing ones for compliant conduct. See § 5.14(a) (an HRO's obligations in this area); § 5.15 (background checks). The policies and procedures could also specify the assistance that the human-resources

department would provide to the compliance program and the risk-management program. This assistance could include monitoring employee activities outside the organization subject to applicable law, assisting in employee training, and carrying out decisions on compensation and promotion that are tied to an employee's compliance with these programs. See § 4.08(b) (risk-management concerns taken into account in the design of employee compensation); § 5.16 (recommending that an employee's compliant conduct be a factor in setting compensation). Under subsection (b)(1)(B), the HRO could also administer personnel and disciplinary decisions arising from an investigation into an employee's violation of the compliance program or deviation from the risk-management program, which could include the temporary reassignment of the employee, an elimination of a bonus, or even the employee's suspension or dismissal from the organization. Except as provided in subsection (b)(4), conducting the investigation would not be within the HRO's responsibilities.

d. HRO responsibilities; advising on implications of personnel decisions. Subsection (b)(2) provides that the HRO should advise and assist executive management and the internal-control officers when a personnel action—such as employee reassignment, suspension, dismissal, or a reduction of compensation—needs to be taken because of compliance-program violations and risk-management program deviations. While the policies and procedures of the human-resources department are likely to cover these matters under subsection (b)(1), the HRO may be called upon to provide advice as to the implications of a specific personnel decision, i.e., how it can be administered or otherwise carried out in accordance with the organization's employment policies and procedures and any applicable law.

e. HRO responsibilities; administering procedures for nonretaliation. An important, and generally legally required, part of an organization's procedures for confidential internal reporting of violations of the compliance program and deviations from the risk-management program is to protect from retaliation those who have used these confidential internal-reporting procedures. See § 5.20 (nonretaliation in this context). Organizations have policies and procedures to put this nonretaliation into practice and to monitor conduct for evidence of retaliation. Because retaliation in this context can be evidenced by adverse personnel actions against the "whistleblower" who used the confidential internal-reporting procedures, subsection (b)(3) provides that the HRO, as the human-resources specialist, should administer the organization's nonretaliation policies and procedures. The HRO should also report any evidence of retaliation to the appropriate

organizational actor, who may be the chief legal officer, the chief compliance officer, or the board compliance and ethics committee. See § 3.10(d)(10) (compliance and ethics committee's oversight of the procedures for confidential internal reporting); § 3.15(b)(5)(B) (chief compliance officer's role in these procedures).

f. HRO responsibilities; reporting and investigating violations of employment-related law. As a result of administering employment and personnel matters in an organization, the HRO may become aware of violations or potential violations of employment-related laws and regulations, such as those relating to antidiscrimination. The HRO may also learn of conduct that violates or could violate the organization's code of ethics. Subsection (b)(4) provides that the HRO should report these matters to the organization's chief compliance officer and chief legal officer, who are, respectively, responsible for the organization's compliance and legal affairs. This reporting gives the HRO a role in promoting effective compliance and an ethical culture in the organization. The HRO may also be delegated the task of conducting investigations of certain kinds of these violations, such as those involving routine employment matters (such as wrongful discharge). Because the chief legal officer is responsible for advising on any material legal violation affecting the organization, see § 3.18(b) (3) and Comment *e*, this subsection requires the HRO to consult with that officer if the HRO has been given any investigative responsibility, even in routine matters. The chief legal officer may permit the HRO to handle an investigation of certain claims, but then assume control over their resolution.

REPORTERS' NOTE

a. That an HRO has compliance and risk-management roles is recognized in the literature. See GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 153 (2017) (discussing the matter generally); COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 150, 152 (2013) (noting that human resources is a "business enabling" function together with legal, compliance, and risk management); BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8, COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES 10 (Oct. 16, 2008) (observing how aspects of the compliance program may be assigned to human resources, among other departments). It is well established that the human-resources department assists in screening candidates for employment, training employees, and administering compensation policies. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 50 (department's role in screening and

training), 58 (its role in compensation). The compliance and risk-management roles of the human resources function are also recognized in practice. See, e.g., KPMG, KEEPING UP WITH SHIFTING COMPLIANCE GOALPOSTS IN 2018: FIVE FOCAL AREAS FOR INVESTMENT 3, 5, 12 (2017) (recommending that human resources be included in compliance management because of its focus on employee data and observing how it can help embed compliance in employee performance evaluations). Conducting background investigations or "checks" on prospective employees is a recommended practice and is required of organizations in certain sectors, such as finance and healthcare. See, e.g., FINRA Rule 3110(e) (2018), http://finra.complinet.com (requiring a FINRA member to investigate the "good character, business reputation, qualifications and experience of" an employee); Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8993 (Feb. 23, 1998) (noting how the chief compliance officer coordinates personnel issues with a hospital's human-resources office). Background investigations are a feature of an effective compliance and ethics program under the U.S. Sentencing Guidelines. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(3) & cmt. app. n.4.(B) 534, 537 (2016) (discussing due diligence in hiring "high-level personnel" and "substantial authority personnel"). Human-resource risks are also recognized in risk-management frameworks. See REPORT OF THE NACD BLUE RIBBON COMM'N ON RISK GOVERNANCE: BALANCING RISK AND REWARD 23 (2009) (including these risks among those about which a public-company board of directors should be concerned).

§ 3.20. Multiple Responsibilities of Internal-Control Officers

(a) Because of its size, operations, or resources, or because of other circumstances and if permitted by law, an organization may elect to have an internal-control officer be responsible for multiple internal-control functions or for non-internal-control operations.

(b) If subsection (a) applies, the organization should put in place safeguards to ensure the effectiveness of the internal-control officer, including the following:

(1) Executive management concludes that the internal-control officer can effectively execute the multiple responsibilities assigned;

(2) The internal-control officer is not given operational or other responsibilities that would create a disabling conflict of interest that would undermine the officer's effective accomplishment of the internal-control responsibilities; and

(3) There are in place organizational procedures to deal with any conflicts of interest (other than those disabling ones that would be excluded under subparagraph

(2) above) that would arise from the assignment of multiple responsibilities to the internal-control officer.

Comment:

a. Multiple responsibilities of internal-control officers. The Principles dealing with internal-control officers provide that, when feasible, an internal-control officer should generally be responsible only for the officer's designated internal-control function and not have other organizational responsibilities. See § 3.15(a), § 3.16(a), § 3.17(a), and § 3.19(a). Those Principles, which are particularly appropriate for a publicly traded company and an organization of comparable size and operations, reflect the conclusion that it could be difficult for an internal-control officer to oversee multiple internal-control functions or to have additional operational responsibilities. Moreover, the independence and impartiality of internal-control officers could be undermined if they were to have a direct organizational interest in transactions or operations that they had also to evaluate from their internal-control perspective. In addition, because an internal-control-officer position, particularly in large organizations, demands considerable specialization and effort, having other internal-control or operational responsibilities could make it difficult for the internal-control officer to devote adequate attention to the officer's internal-control duties.

Subsection (a) recognizes, however, that, in certain circumstances and if permitted by the laws and regulations governing it, an organization may elect to have an internal-control officer take on other internal-control roles or be "dual-hatted" with responsibility for business or operations. These circumstances include situations in which the organization is small or has limited resources or operations. An organization may thus not have the personnel or resources to staff a specific internal-control officer position on a stand-alone basis. It may need to have an employee who has other responsibilities perform internal-control tasks as well. A large organization may also engage in this practice for varying reasons (e.g., have the chief legal officer serve as a chief compliance officer because of a desire to centralize control over legal and law-related matters).

b. Safeguards when an internal-control officer has additional responsibilities. Subsection (b) provides that, if an internal-control officer were to have other responsibilities, the organization should adopt procedures or safeguards to ensure the effectiveness of the internal-control officer in the conduct of that officer's primary internal-control duties and to deal with the problems or conflicts of interest that may arise as a result of this "dual hatting." The subsection identifies three safeguards that point to two problems or issues, but recognizes that there may be others that could

be addressed by additional procedures. Subsection (b)(1) sets forth the understandable caution that, given the importance of the internal-control tasks, executive management who asks an internal-control officer to assume other responsibilities should conclude that the officer has the ability and time to accomplish all of them effectively. Subsection (b)(2) provides that an organization should avoid assigning to an internal-control officer operational responsibilities that would undermine that officer's internal-control position. For example, it would generally be incompatible for the head of a business firm's sales department to serve as a chief compliance officer, because this person would likely not have the independence and objectivity to review the sales department's compliance with laws and regulations, in light of the pressure to meet the department's sales targets. Subsection (b)(3) recommends that, if an internal-control officer were to have additional internal-control or operational responsibilities, organizational procedures should deal with any acceptable conflicts of interest (i.e., non-disabling ones) that may arise as a result of the officer's wearing two hats. Subsection (b) does not define the procedures but leaves organizations the freedom to design them to respond to their own particular circumstances. For example, the organization's compliance program might assign the chief legal officer to review the chief compliance officer's business transactions if the latter is also a business executive and report any problems to a specified senior executive. Another way for an organization to deal with a potential conflict of interest arising from an internal-control officer's multiple activities is to have an outside consultant review them and report its findings to executive management or the board of directors.

REPORTERS' NOTE

a. Authorities understand that an internal-control officer occupies a business-support role and is thus not part of an organization's primary operational or business functions. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 152 (2013) (referring to internal-control functions as "business enabling" functions and as the "second line of defense" for internal control); ETHICS RES. CTR., LEADING CORPORATE INTEGRITY: DEFINING THE ROLE OF THE CHIEF ETHICS & COMPLIANCE OFFICER (CECO) 19 (2007) ("Every additional responsibility jeopardizes a CECO's ability to remain focused and to perform effectively. In light of regulatory encouragement for an organization to demonstrate a strong commitment to ethics and compliance, additional risk is posed if the highest official dedicated to ethics is not even dedicated full-time."). It is also recognized that, as a result of the small size, limited operations or resources, or other circumstances of certain organizations, a person with business or operational responsibilities may have to serve as an internal-control officer, or an internal-control officer may have to perform multiple internal-control tasks. See INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO

19600 10 (2014) (paragraph 5.3.2, "Some organizations – depending on their size – also have someone who has overall responsibility for compliance management, although this may be in addition to other roles or functions, including existing committees, organizational unit(s), or [may] outsource elements to compliance experts."); U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. app. n.2.(C)(iii) 536-537 (2016) (noting how small organizations may have an effective compliance and ethics program by "using available personnel, rather than employing separate staff, to carry out the compliance and ethics program"); Office of Inspector Gen., Dep't of Health and Human Serv., Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8993 (Feb. 23, 1998) ("Every hospital should designate a compliance officer to serve as the focal point for compliance activities. This responsibility may be the individual's sole duty or added to other management responsibilities, depending upon the size and resources of the hospital and the complexity of the task."); Compliance Programs of Investment Companies and Investment Advisers, Advisers' Act Release No. 2204, 68 Fed. Reg. 74714, 74725 n.109 (Dec. 24, 2003) (stating SEC's awareness that small investment advisers need not hire a separate chief compliance officer). Organizations may have one internal-control officer perform several internal-control functions. See SOC'Y OF CORP. COMPLIANCE AND ETHICS & NYSE GOVERNANCE SERV., COMPLIANCE AND ETHICS PROGRAM ENVIRONMENT REPORT 9 (2014) (observing that 8% of firms surveyed have the chief legal officer also act as the chief compliance officer).

b. If an internal-control officer also has operational or business responsibilities, the practice among organizations is to adopt procedures in order to avoid, or to deal with, conflicts of interest arising from the officer's dual responsibilities. See generally SOC'Y OF CORP. COMPLIANCE AND ETHICS, CODE OF PROFESSIONAL ETHICS FOR COMPLIANCE AND ETHICS PROFESSIONALS, supra, at 7 (R2.7: "CEPs must disclose and ethically handle conflicts of interest and must remove significant conflicts whenever possible."). See, e.g., Compliance Programs of Investment Companies and Investment Advisers, Advisers' Act Release No. 2204, 68 Fed. Reg. 74714, 74722 (Dec. 24, 2003) (discussing how the requirement that a chief compliance officer report to a mutual fund's board of directors addresses possible conflicts arising from that officer's operational duties); FINRA Rule 3130.08 (2018), http://finra.complinet.com ("The requirement to designate one or more chief compliance officers does not preclude such persons from holding any other position within the member, including the position of chief executive officer, provided that such persons can discharge the duties of a chief compliance officer in light of his or her other additional responsibilities.").

§ 3.21. Outsourcing, Use of Technology, and Engagement of Third-Party Service Providers

(a) Because of its size, operations, or resources, or because of other circumstances and if permitted by law, an organization may outsource an internal-control function to a third party. The organizational actor who has direct responsibility for the internal-control

function that is being outsourced and who approves the outsourcing remains responsible for it.

(b) If permitted by law, an internal-control officer may use technology and engage professionals, consultants, or other third-party service providers to perform, or to assist in, the responsibilities of the internal-control function overseen by that officer, including evaluating the adequacy and effectiveness of the function.

(c) When subsection (b) applies:

(1) the internal-control officer remains responsible for the internal-control function; and

(2) policies and procedures should provide that the internal-control officer shall evaluate and regularly reassess the effectiveness of the technology and shall supervise the performance of any professional, consultant, or other third-party service provider to whom an internal-control responsibility has been delegated.

Comment:

a. Outsourcing. Subsection (a) provides that an organization may outsource an internal-control function because its size, operations, or resources, or other circumstances make it difficult to have that function provided "in house" or make it more efficient to have it done by an outside service provider. See also § 5.21 (the role of third-party service providers in the compliance function); § 6.22 (compliance consultants). Outsourcing is common today in small organizations, and regulators allow them to engage in it, particularly for the compliance and internal-audit functions. Large organizations may engage in this practice as well if, among other reasons, they find a third party to be an efficient, up-to-date provider of the internal-control services. As noted in the subsection, outsourcing may be limited or prohibited by law for certain organizations.

Subsection (a) also provides that the organizational actor who has authority over the internal-control function that is being outsourced and who makes the outsourcing decision should remain responsible for that outsourced function. Typically, this will be executive management, who will engage a third party to provide the internal-control function and supervise that party's performance of the internal-control responsibilities, just as it would an internal-control officer. See § 3.14(a) (executive management's directing the implementation of internal-control functions). It is expected that the board of directors, or one of its committees, will oversee this engagement in

accordance with the standards set out in § 3.08 (the board's oversight of the internal-control functions). This Principle does not address any liability arising from outsourcing. See also § 2.05.

b. Use of technology and consultants. Subsection (b) provides that an internal-control officer may use technology and engage professionals, consultants, or other third-party service providers to help in performing the responsibilities of the internal-control function. Again, as noted in the previous subsection, this use or engagement may be limited or prohibited by law for certain organizations or regarding specific internal-control responsibilities. It has become common, and indeed in some cases necessary, for internal-control officers to use different kinds of technology in their work. Indeed, automated technology and artificial intelligence are making significant inroads into compliance and risk management, particularly as to surveillance and monitoring, see § 4.12 and Comments *a-d* (risk-management monitoring); § 5.09 (compliance monitoring) and Comment *b* (discussing how technology is used in this monitoring). Similarly, it is usual for internal-control officers to draw upon the expertise of professionals, consultants, and other third-party service providers either to advise on or even to perform internal-control tasks or to conduct an evaluation or audit of the effectiveness of the internal-control function. The kinds of assistance offered by a third party are sometimes linked, as when an outside consultant installs technology that will perform an internal-control task, instructs the internal-control officer on its use, and then regularly consults on its operation and effectiveness. Because the organization and the internal-control officer may find it more efficient (and less costly) to outsource certain internal-control responsibilities or tasks, they should have the authority to do so. In addition, subsection (b) acknowledges that third parties are often asked to review the operation of an internal-control function, for example in anticipation of a regulator's examination of it, and to make suggestions for its improvement.

c. Ongoing responsibility of internal-control officer for technology and supervision of third-party service provider. Subsection (c) provides two necessary corollaries to an internal-control officer's use of technology and engagement of a third-party service provider. First and not surprisingly, under subsection (c)(1), the internal-control officer remains responsible for the internal-control function in these circumstances. Second, under subsection (c)(2), there should be in place policies and procedures for evaluation of the use of technology and supervision of the engagement of third-party service providers. Executive management, with the assistance of internal-control officers and with the approval of the board of directors, would direct the

implementation of these policies and procedures, which should ensure that the internal-control officer has the resources and the capacity to conduct the evaluation and supervision.

Regarding the use of technology, the policies and procedures should provide for an internal-control officer's evaluation and regular assessment of the technology's effectiveness in the performance of or the assistance in the internal-control tasks. They might state that the internal-control officer would ask for the advice of the organization's chief information technology officer, or a technology consultant, when evaluating whether to use technology in an internal-control task, if the officer lacks the required expertise to make this evaluation. The policies and procedures may also require that the product be initially tested under the internal-control officer's supervision and then periodically retested to ensure that it is performing the internal-control task in accordance with expectations and legal requirements. For example, a chief compliance officer may wish to use surveillance technology to review transactions for possible violations of the compliance program and the code of ethics. With the assistance of the organization's chief technology officer, the chief compliance officer would evaluate and test the technology to see whether it comprehensively reviews all transactions and has the capacity to identify those that are problematic and that require further evaluation. If the organization purchases or leases the technology, the officer would be expected, again, if necessary, with the help of an information technology officer or other knowledgeable party, to test the technology periodically to make sure that it is not missing transactions from its coverage or otherwise not performing as planned.

Regarding the internal-control officer's engagement of a third-party service provider to perform an internal-control task, the policies and procedures should provide for the officer's necessary and regular supervision of the provider in its performance. The degree and nature of the supervision will depend upon the facts and circumstances of the delegation and the task(s) being delegated. For example, if the chief risk officer were to engage a consultant to assess the effectiveness of the organization's risk-management program, procedures would have to deal with, among other things, safeguarding the information provided to the consultant and evaluating the consultant's background and assumptions. If the internal-control officer does not have the expertise to conduct this supervision, the officer should delegate this duty to another organizational actor. At the very least, the internal-control officer, or other organizational actor conducting the supervision, should verify at the outset of the engagement that the third-party service provider has the necessary time, resources, and capacity to perform the engagement expeditiously. The

following example demonstrates the responsibility of an internal-control officer who uses a third party for an internal-control task:

> Chief audit officer engages outside vendor to assist in the internal audit of Company's electronic data processing. The vendor recommends and performs all the internal-audit-testing procedures for the control of the data processing, but the chief audit officer must approve this part of the internal audit and the testing procedures. The chief audit officer is also responsible for the results of this outsourced internal-audit work, although the vendor may assist the officer when the results are reported to the Company's audit committee.

REPORTERS' NOTE

a. Organizations of limited size, operations, and resources may outsource to a third party one or more of their internal-control functions. When internal-control functions are required by law or regulation, regulators permit such outsourcing in certain cases. See, e.g., SEC OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, NATIONAL EXAM PROGRAM RISK ALERT: EXAMINATIONS OF ADVISERS AND FUNDS THAT OUTSOURCE THEIR CHIEF COMPLIANCE OFFICERS 1 (2015) (discussing the trend of smaller investment advisers and funds to outsource chief-compliance-officer responsibilities). See also COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES 153 (2013) ("At smaller organizations, legal and compliance roles may be shared by the same professional, or one of these roles can be outsourced with close oversight by management."); see id. at 130, 154 (referring to outsourcing of the internal-audit function); INT'L STANDARD, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, ISO 19600 10 (2014) (paragraph 5.3.2, "Some organizations – depending on their size – also have someone who has overall responsibility for compliance management, although this may be in addition to other roles or functions, including existing committees, organizational unit(s), or [may] outsource elements to compliance experts."). See generally Miriam H. Baer, *Governing Corporate Compliance,* 50 B.C. L. REV. 949, 993-999 (2009) (discussing the "compliance industry" of compliance consultants). It is equally understood that, if an internal-control function is outsourced, the organization remains responsible for it, particularly if the function is required by law or regulation. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 147 ("When outsourced service providers perform controls on behalf of the entity, management retains responsibility for those controls.").

There are advantages to the use of third parties for outsourcing an internal-control function because they can bring an expertise and experience that an organization might not have, or readily find, through an internal hire. This use also allows the organization to obtain an internal-control function based upon industry standards. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. app. n.2. (C)(iii) 5037 (2016) (observing that a small organization, with few resources, may achieve an effective compliance and ethics program by "(IV) modeling its own compliance and

ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations."). There are also disadvantages to using an outsider, such as that the third party will not understand the organization, will not have sufficient authority in it, and will apply a standardized approach to the internal-control function without tailoring it to the organization's needs and affairs. See SEC OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, NATIONAL EXAM PROGRAM RISK ALERT: EXAMINATIONS OF ADVISERS AND FUNDS THAT OUTSOURCE THEIR CHIEF COMPLIANCE OFFICERS, supra, at 4-6 (pointing out these drawbacks).

b. Outsourcing an entire internal-control function should be distinguished from outsourcing a specific internal-control responsibility or task, or asking a third party, or using technology, to provide advice or assistance to an internal-control officer on one or more internal-control tasks. Such delegation and use have become widespread, even in large organizations. See COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL – INTEGRATED FRAMEWORK: FRAMEWORK AND APPENDICES, supra, at 155 (discussing outsourcing in general). See also DELOITTE & COMPLIANCE WEEK, IN FOCUS: 2015 COMPLIANCE TRENDS SURVEY 11 (2015) (noting that only 24% of survey respondents do not outsource any part of compliance); id. at 13 (listing compliance tasks where compliance officers report using technology); PWC, STATE OF COMPLIANCE SURVEY: MOVING BEYOND THE BASELINE: LEVERAGING THE COMPLIANCE FUNCTION TO GAIN A COMPETITIVE EDGE 20 (2015) (reporting on the growing outsourcing of compliance tasks but noting that only 21% of CCOs use a dedicated governance, risk, and compliance technological tool). Firms are under increasing cost pressure to automate their internal-control functions. See MCKINSEY, TWO ROUTES TO DIGITAL SUCCESS IN CAPITAL MARKETS 18, 20-21 (W.P. No. 10 on Corp. & Inv. Banking, Oct. 2015) (discussing these pressures); KPMG, KEEPING UP WITH SHIFTING COMPLIANCE GOALPOSTS IN 2018: FIVE FOCAL AREAS FOR INVESTMENT 6-10 (2017) (discussing ways in which the compliance function can use technology in the automation of compliance tasks and the benefits of this usage). Vendors have responded to this need by offering to organizations outsourced and technologically-driven internal-control products and services. See, e.g., PWC, ENABLING PERFORMANCE THROUGH ADVANCED MONITORING AND TESTING ACTIVITIES: AN OUTSOURCED MONITORING AND TESTING SOLUTION (April 2015) (offering an offsite data-analytics tool covering such matters as regulatory-compliance testing, third-party risk management, and internal control over financial reporting). Whether or not outsourced, use of technology in internal control, even if such use is widespread, raises a number of supervisory issues. See, e.g., FINRA, REPORT ON CYBERSECURITY PRACTICES (Feb. 2015) (reporting on practices that firms use to protect their technology from cyberattacks).

c. If an internal-control responsibility or task, as opposed to the entire internal-control function, is outsourced, the expectation is that the head of that internal-control function will oversee it. See, e.g., BASEL COMM. ON BANKING SUPERVISION, BCBS NO. 113, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS 15 (2005) (Principle 10: "Compliance should be regarded as a core risk management activity within the bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.").

The supervision of the third party in the performance of its delegated internal-control tasks is similar to what the firm and the responsible internal-control officer should do for any outsourced activity. See generally BASEL COMM. ON BANKING SUPERVISION, THE JOINT FORUM: OUTSOURCING IN FINANCIAL SERVICES (2005) (setting forth principles of outsourcing, including adopting an outsourcing policy). See also FIN. EXECUTIVES RESEARCH FOUND., INSIGHT ON OUTSOURCED SERVICE PROVIDERS (2015) (providing step-by-step guidance with respect to the use and supervision of outside service providers).

CHAPTER 5

COMPLIANCE

TOPIC 1

THE COMPLIANCE FUNCTION

§ 5.01. Nature of the Compliance Function

The compliance function is the set of operations, offices, personnel, and activities within the organization that carry out its compliance responsibilities.

Comment:

a. The compliance function is an important control activity within an organization. Together with risk management, it constitutes the "second line of defense" against activities that violate internal or external norms. Depending on the nature of the organization, the compliance function can include a variety of rules, principles, controls, authorities, and practices designed to ensure that the organization conforms to external and internal norms. In many complex organizations, the compliance function is assigned to a specialized compliance department headed by an officer with a title such as "chief compliance officer."

REPORTERS' NOTE

a. In general. For general discussions of the compliance function, see, e.g., Miriam Hechler Baer, *Governing Corporate Compliance*, 50 B.C. L. REV. 949 (2009); John Braithwaite, *Enforced Self-Regulation: A New Strategy for Corporate Crime Control*, 80 MICH. L. REV. 1466 (1982); Geoffrey P. Miller, Compliance in Corporate Law, in Jeffrey Gordon & Georg Ringe eds., Oxford Handbook of Corporate Law and Governance (Oxford U. Press, forthcoming); GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE 137-138 (Wolters Kluwer 2014); SHARON ODED, CORPORATE COMPLIANCE: NEW APPROACHES TO REGULATORY ENFORCEMENT (EDWARD ELGAR 2013); JEFFREY M. KAPLAN, JOSEPH E. MURPHY & WINTHROP M. SWENSON, COMPLIANCE PROGRAMS AND THE CORPORATE SENTENCING GUIDELINES (THOMSON/WEST 2007). For a supervisory perspective, see BASEL COMMITTEE ON BANKING SUPERVISION, CONSULTATIVE DOCUMENT, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS, http://www.bis.org/publ/bcbs113.pdf (describing the principles that should underpin a bank's compliance function).

§ 5.02. Goals of the Compliance Function

Goals of the compliance function include the following:

(a) providing input on the effective strategic management of the organization;

(b) deterring misconduct by employees, agents, or others whose actions can be attributed to the organization;

(c) enforcing the organization's code of ethics;

(d) investigating and identifying violations of the law;

(e) establishing and maintaining a culture of ethics and compliance within the organization; and

(f) lowering the organization's expenses by preventing legal violations in a cost-effective manner.

Comment:

a. In addition to its role in preventing violations, the compliance function should play a strategic, advisory and consultative role in organizational decisionmaking. When an organization is considering important questions regarding its future, it is often well advised to give the chief compliance officer a voice in the decisionmaking process. Depending on the facts and circumstances, it may be appropriate for a compliance officer to be involved in a wide range of strategic decisions. This officer will ensure that any business or other decisionmaking will be in accordance with the organization's compliance program and procedures and its code of ethics. Compliance should thus be integrated into institutional design so that compliance officers can offer their advice early on in the decision-making process and help the organization avoid problems further down the line.

b. Although analyses of the compliance function often focus on instances of violations that are caught and sanctioned, compliance has an even more important role in preventing violations from occurring. Employees and agents face temptations to engage in impermissible activities. If they believe that they can engage in these activities with impunity, the level of violations will be higher than if they understand that they face a serious risk of adverse consequences. If employees are deterred from committing violations in the first place, organizations will not be required to investigate or punish their conduct, will not have to face potential regulatory sanctions, and will not have to experience the financial costs and loss of reputation that can follow when violations

occur. Meanwhile, members of the public will not experience the costs of harmful conduct when violations do not occur.

At the same time, the focus on possible acts of employee misconduct does not suggest that organizations are rife with illegality or breaches of ethics. Violations are the exception in most companies rather than the norm. Many, perhaps most, organizations try to construct an environment in which employees share the organization's vision and see themselves as part of a team within an environment of mutual trust. Effective compliance demands vigilance, but does not demand that one adopt a jaundiced view of the morals or ethics of organizations or their employees in general. Part of the goal of the compliance function is to help people of integrity to understand the substantive, and sometimes nonintuitive, obligations of compliant conduct.

c. The compliance function is not exclusively concerned with legal norms. The organization may elect to impose other standards or norms of behavior on itself and its agents and employees. The document that embodies these extralegal norms and that describes the consequences of violating them is referred to herein as a "code of ethics." See § 1.01(g). To the degree that these extralegal norms and standards define permissible and impermissible activities within the organization, the compliance function may be responsible for investigating violations of these norms as well.

d. Although deterrence is a primary goal, the compliance function must also investigate violations, both because the violations themselves require remediation and because, if the organization did not investigate and punish violations, the goal of deterrence would be substantially undermined.

e. The compliance function is a key element in establishing and maintaining an organizational culture of ethics and compliance within an organization. An active, vigorous, and visible compliance function communicates to others in the organization not only that they risk sanctions if they commit violations, but also that the organization itself is committed to maintaining a culture of compliance.

f. The compliance function can promote profitability because compliant corporations conserve on legal fees, avoid paying fines, and reduce reputational risk. The compliance function should not limit an organization's ability to engage in profitmaking activities so long as the organization has reasonably concluded that such activities are permissible under the law, regulations, and codes of ethics.

REPORTERS' NOTE

a. *Culture of compliance*. For general commentary, see Michael D. Greenberg, *Corporate Culture and Ethical Leadership Under the Federal Sentencing Guidelines: What Should Boards, Management, and Policymakers Do Now?* (RAND Corporation 2012), http://www.rand.org/pubs/conf_proceedings/CF305.html; Scott Killingsworth, *Modeling the Message: Communicating Compliance Through Organizational Values and Culture*, 25 GEO. J. L. ETHICS 961 (2012).

Government leaders have spoken about the importance of organizational culture in promoting safe and ethical management. See William C. Dudley, Enhancing Financial Stability by Improving Culture in the Financial Services Industry, available at https://www.bis.org/review/r151111a.htm (Nov. 5, 2014); Brent Snyder, Deputy Assistant Attorney General, Antitrust Division, U.S. Department of Justice, Compliance Is a Culture, Not Just a Policy, Remarks as Prepared for the International Chamber of Commerce/United States Council of International Business Joint Antitrust Compliance Workshop (Sept. 9, 2014); Daniel Tarullo, Good Compliance, Not Mere Compliance, remarks at the Federal Reserve Bank of New York Conference, Reforming Culture and Behavior in the Financial Services Industry, Oct. 20, 2014; Thomas Baxter, Executive Vice President and General Counsel, Federal Reserve Bank of New York, Compliance – Some Thoughts About Reaching the Next Level (Feb. 9, 2015).

b. *Mechanisms for cultural change.* Most commentators agree that it is difficult to change an established organizational culture, in part because the assumptions and values on which the culture is based are taken for granted within the institution. See Jon R. Katzenbach, Ilona Steffen & Caroline Kronley, *Cultural Change that Sticks*, HARV. BUS. REV. (2012) ("it takes years to alter how people think, feel, and behave, and even then, the differences may not be meaningful"); John P. Kotter, *Leading Change: Why Transformation Efforts Fail*, HARV. BUS. REV. (2007).

Regulators may seek to influence cultural change within organizations. Regulatory efforts have the advantage that the regulator is unlikely to share the organization's ingrained attitudes and norms. But regulatory change efforts also face significant obstacles: agents of regulatory change may face resistance from within the organization, may lack the credentials to speak with authority to employees of the organization, or may fail to take into account the institution's unique history and values. Nevertheless, regulatory "nudges" for cultural change can have an impact, especially if repeated by a variety of government officials over an extended period. See generally Cass R. Sunstein & Richard Thaler, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

c. Self-regulation by the affected industry may have somewhat greater prospects for success. Members of a self-regulatory organization are likely to place greater confidence in the judgments of such an organization than in the dictates of a government regulator, and thus may be more inclined to allow the self-regulatory organization to guide the evolution of values. See generally Neil Guggenheim & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 LAW AND POLICY 363 (1997). Some industries have already implemented self-regulatory strategies that may affect organizational culture. See American Chemical Council, Responsible

Care Guiding Principles, https://responsiblecare.americanchemistry.com/Responsible-Care-Program-Elements/Guiding-Principles/PDF-Responsible-Care-Guiding-Principles.pdf; Nancy B. Kurland, *The Defense Industry Initiative: Ethics, Self-Regulation, and Accountability*, 12 J. BUS. ETHICS 137 (1993); Errol E. Meidinger, *"Private" Environmental Regulation, Human Rights, and Community*, 7 BUFFALO ENVTL. L.J. 123 (1999). Self-regulatory bodies, however, may also become means for entrenching noncompliant attitudes, may encourage firms to "free ride" on the work of collective enterprises, or may support an atmosphere of complacency on the part of organizations who believe that the compliance problems in the industry are being effectively managed when they are not. To counteract these risks, some have suggested employing self-regulation with government supervision of the regulators. Jodi Short &Michael Toffel, *Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment*, 55 ADMIN. SCI. Q. 361 (finding that the government should not abdicate its role as regulatory enforcer, and suggesting that self-regulation with government surveillance can enhance overall regulatory performance). In 2014, a number of banks active in the United Kingdom tried to improve ethical standards in the industry by forming an industry self-regulating body, the Banking Standards Review Council. See Richard Lambert, Banking Standards Review Proposals (May 19, 2014). In the United States, the Financial Industry Regulatory Authority (FINRA) serves as a unique form of self-regulator. See http://www.finra.org/industry/rules-and-guidance; Barbara Black, *Punishing Bad Brokers: Self-Regulation and FINRA Sanctions*, 8 BROOK. J. CORP. FIN. & COM. L. 23 (2013); Saule T. Omarova, *Rethinking the Future of Self-Regulation in the Financial Industry*, 35 BROOK. J. INT'L L. 666 (2010). Much of the potency of FINRA's supervision is a product of the SEC's endorsement and encouragement of its regulatory mandate. The FINRA model is an interesting compromise between an entirely self-regulatory body and a government regulator, and illustrates the viability of a public–private scheme. Some have criticized FINRA, however, on the ground that it lacks transparency or fails to engage in vigorous enough supervision. See, e.g., https://www.reuters.com/investigates/special-report/usa-finra-brokers/; http://www.investmentnews.com/article/20170902/FEATURE/170909996/finra-whos-watching-the-watchdog.

A behavioral-economic approach holds promise for identifying strategies that may influence culture in constructive ways. Behavioral-economic theory looks to the factors that actually motivate people to comply or not to comply with applicable norms—factors that may or may not align with an employee's or agent's economic self-interest. See Donald C. Langevoort, *Monitoring: The Behavioral Economics of Corporate Compliance with Law*, 2002 COLUM. BUS. L. REV. 71 (2002); Donald Langevoort, *Chasing the Greased Pig Down Wall Street: A Gatekeeper's Guide to the Psychology, Culture, and Ethics of Financial Risk Taking*, 96 CORNELL L. REV. 1209 (2011). On behavioral approaches generally, see Cass R. Sunstein ed., Behavioral Law and Economics (Cambridge, Mass.: Cambridge Univ. Press 2000). For an interesting real-world example, see https://www.bryancave.com/images/content/8/9/v2/89927/2017-01-jan-feb-ethikos-killingsworth.pdf (recommending that answers to employee certifications will be more honest if the responder's signature is at the top of the form rather than at the bottom).

d. *Organizational culture.* The concept of organizational culture, while nearly universally acknowledged to be significant, is notoriously difficult to define. As Federal Reserve Governor Daniel Tarullo aptly put the matter: "culture is a somewhat contested academic concept and, however defined, is difficult to observe and assess from the outside." Daniel Tarullo, Good Compliance, Not Mere Compliance, remarks at the Federal Reserve Bank of New York Conference, Reforming Culture and Behavior in the Financial Services Industry, Oct. 20, 2014.

Roughly speaking, organizational culture could be said to consist of shared values and understandings that foster norms and shape behavior. See EDGAR H. SCHEIN, ORGANIZATIONAL CULTURE AND LEADERSHIP (5th ed. 2016); George G. Gordon, *Industry Determinants of Organizational Culture*, 16 ACAD. MGMT. REV. 396, 396-397 (1991). Culture in this sense may be specific to an organization, but may also reflect industry norms. See Margaret E. Phillips, *Industry Mindsets: Exploring the Cultures of Two Macro-Organizational Settings*, 5 ORG. SCI. 384, 384-385 (1994).

Biggerstaff, Cicero, and Puckett attempt to measure whether culture matters to an organization's propensity to commit violations. These authors found that firms whose chief executive officers had personally benefited from backdated options were more likely to engage in other corporate misbehaviors such as financial fraud. The authors take this as evidence that culture does matter, and that firms with a suspect ethical culture are more likely than other firms to engage in compliance violations. Lee Biggerstaff, David C. Cicero & Andy Puckett, *Suspect CEOs, Unethical Culture, and Corporate Misbehavior*, 117 J. FIN. ECON. 98 (2015).

§ 5.03. General Compliance Activities of Organizations

An organization should do the following with respect to compliance:

(a) undertake reasonable measures to ensure that employees and agents comply with the requirements of the law and applicable norms when acting on behalf of the organization;

(b) conduct appropriate investigations when made aware of credible evidence of significant violations of law or of the organization's compliance policy or code of ethics;

(c) undertake reasonable remedial measures to correct identified violations;

(d) be honest and candid towards regulators, prosecutors, and other responsible government officials, both in required reporting and in discretionary communications; and

(e) preserve books, records, and other information pertinent to potential legal violations, except pursuant to general, previously announced, legally authorized, and consistently performed document disposal and retention policies.

Comment:

a. An organization acts only through human beings. Pursuant to the principle of respondeat superior, violations of internal or external norms by an organization's employees or agents may be attributed to the organization. Even when misconduct by employees or agents is not legally attributed to an organization, it can nevertheless create significant reputational harm. Accordingly, organizations should undertake reasonable measures to ensure that employees conform to the requirements of law and the organization's compliance policies and procedures and code of ethics, as well as other applicable norms, when acting on behalf of the organization. Whether or not a compliance measure is appropriate depends on the facts and circumstances at hand: for example, measures that may be required to ensure compliance in large firms may not be needed in smaller ones. In all cases, however, the guiding principle is one of reasonableness: the organization should engage in compliance activities that are reasonable under the circumstances.

b. When confronted with credible evidence of a significant compliance violation, the organization should not look the other way or remain willfully ignorant of the facts. Instead, it should investigate further to see whether a violation has in fact occurred and, if so, the extent of its scope and effect. However, the desirability of performing such an investigation is limited by several considerations. If the evidence of misconduct brought to the organization's attention is not credible, there is no sound basis for the organization to inquire further. Moreover, any investigation that occurs is inevitably a function of the facts and circumstances, including the significance of the potential offense. Trivial violations may not require further inquiry, but significant matters should receive attention commensurate with their implications for the organization. Accordingly, any investigation that the organization performs should be reasonable in its scope and intensity.

c. If the organization has knowledge that a significant compliance violation has occurred, it should undertake remedial measures. The nature and extent of these measures is a function of the facts and circumstances. Such measures include penalizing the employee or employees responsible for the offense, changing procedures for internal controls, enhancing employee training programs, modifying governance arrangements, notifying regulators or third parties

whose interests may have been harmed, or any other response deemed to be appropriate under the circumstances.

d. Organizations are often subject to legal requirements to report information to regulators. Organizations should fulfill these obligations fully and fairly and not seek to disguise or mislead government officials. The organization should behave towards regulators with honesty and candor; deceiving a regulator may itself violate the law. Moreover, honesty and candor towards regulators makes good business sense. Regulators who perceive that an organization under their supervision is withholding information or acting deceitfully are likely to impose more burdensome regulatory requirements and more onerous penalties for violations than they would if they trusted that the organization is cooperative and forthcoming.

On the other hand, organizations are not obligated to volunteer information when not required to do so by law. Nor, unless required to do so by law, is an organization required to assist the regulator in performing the regulator's responsibilities.

Even when not required to do so, an organization may decide that it will cooperate with regulatory supervision or investigations. Such cooperation may build trust with the regulators, reduce the risk or intensity of regulatory sanctions for violations if they occur, contribute to fostering a culture of compliance within the organization, and enhance the organization's public image. In deciding on whether to cooperate, the organization may take into account the potential risks, including the fact that cooperation may hinder its ability to use legally permissible means to defend itself if accused of a violation.

e. In carrying out the compliance function, an organization should, to the extent feasible, maintain books, records, and other information pertinent to potential legal violations. These records are important resources because it is only through an examination of these materials that the organization and its regulators can investigate what actually happened. Disposing of books and records with the purpose of concealing compliance violations both undermines the compliance function and, in some circumstances, may constitute independent violations of the law. It may be appropriate for an organization to dispose of compliance-related books and records when such books and records may legally be discarded and are no longer useful, and when doing so is not for the purpose of concealing a violation but is done pursuant to a general, previously announced, and consistently performed policy of document disposal and retention. In this regard, the growing importance of information technology hardware seems to call for more standardized procedures

for decommissioning and disposing of old hardware as part of a comprehensive data-security protocol; failure to do so thoroughly could also result in a security breach. See https://www.protondata.com/blog/data-security/looking-data-destruction-lens-security-best-practices.

§ 5.04. Enterprise Compliance

Subject to § 2.03, the compliance function should be supervised or managed on an enterprise-wide basis.

Comment:

a. It is often desirable for the organization to direct the compliance function on an enterprise-wide basis rather than through a "silo" structure. In this way, accountability and escalation flow to a central authority. Enterprise compliance ensures that problems do not "fall through the cracks" of oversight and provides protection against inadvertent violations of laws of jurisdictions with which the compliance officer responsible for a particular division or function may be unfamiliar. Enterprise compliance also facilitates the development of a culture of compliance within the organization and allows for more effective communication of a healthy tone at the top. Enterprise compliance, moreover, takes account of the fact that it is generally the organization as a whole that will suffer a loss of reputation if any of its constituent parts engages in significant compliance violations.

As set forth in § 2.03, however, these Principles are subject to modification in light of the facts and circumstances. Different organizations appropriately structure their compliance functions in different ways. Accordingly, it may sometimes be appropriate for the organization to distribute the management of the compliance function to separate business units with only minor centralized oversight. See http://deloitte.wsj.com/riskandcompliance/2013/06/04/enterprise-compliance-answers-to-five-common-questions/ (discussing the pros and cons of different kinds of enterprise compliance—centralized, decentralized, and "hybrid.") For example, large and complex organizations will unavoidably have many compliance responsibilities and utilize many different approaches to fulfilling those responsibilities. It would not be unusual, for example, for a large company to have several dozen compliance activities, each addressing compliance with a specific category of legal requirement. Each of these could be seen as a separate compliance program

focusing on a specific area of legal and regulatory risk. While each of these risk-specific compliance activities often should be brought under a single enterprise umbrella, one should not underestimate the challenge of knitting together their management and supervision into a unitary, enterprise-wide, overall compliance operation. Silos, in other words, may be unavoidable, even though a company may do its best to centralize the compliance task. One approach worthy of consideration in cases such as these is to maintain the distributed compliance function but to create a small, central, enterprise-wide activity to audit its effectiveness.

REPORTERS' NOTE

a. *International comparison.* The European Banking Authority's Guidelines on Internal Governance encourages banks to institute robust compliance functions, headed by "a person responsible for this function across the entire institution and group (the Compliance Officer or Head of Compliance)." "EBA Guidelines on Internal Governance (GL 44)," Sept. 2011, https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance.

b. *Official guidance.* The value of enterprise compliance is stressed in Federal Reserve Board, Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles, SR 08-8/CA 08-11 (Oct. 16, 2008) and in Item 6(A) of the U.S. Sentencing Guidelines. As far back as 2006, enterprise-wide compliance risk management has been promoted as an effective compliance structure, especially within the realm of BSA/AML compliance. See Federal Reserve Board, At the Fiduciary and Investment Risk Management Association's Twentieth Anniversary Training Conference, Washington, D.C. (April 10, 2006) (speech by Governor Mark W. Olson), https://www.federalreserve.gov/newsevents/speech/olson20060410a.htm.

c. *Organizational adoption.* Many organizations have centralized their compliance function on an enterprise basis—sometimes voluntarily, and sometimes in response to regulatory pressure. See, e.g., United States v. HSBC Bank N.A. and HSBC Holdings PLC, Deferred Prosecution Agreement, No. 12-CR-763 (E.D.N.Y. July 1, 2013) (discussing HSBC's steps to enhance the effectiveness of its compliance function by giving the head of group compliance direct oversight over every compliance officer).

TOPIC 2

EFFECTIVE COMPLIANCE

§ 5.05. Elements of an Effective Compliance Function

Elements of an effective compliance function include:

(a) a compliance program;

(b) support and oversight from the organization's board of directors;

(c) effective management;

(d) adequate funding, staffing, and other resources;

(e) incentives for compliant behavior; and

(f) procedures for independent validation.

Comment:

a. This Section outlines elements that an organization should include in order to ensure that its compliance function is real and substantial and not a "Potemkin Village" that presents the appearance, but not the reality, of effective operation. This Section identifies a number of features found in authoritative descriptions of effective compliance programs. It also reflects standard practices for compliance programs in a variety of industries. Together with authoritative statements by regulators charged with enforcing particular bodies of law, industry practice is an important source of information about the elements of an effective compliance program.

One important element of an effective compliance function is a compliance program: a set of rules, procedures, authorities, standards, and requirements that implement the compliance policy within an organization. A compliance program is the concrete expression of the values and basic commitments contained in the compliance policy. The compliance program is governed by a set of written rules and standards. An organization may combine these rules and standards in a single document along with its compliance policy, or it may distribute the relevant rules and standards among a number of publications. These documents may be combined with the organization's code of ethics, if the organization chooses to promulgate one.

b. Support from the organization's board of directors and executive management is thus an essential component of an effective compliance program. By setting a "tone at the top," the leadership of an organization creates an expectation that all persons associated with the organization should behave in a legal and ethical manner. Support from the top is especially important in organizations where employees and agents might otherwise view the compliance

function with a degree of suspicion, borne of the fact that the compliance officer checks on their activities and reports evidence of misconduct, or a belief that compliance is an impediment to efficient operations. An organization's leaders should counteract such an attitude, if it exists.

c. It is important that executive responsibility for compliance be clearly assigned. A well-functioning compliance program should generally be headed by a senior officer who has responsibility for its functioning and success. For large organizations, the chief compliance officer should devote essentially all of his or her time to the compliance function and should be assisted by a staff of sufficient size with access to resources adequate for the job. For smaller organizations, the chief compliance officer may also perform other functions. It is not necessary that the person have the title "chief compliance officer" so long as his or her responsibilities and activities are consistent with the role.

d. The compliance function requires sufficient funding and other resources if it is to carry out its responsibilities in an effective manner. Among other things, the compliance function should employ the technology necessary to detect noncompliance, including, as appropriate, supervisory programs specifically designed to address the risks inherent in algorithmic and similar investment techniques.

e. The compliance function cannot succeed unless employees are incentivized to comply. Accordingly, appropriate discipline for violations is an important part of any compliance function. Moreover, both compliant and noncompliant conduct should be taken into account when designing incentive compensation systems. Accordingly, an organization may decide to award bonuses or other financial rewards to employees who display conspicuously good behavior with respect to compliance.

Nonmonetary incentives may also be important. Employees who are given nonfinancial recognition for conspicuously compliant behavior—such as awards, rights to participate in company events, recognition in company newsletters or other publications, or praise from company leaders—may respond as strongly as they would to financial inducements. The celebration of ethical conduct with "buy-ins" from employees and agents at all levels of the organization can be a key to achieving a culture of compliance and ethics within an organization. By the same token, nonmonetary penalties may be equally as effective as financial sanctions in a given case of conspicuously noncompliant behavior. Examples include termination, demotion,

suspension, reassignment, probation, warnings, censures, and reporting of an individual's conduct to law-enforcement authorities.

f. The compliance function works best if it is subject to independent validation and review. Such validation and review work to ensure that the compliance function retains an appropriate degree of independence from the business lines of the organization, including its senior operating officials. An independent validation process also helps to ensure that the compliance function is well-designed and performing as intended. The independent validation and review can be undertaken by the organization's internal-audit department, by an outside consultant, or by any other party who possesses the requisite expertise, access, and independence.

REPORTERS' NOTE

a. *Assignment of responsibility.* See Remarks by Leslie R. Caldwell, Assistant Attorney General for the Criminal Division (Oct. 1, 2014) ("A company should assign responsibility to senior executives for the implementation and oversight of the compliance program.").

b. *Behavioral compliance.* Behavioral compliance—the design and management of compliance strategies drawing on cognitive and psychological research—is an important analytic method and a potentially valuable addition to the organization's menu of strategies for performing the compliance function. A leading contribution to the literature on this topic is Donald C. Langevoort, *Monitoring: The Behavioral Economics of Corporate Compliance with Law*, 2002 COLUM. BUS. L. REV. 71 (2002). See also Donald C. Langevoort, *Behavioral Ethics, Behavioral Compliance,* in Jennifer Arlen, ed., Research Handbook on Corporate Crime and Financial Misdealing (Edward Elgar, 2018) (forthcoming)

c. *Elements of effective compliance functions.* For general treatments, see, e.g., Biegelman & Biegelman, Building a World-Class Compliance Program (John Wiley & Sons, Inc. 2008); Kaplan & Murphy, Compliance Programs and the Corporate Sentencing Guidelines: Preventing Criminal and Civil Liability, 2017-2018 Edition (Thomson Reuters, 2017); Corporate Executive Board, Charting a New Course: Measuring and Monitoring the Effectiveness of Compliance and Ethics Programs (New York: Compliance and Ethics Leadership Council 2006). For an economic approach, see Geoffrey P. Miller, *An Economic Analysis of Effective Compliance Programs*, in Jennifer Arlen ed., Research Handbook on Corporate Crime and Financial Misdealing (Edward Elgar 2018) (forthcoming).

d. *Incentives for compliant behavior.* The value of incentives for compliant behavior is recognized in the U. S. Sentencing Guidelines. Item 6(A) of the Guidelines states that "[t]he organization's compliance and ethics program shall [include] appropriate incentives to perform in accordance with the compliance and ethics program."

e. *Industry practice.* The Commentary to the U. S. Sentencing Guidelines recognizes that industry practice is a factor for consideration and provides that "[a]n organization's failure to

incorporate and follow applicable industry practice . . . weighs against a finding of an effective compliance and ethics program." U. S. SENTENCING GUIDELINES MANUAL § 8B2.1 (U.S SENTENCING COMM'N 2016),

f. International approaches. Elements of effective compliance programs are set forth in a number of international publications.

The Organization for Economic Cooperation and Development's Good Practice Guidance includes the following elements of an effective anti-bribery program: (1) strong, explicit, and visible support for, and commitment from senior management to, the company's internal controls, ethics, and compliance program; (2) a clearly articulated and visible corporate policy prohibiting foreign bribery; (3) an understanding that compliance is the duty of individuals at all levels of the company; (4) oversight of ethics and compliance programs; (5) ethics and compliance programs or measures designed to prevent and detect foreign bribery, applicable to all directors, officers, and employees, and applicable to all entities over which a company has effective control; (6) ethics and compliance programs or measures for business partners designed to prevent and detect foreign bribery; (7) a system of financial and accounting procedures, including a system of internal controls, reasonably designed to ensure the maintenance of fair and accurate books, records, and accounts; (8) measures designed to ensure periodic communication and documented training for all levels of the company; (9) appropriate measures to encourage and provide positive support for the observance of ethics and compliance programs or measures against foreign bribery at all levels of the company; (10) appropriate disciplinary procedures; (11) effective measures for providing guidance and advice on complying with the company's ethics and compliance program, internal confidential reporting, and appropriate responsive action; and (12) periodic reviews of the ethics and compliance program. Organization for Economic Cooperation and Development's Good Practice Guidance on Internal Controls, Ethics, and Compliance (18 February 2010), http://www.oecd.org/daf/anti-bribery/44884389.pdf.

The United Kingdom Ministry of Justice guidance on the Bribery Act sets out six principles for an adequate procedures compliance program: ix Principles of an Adequate Procedures Compliance Program U.K. Ministry of Justice in relation to the U.K.'s Bribery Act 2010. Adequate procedures include: (1) proportionate procedures, (2) top-level commitment, (3) risk assessment, (4) due diligence, (5) communication, and (6) monitoring and review. See U.K. Ministry of Justice, The Bribery Act 2010: Guidance about procedures which relevant commercial organizations can put into place to prevent persons associated with them from bribing, pp. 20-31, http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

g. Measuring effectiveness. Attempts have been made to measure compliance-program effectiveness. A notable example is LRN Corporation's "Program Effectiveness Index." See LRN, 2018 Ethics and Compliance Program Effectiveness Report. As yet, however, there appears to be no generally accepted measure of program effectiveness independently validated by academic analysis.

h. "Paper" compliance functions. See, e.g., Kimberly D. Krawiec, *Cosmetic Compliance and the Failure of Negotiated Governance*, 81 WASH. U. L.Q. 487 (2003). Government agencies

recognize the danger of "Potemkin Village"-type programs. See, e.g., Information ¶ 39, United States v. Siemens Aktiengesellschaft, No. 1:08-CR-367 (D.D.C. Dec. 12, 2008), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2013/05/02/12-12-08siemensakt-info.pdf ("[w]hile foreign anti-corruption circulars and policies were promulgated, that 'paper program' was largely ineffective at changing SIEMENS' historical, pervasive corrupt business practices.").

i. Particular industries and subject matters. Information on effective compliance programs is found in many public and private publications addressed to particular industries and subject-matter areas, including, but by no means limited to, the following:

Anticorruption Law: Department of Justice Criminal Division and Securities and Exchange Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act Guidance on the government's expectations for an effective compliance program under the Foreign Corrupt Practices Act is found in United States v. Metcalf & Eddy, Inc., No. 99-cv-12566 (D. Mass. 1999).

Antitrust Law: J. Murphy & W. Kolasky, *The Role of Anti-Cartel Compliance Programs In Preventing Cartel Behavior*, 26 ANTITRUST 61 (2012); American Bar Association Section of Antitrust Law, Antitrust Compliance: Perspectives and Resources for Corporate Counselors (2010); Office of Fair Trading (UK), How Your Business Can Achieve Compliance with Competition Law 26 (June 2011); Competition Bureau Canada, Information Bulletin: Corporate Compliance Programs (2015), http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03927.html.

Banking Law: Basel Committee on Banking Supervision, Compliance and the Compliance Function in Banks, SR 08-8 (Oct. 16, 2008); Board of Governors of the Federal Reserve System, Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles (Oct. 16, 2008). The Dodd–Frank Act's Volcker Rule requires that covered financial institutions establish programs to assure compliance. For banking entities with total assets greater than $10 billion and less than $50 billion, the rule specifies six elements that each compliance program must include: (1) written policies and procedures; (2) a system of internal controls reasonably designed to monitor compliance; (3) a management framework that clearly delineates responsibility and accountability for compliance; (4) independent testing and auditing of the effectiveness of the compliance program; (5) training for trading personnel and managers, as well as other appropriate personnel, to effectively implement and enforce the compliance program; and (6) creating and keeping records sufficient to demonstrate compliance, which a banking entity must promptly provide to the relevant supervisory Agency upon request and retain for a period of no less than five years.

Criminal Enforcement: See Remarks by Leslie R. Caldwell, Assistant Attorney General for the Criminal Division (Oct. 1, 2014), http://www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-22nd-annual-ethics: ((1) high-level commitment to the compliance policy; (2) a written compliance code; (3) periodic risk-based review; (4) proper oversight and independence of the compliance program; (5) training and

guidance; (6) internal reporting; (7) investigation; (8) enforcement and discipline; (9) oversight of agents and business partners; and (10) monitoring and testing).

Criminal Sentencing: The U.S. Sentencing Commission's Guidelines set forth minimum requirements for an effective compliance program. The essential requirements are that the organization engage in due diligence to seek to prevent criminal conduct by employees and agents, and that the organization promote a culture that encourages ethical conduct and compliance with the law. Specific requirements include the following: (1) the corporation must establish standards and procedures to prevent and detect criminal conduct; (2) the corporation's board of directors must be knowledgeable about the compliance and ethics program and must exercise reasonable oversight with respect to implementation and effectiveness; (3) the corporation's senior personnel must ensure that the corporation has an effective compliance program and specific individuals must be assigned responsibility for it; (4) specific individuals must be assigned responsibility for implementing the compliance and ethics program; (5) the corporation must use reasonable efforts not to place in high-level executive positions individuals who have engaged in prior illegal conduct or other behaviors inconsistent with an effective compliance and ethics program; (6) the corporation must engage in effective compliance training programs and must distribute information about its compliance-related standards and procedures; and (7) the corporation must undertake reasonable steps to ensure that its compliance and ethics program is followed by the company's employees and agents. See U.S. SENTENCING GUIDELINES MANUAL (U.S. SENTENCING COMM'N 2016).

Employment Law: on sexual harassment, see EEOC, Promising Practices for Preventing Harassment, https://www.eeoc.gov/eeoc/publications/promising-practices.cfm?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term

Energy Law: Federal Energy Regulatory Commission, Policy Statement on Compliance, 125 FERC ¶ 61,058 (Oct. 16, 2008).

Environmental Law: Environmental Protection Agency, Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations, 65 Fed. Reg. 19,618 (Apr. 11, 2000); see also EPA's Interim Approach to Applying the Audit Policy to New Owners, https://www.epa.gov/compliance/epas-interim-approach-applying-audit-policy-new-owners.

Foreign Corrupt Practices: See In the Matter of Bruker Corporation, SEC Securities Act Release No. 73835 (Dec. 15, 2014). The proceeding involved Bruker Corp., a manufacturer of analytical tools and life science and materials research systems. When the parent company discovered that employees at the company's Chinese subsidiaries had been bribing Chinese government officials, it undertook a number of corrective actions that the SEC release describes as praiseworthy, including: (1) instituting preapproval processes for nonemployee travel and significant changes to contracts; (2) establishing a new internal-audit function and hiring a new director of internal audit who was charged with oversight of Bruker's global compliance program, including FCPA compliance; (3) adopting an amended FCPA policy translated into local languages; (4) implementing an enhanced FCPA training program, which included training programs in local languages as well as mandatory online employee training programs regarding

ethics and FCPA compliance; (5) enhancing due-diligence procedures for third parties; and (6) implementing a new global whistleblower hotline. The SEC also lauded the fact that the company had cooperated fully with the government once it discovered the misconduct.

Government Procurement Law: Federal Acquisition Regulations System 3.1002 (Contractor Code of Business Ethics and Conduct).

Health Law: Section 6401(a)(7) of the Patient Protection and Affordable Health Care Act of 2010 requires providers and suppliers enrolled in federal healthcare programs to create and maintain compliance programs. Section 6102 of the Act requires operators of skilled nursing facilities to implement a compliance and ethics program that is effective in preventing violations of the Act and promoting the quality of care. The Department of Health and Human Services promulgates compliance requirements for discrete industry sectors. See Department of Health and Human Services, Office of Inspector General, Compliance Program Guidance for Pharmaceutical Manufacturers, 68 Fed. Reg. 23731 (May 5, 2003); Department of Health and Human Services, Office of Inspector General, Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987 (Feb. 23, 1998); Department of Health and Human Services, Office of Inspector General, Compliance Program Guidance for Clinical Laboratories, 63 Fed. Reg. 45076 (Aug. 24, 1998); Department of Health and Human Services, Office of Inspector General, Compliance Program Guidance for Third-Party Medical Billing Companies, 63 Fed. Reg. 70138 (Dec. 18, 1998); Department of Health and Human Services, Office of Inspector General, Supplemental Compliance Program Guidance for Nursing Facilities, 73 Fed. Reg. 56832 (Sept. 30, 2008).

Money Laundering and Terror Finance: Financial Association Task Force, Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing for Legal Professionals (Oct. 23, 2008).

Securities Law: European Securities and Markets Authority, Guidelines on Certain Aspects of the MiFID Compliance Function Requirements (Final Rep.) (July 2012), https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-388_en.pdf; Securities Industry and Financial Markets Association, The Evolving Role of Compliance (Mar. 2013), http://www.sifma.org/issues/item.aspx?id=8589942363.

Trade Law: U.S. Department of Commerce, Bureau of Industry and Security, Office of Exporter Services, Export Management and Compliance Division, Compliance Guidelines: How to Develop an Effective Export Management and Compliance Program and Manual (Nov. 2013), https://www.bis.doc.gov/index.php/forms-documents/compliance-training/export-management-compliance/1256-emcp-guidelines-november-2013/file.

j. Tone at the top. The "tone at the top" is much discussed by government officials who are associated with compliance. For an example, see Stephen Cutler, Director, Division of Enforcement, SEC, *Tone at the Top: Getting It Right*, Second Annual General Counsel Roundtable (Dec. 3, 2004), http://www.sec.gov/news/speech/spch120304smc.htm.

§ 5.06. Compliance Program

The organization's compliance program should be reasonably designed to prevent and detect violations of internal and external laws and norms. It should:

(a) be governed by written rules and procedures approved by the board of directors;

(b) be informed by an assessment of risk to the organization;

(c) be based at least in part on underlying principles rather than standardized procedures;

(d) assign responsibility for compliance within the organization;

(e) be impartially and fairly administered;

(f) provide reliable and timely advice to employees regarding their compliance obligations;

(g) be effectively communicated to affected employees;

(h) include appropriate compliance training for employees, agents, and members of the board of directors;

(i) include procedures for internal reporting of violations;

(j) include procedures for monitoring employee conduct;

(k) include procedures for investigating violations;

(l) include procedures for disciplining violations;

(m) create appropriate incentives for compliant behavior and disincentives for violations;

(n) be regularly assessed for effectiveness and updated as necessary; and

(o) be periodically reviewed and reaffirmed by the organization's senior executives and board of directors.

Comment:

a. The compliance program should be governed by written documents that implement the principles and general statements contained in the compliance policy. These documents should set forth objective, specific, verifiable responsibilities and expectations. Because the compliance-program documentation sets forth specific rules, procedures, and standards that must be implemented by an organization's employees and agents at varying levels of seniority and responsibility, it should, when possible, be written in plain and simple language that is easily

understood by those charged with implementing its requirements. Documents written in complex "legalese" are likely to be both off-putting and ineffective. An organization may elect to combine its compliance policy with other compliance-related documents, such as the organization's code of ethics.

The operative elements of the compliance program should generally be embodied in writing (and in some industries, *must* be maintained in written form). Written policies and procedures can convey a sense of the importance of the topic being discussed, are easier to communicate within the organization, and protect against changes in meaning that could occur if the policy were conveyed by word of mouth. Even when compliance policies and procedures are reduced to printed form, an organization may still find it beneficial to communicate this information by other media, such as videos, Web-based communication strategies, or in-person communications.

b. The compliance program should be informed by an assessment of the organization's compliance risk. The risk assessment should examine the inherent risk of compliance violations, the controls that operate to reduce the risk, and the residual risk that remains given the presence of these controls. Activities that pose a low residual risk of compliance violations require fewer resources than activities that pose a high risk. The level of residual risk identified by the risk assessment should be consistent with the organization's risk-appetite statement. See § 4.07(d) for discussion of risk tolerance for compliance risk. Compliance risk assessments should be regularly revisited in order to ensure that the organization's compliance program remains responsive to an evolving risk landscape.

c. The compliance program should not consist solely of a series of "check-the-box" requirements that employees must fulfill. A purely "rules-based" compliance program creates a danger that employees, knowing the questions that will be asked, will learn how to engage in impermissible conduct that is not identified by the questions. Accordingly, while at some level "check-the-box" requirements are inherent in compliance, the program should also include an important "principles" component, under which program resources and program responses are informed by an awareness of the purposes that the compliance program is seeking to achieve.

d. One risk, given the complexity of an organization's compliance program, is the possibility that responsibilities will not be clearly allocated to individuals or offices within the organization. Without such a clear allocation, important compliance-based tasks may "fall through

the cracks" because they are seen as someone else's responsibility. Moreover, without a clear allocation of "ownership" of the function to a particular individual or office, the enhanced diligence that comes with a sense of personal accountability may be lost. Accordingly, the compliance program should clearly assign responsibility for compliance tasks within the organization, and more generally, should clearly inform employees and agents how to do their jobs in accordance with laws, regulations, and professional and ethical standards.

e. The compliance program should set forth rules applicable to everyone, and not just lower-level employees. Any bias or unfairness in the application of the program—or even the perception of bias or unfairness—undermines its moral force and its effectiveness. If employees see that compliance applies only to lower-level individuals and not to people in the upper echelons of an organization, they may infer that compliance does not really matter in the organization at all. Moreover, regulators are unlikely to give full credit to a compliance program that does not operate equally across the board. Accordingly, it is essential that the program be impartially and fairly applied to everyone, including the board of directors, the chief executive officer, and other senior figures in the organization. Moreover, as set forth in § 3.16, the officer charged with administering the compliance program should be given a degree of independence sufficient to protect him or her against the possibility or perception of undue influence or partiality.

f. Compliance programs do not only exist to monitor employees in order to detect misconduct and encourage employees to behave in a compliant fashion. They also act as repositories of information and sources of advice on compliant behavior for employees. Often employees are motivated to "do the right thing" but do not know what the right thing is under the circumstances confronting them at the time. Compliance programs should fill that gap by providing readily available procedures for obtaining advice—on a confidential basis if appropriate—to employees on appropriate conduct. If the advice turns out to have been mistaken, employees who in good faith rely on it should be protected against internal sanctions.

g. A compliance program accomplishes little if it is filed and forgotten. The relevant elements of the program must be communicated both to those charged with implementing the internal controls and also to employees and agents whose conduct creates a compliance risk for the organization. Moreover, this communication process must be effective. Communications that convey a signal of importance are more likely to be heard than ones suggesting the opposite. A mass e-mail sent to all employees might be deleted and have no influence on behavior, but an

individual e-mail directed to each employee by name is likely to have a greater impact. Oral or visual communications may be effective, especially if accompanied by written material. Communications that require some sort of feedback from the recipient are likely to be more effective than communications that can simply be ignored. Repeated communications are more effective than one-time messages, especially if there is variation in the media of the communication.

The media used to communicate the compliance program will necessarily be determined by the facts and circumstances of the organization. An in-person meeting with the chief compliance officer or chief executive officer might work for a small organization but could be infeasible for a large one. Institutions that are geographically dispersed will require different forms of communications than organizations operating out of a single office. The organization's governance structure may also make a difference: for an organization with a single dominant leader, communication from that individual may be important; for organizations with more distributed power structures, a subordinate official such as the head of a division may be a more effective spokesperson. For larger organizations, placing elements of the compliance program on the organization's website may be effective, as may the use of social media to communicate information.

Compliance policies and procedures should be provided to employees on a periodic basis. Some organizations distribute these documents once each year. The organization may also elect to distribute the compliance policies and procedures to agents and counterparties whose involvement with the company poses compliance risks. Larger companies may find it desirable to reproduce their compliance policies and procedures on their websites and make them available to the public. Creative compliance departments have gone further and used social media to publicize their compliance policies and other information pertinent to the compliance function.

h. Merely receiving the message may not be fully effective in embedding compliant behaviors. Ongoing training may also be required to ensure that the messages are received, understood, and, if possible, internalized by employees and agents. Considerations pertinent to the type of training an organization may wish to administer are outlined in § 5.10.

An important feature of training is its effect, if successful, in enlisting employee "buy-in" to the compliance function. People are more likely to conform to values and norms that are salient to them. Merely announcing compliance obligations from "on high" is likely to be less effective

than providing a means through which employees can experience the value of compliance in a lived way. In certain organizations, compliance may be enhanced if employees are required periodically to undertake some action that calls their attention to their compliance obligations. An example is a rule that key employees must certify in writing on an annual basis that they understand the compliance requirements applicable to them and that, to the best of their knowledge and belief, the functions under their authority are in compliance with applicable legal or ethical rules. Another strategy is to couch the relevant compliance requirements in language that speaks to employees' interests, identities, and values. Survey methodologies may also promote buy-in by encouraging employees to express their views on the compliance function in a way they know will be evaluated and reviewed by senior managers.

i. Internal-reporting procedures are important elements of an effective compliance program. Accordingly, the organization should provide safe and reliable mechanisms that employees can use to make internal reports. The organization should offer informants assurances of confidentiality and protections against retaliation. It should also adopt and publicly announce a policy prohibiting retaliation against informants. Internal reporting is part of a broader culture of compliance, and accordingly both contributes to a compliant culture and also benefits from such a culture, in the sense that employees are likely to feel safe coming forward if they work at a firm with a good culture of compliance.

j. An effective compliance program should include procedures for monitoring employee conduct. In many cases involving routine or repeated transactions, the organization may find it economical and effective to implement automated monitoring systems. Before implementing such a system, however, the organization should consider whether the system is effectively designed to take account of facts and circumstances pertinent to that organization, and it should periodically review the system's operation to ascertain whether it remains effective. Because no automated system can replace human judgment, organizations should be alert to the dangers of overreliance on such resources.

k. An effective compliance function includes procedures for investigating evidence of violations. Investigations face potential problems if they are not organized according to a prepared plan and design. The organization's leadership may overreact to evidence of a possible violation, or alternatively may fail to respond forcefully enough when red flags of misconduct are observed. The investigation may not be sufficient in the sense that important leads are ignored or ruled out

because they are deemed to be outside the scope of the inquiry. Investigators may not carry out tasks in a logical and effective order. For example, suspected wrongdoers may tamper with or destroy evidence before information can be retrieved, or the investigators may conduct interviews without having first obtained a sufficient understanding of the background facts. Investigators may become overzealous and act in ways that intrude on a suspect's privacy or undermine company morale. Accordingly, depending on the facts and circumstances of the organization, it may be desirable for an organization to establish procedures in advance for investigating violations. Such procedures should not prematurely commit the organization to any particular course of action but should provide a framework that the organization can call on when faced with the need for urgent decisions about matters that may affect the organization's reputation or financial position. For more on investigations, see §§ 5.24 through 5.31.

l. An effective compliance program must include procedures for disciplining employees who are found to have violated internal or external norms. The penalty for such misconduct should be administered impartially and should take account of the wrongfulness of the conduct and the harm the conduct creates.

m. An effective compliance program should include measures to incentivize employees to conform their conduct to governing norms. Such incentives include both threats of punishment for misconduct and promises of reward for conspicuously compliant conduct. Accordingly, an effective compliance program should, as appropriate, contain procedures and standards for disciplining employees. For large organizations, these procedures will often be formalized and reduced to writing. For smaller organizations, a less formal structure may be appropriate. In addition to the "stick" of discipline, an organization may seek to incentivize compliant behaviors by rewarding conspicuously good conduct. For example, the organization may elect to include compliance as a component of each employee's performance objectives and to base bonuses or other compensation on achievement of those objectives. Some critics challenge the concept of rewards for compliant behavior on the ground that people should not be paid for doing the right thing. This criticism is unwarranted. All forms of incentive-based compensation reward employees for doing well—whether the good performance takes the form of enhancing profits or observing the rules.

n. It is not sufficient merely to establish a compliance program. Even well-designed programs can fall into desuetude, be captured by powerful interests within the organization, or

become outmoded as a result of legal or organizational changes. Accordingly, it is essential that the compliance program be assessed for effectiveness, either periodically or on an ongoing basis.

The assessment of a program's effectiveness may be based on qualitative evaluations, quantitative metrics, or both. Quantitative metrics have the advantage of being relatively objective and subject to rigorous analysis and tracking over time. For example, the organization may keep statistics on employment-training completion rates, hotline usage, frequency and result of internal audits of the program, rates of completion of required reports, and so on. Quantitative metrics have inherent limitations, however: they are subject to being "gamed" by people who wish to manipulate the results; and the data points can easily be mistaken for the fundamental question of whether the program really is effective. Qualitative evaluations such as self-evaluations, focus-group discussions, exit interviews, and the like can be a useful supplement to the quantitative approach. Organizations may employ survey methods to obtain information from larger groups of employees. In appropriate cases, the review process could take the form of a special compliance audit involving business executives, compliance personnel, internal audit, and representatives from the legal department.

o. The compliance landscape is rapidly changing. New legal requirements replace old ones; new ethical standards are adopted. Regulatory priorities shift along with perceptions about risk as well as experience over time. Organizations develop new ways of communicating with employees or improve the quality of existing communication channels. Technological developments may enable the organization to engage in more effective compliance activities. The compliance policy must not become ossified. Periodic revisiting of the policy also has the potentially beneficial effect of reminding employees and agents on a regular basis of the importance that the organization gives to compliance issues.

p. The compliance program should be periodically reaffirmed by the board of directors in the organization and also by the organization's senior management. Reaffirmation of the program by the board of directors and senior management reinforces the "tone at the top" by signaling the importance the organization gives to the compliance function. Such reaffirmation also reminds senior managers and members of the organization's board of directors of the importance of the compliance function and may help them feel a personal responsibility for the process. It may also be advisable for the organization to require all of its employees and agents to reaffirm their agreement to the compliance program on a periodic basis.

REPORTERS' NOTE

a. An influential list of elements of an effective compliance program is found in the U.S. Sentencing Guidelines' requirements for an effective compliance and ethics program. See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (U.S. SENTENCING COMM'N 2016). In order to achieve favorable treatment under the Guidelines, an organization is required to establish standards and procedures to prevent and detect criminal conduct; its governing authority must be knowledgeable about the content and operation of the compliance and ethics program and exercise reasonable oversight with respect to the implementation and effectiveness of the program; specific high-level personnel must be assigned overall responsibility for the program; the organization must use reasonable efforts not to include within the personnel exercising substantial authority any individual whom the organization knows, or should know through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective program; the organization must take reasonable steps to communicate periodically and effectively its standards and procedures and other aspects of the compliance and ethics program to high-level personnel; the organization must take reasonable steps to ensure that the compliance and ethics program is followed, to evaluate the effectiveness of the program on a periodic basis, and to maintain a system for reporting or seeking guidance regarding potential or actual criminal conduct without fear of retaliation; must be promoted and enforced consistently throughout the organization; and, after criminal conduct is detected, must take reasonable steps to respond appropriately and to prevent further similar criminal conduct. The organization is further required to periodically assess the risk of criminal conduct and to take appropriate steps to design, implement, or modify the program in order to reduce the risk of criminal conduct. Section 5.06 is intended to be consistent with the requirements of the Sentencing Guidelines, but is not addressed to the issue of sentencing in federal criminal cases, and covers a range of misconduct other than criminal violations.

Principles of effective compliance programs are found in a variety of specific contexts. An example is the Report of the Co-Chairs of EEOC's Select Task Force on the Study of Harassment in the Workplace, which identifies five core principles that have generally proven effective in preventing and addressing workplace harassment: committed and engaged leadership; consistent and demonstrated accountability; strong and comprehensive harassment policies; trusted and accessible complaint procedures; and regular, interactive training tailored to the audience and the organization. See EEOC, Promising Practices for Preventing Harassment, https://www.eeoc.gov/eeoc/publications/promising-practices.cfm?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term.

b. *Achieving buy-in.* On strategies for achieving employee buy-in to compliance values, see Tom R. Tyler, et al., *The Ethical Commitment to Compliance: Building Value-Based Cultures*, 50 CAL. MGMT. REV. 31 (2008); Linda K. Treviño et al., *Managing Ethics and Legal Compliance: What Works and What Hurts*, 41 CAL. MGMT. REV. 131 (1999).

c. *Assessment and updating.* Rules applicable to investment companies, investment advisers, and broker-dealers require that the compliance program be reviewed annually for adequacy and effectiveness and updated as appropriate when problems are found. SEC Rule 38a-

1 (investment companies); SEC Rule 206(4)-7 (investment advisers); FINRA Rule 3120 and 3130
2 (broker-dealers).
3 *d. Company-wide focus.* The importance of impartial compliance programs that focus on
4 the executive management as well as lower-level employees is stressed in MICHAEL D.
5 GREENBERG, CULTURE, COMPLIANCE, AND THE C-SUITE: HOW EXECUTIVES, BOARDS, AND
6 POLICYMAKERS CAN BETTER SAFEGUARD AGAINST MISCONDUCT AT THE TOP (Rand 2013).
7 *e. Enlisting employee participation.* Creative compliance departments have experimented
8 with the use of media and devices for enlisting employee participation. Lockheed Martin, for
9 example, reportedly staged a contest in which employees were invited to produce their own short
10 videos promoting ethical workplace behavior. Three finalists were invited to attend the annual
11 meeting for the company's ethics officers, and the company included their videos in its ethics
12 training materials. Lockheed also instituted an Annual Chairman's Award "for actions or behavior
13 that exemplifies the company's ethics commitment." See Joseph E. Murphy, *Using Incentives in*
14 *Your Compliance and Ethics Program* (Society of Corporate Compliance and Ethics 2011). For
15 example, computer manufacturer Dell uses compliance-training games to enhance compliance
16 performance in the areas of anti-corruption, privacy, and data protection. See
17 https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2015/
18 11/10/how-dell-and-ge-embed-a-culture-of-compliance.aspx. See also https://www.forbes.com/
19 sites/forbesagencycouncil/2017/06/12/five-tips-for-using-games-to-train-your-
20 employees/#77d575c11fb4 ("gamification aligns training with the thoughts and habits that are
21 ingrained in employees' minds, turning their ambition into a competition with themselves and their
22 colleagues.").
23 *f. Internal reporting.* A 2015 study by the Ethics Research Center concluded that
24 employees were more likely to report misconduct internally in firms that, in the view of the
25 researchers, had effective compliance programs than in firms that did not have effective
26 compliance programs. See Ethics Research Center, The State of Ethics in Large Companies (Mar.
27 2015).
28 *g. Relevance of violations.* The U.S. Sentencing Guidelines recognize that the mere fact
29 that a violation has occurred is not in itself proof that the organization's compliance program is
30 ineffective. However, a "recurrence of similar misconduct creates doubt regarding whether the
31 organization took reasonable steps" to achieve an effective program. U.S. SENTENCING GUIDELINES
32 MANUAL,
33 § 8B2.1 cmt. app. n.2(D) (U.S. SENTENCING COMM'N 2016).
34 *h. Risk assessments.* The importance of a risk assessment as a fundamental feature of an
35 effective compliance program is repeatedly stressed in official pronouncements. For example, the
36 SEC-DOJ Resource Guide has this to say about foreign-corrupt-practice compliance programs:
37 "Fundamentally, the design of a company's internal controls must take into account the operational
38 realities and risks attendant to the company's business, such as: the nature of its products or
39 services; how the products or services get to market; the nature of its work force; the degree of
40 regulation; the extent of its government interaction; and the degree to which it has operations in

countries with a high risk of corruption. A company's compliance program should be tailored to these differences. Businesses whose operations expose them to a high risk of corruption will necessarily devise and employ different internal controls than businesses that have a lesser exposure to corruption, just as a financial services company would be expected to devise and employ different internal controls than a manufacturer." Department of Justice Criminal Division and Securities and Exchange Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act, p. 40.

The need for compliance risk assessments is stressed in the U.S. Sentencing Guidelines, which require companies to conduct periodic assessments of risk of criminal conduct and to take appropriate steps to design, implement, or modify the compliance program to reduce the risk so identified. The Organization for Economic Cooperation and Development indicates that risk assessments should be the basis for effective internal controls and for the design of an effective compliance program. See OECD, Risk Management and Corporate Governance (2014). The Committee of Sponsoring Organizations of the Treadway Commission emphasizes the need for risk management in internal controls in its 2004 publication, Enterprise Risk Management – Integrated Framework, and its 2012 publication, Risk Assessment in Practice. The International Organization for Standardization's ISO 31000 standard offers general best-practice advice for risk management. The UK Bribery Act "6 Principles" requires firms to examine categories of risk associated with corrupt foreign practices, including country, sectoral, transaction, business opportunity, and business-partner risk, and to establish priorities, resource allocations, and controls based on the results of this risk assessment. See UK Ministry of Justice, The Bribery Act 2010: Guidance about procedures that relevant commercial organizations can put into place to prevent persons associated with them from bribing (Mar. 2011).

Cyber risk is increasingly recognized as a separate and increasingly important category. See http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/april/Oliver-Wyman-Overcoming-The-Cyber-Risk-Appetite-Challenge.pdf; https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Audit/gx-audit-high-impact-areas.pdf

i. Social media. See PricewaterhouseCoopers, State of Compliance 2014 Survey: What It Means to Be a "Chief" Compliance Officer: Today's Challenges, Tomorrow's Opportunities 21 (2014) (emphasizing the utilization and monitoring of social media as an area coming within the ambit of compliance). The Society of Corporate Compliance and Ethics and the Health Care Compliance Association surveyed 900 compliance specialists on what they perceived as the most urgent compliance risks. The data showed that for all respondents, "social media compliance risks" ranked second in significance amongst these "hot topics." For small companies, privately-held companies, nonprofits, and healthcare companies, "social media compliance risks" was ranked the most significant "hot topic" amongst compliance risk categories. Society of Corporate Compliance and Ethics and the Health Care Compliance Association, Compliance and Ethics Hot Topics (Jan. 2016), http://www.corporatecompliance.org/Portals/1/PDF/Resources/Surveys/2016-hot-topics-survey-report.pdf?ver=2016-02-15-092521-740.

Social media can be integrated into the compliance function and deployed to promote a culture of compliance by more effectively reaching employees and advertising successful compliance activities and events. Social media is not confined to public profiles and can be used intra-organizationally as a salient tool for information transfer and activity monitoring. Cf. Ryan Holmes, *Social Media Compliance Isn't Fun, But It's Necessary*, HARV. BUS. REV. (Aug. 23, 2012) (noting the futility of suppressing social-media usage, and suggesting integrating social media with other operational functions).

j. Data analytics. Deloitte's "Internal Audit Insights 2018" report highlights RPA (robotic process automation) – the use of software to perform rules-based tasks in a virtual environment – as a way of automating repetitive controls testing and internal reporting tasks. However, the report also concedes that internal audit has been slow to change the status quo and adopt new methodologies, and that traditional audit approaches can choke innovation. See https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Audit/gx-audit-high-impact-areas.pdf. On the potential of data analytics for focusing compliance resources on the areas of greatest risk, see https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2015/11/10/how-dell-and-ge-embed-a-culture-of-compliance.aspx.

TOPIC 3

SPECIFIC COMPLIANCE ACTIVITIES

§ 5.07. Compliance Risk Assessment

(a) When deciding how to allocate resources provided for the compliance function, the chief compliance officer should undertake a compliance risk assessment.

(b) Depending on the facts and circumstances, factors relevant to the compliance risk assessment may include:

(1) the nature of the organization's business;

(2) the industry's history of violations;

(3) the organization's history of violations;

(4) compensation arrangements for executives and employees;

(5) whether the organization has introduced a new product line or entered into a new business activity;

(6) whether there has been a change in applicable laws;

(7) whether internal controls are subject to manual override;

(8) the extent of the organization's foreign activities;

(9) the organization's exposure to compliance violations by agents, vendors, customers, or supply-chain counterparties;

(10) regulatory enforcement priorities; and

(11) the probable impact of compliance violations on the organization's reputation.

(c) Any risk assessment performed pursuant to subsection (a) should, if feasible and appropriate, be:

(1) in writing;

(2) evaluated both in terms of the absolute level and the trend of compliance risk; and

(3) reviewed and, if advisable, revised on a periodic basis and be subject to revision as new risks become apparent or old ones subside.

(d) In performing the risk assessment pursuant to subsection (a), the chief compliance officer should make an independent judgment about the compliance risks facing the organization but should also take account of the views of others within the organization, particularly the chief legal officer.

Comment:

a. The compliance function should be risk-based, in the sense that the nature and intensity of the compliance activities should be determined by the compliance risk involved. Accordingly, when deciding how to allocate the resources provided for the compliance function, the chief compliance officer or other appropriate official should undertake a compliance risk assessment by looking both at the probability of a violation and the impact on the organization if a violation occurs. The risk assessment may be based on the results of internal audits, history of violations, industry trends, guidance from government officials, compliance-related complaints, private communications from employees or agents of the organization, and any other relevant information.

The risk assessment need not result in an organization's decision to exit a line of business or customer relationship simply because the business or relationship poses a high inherent compliance risk. If the compliance function is effective, it may transform an unacceptable inherent risk into an acceptable residual risk, and thus allow the organization to participate in the activity at issue.

Another risk that organizations should address in their compliance programs is the possibility that employees who have once engaged in misconduct will do so again. While a history of past misconduct is not necessarily a reason to deny a person an opportunity for employment, it is a factor that an organization should appropriately take into account.

Risk assessments themselves can pose risk to an organization because they may be erroneous. An erroneous risk assessment may lead to a cascade of problems because the organization will allocate compliance resources on an incorrect basis. The result is that the organization overspends for compliance in areas that pose only a low risk of violations and underspends in higher-risk areas. The problem of managing the "meta-risk" of incorrect risk assessments is a difficult challenge for the compliance function.

b. The factors relevant to the compliance risk assessment depend on the facts and circumstances. Subsection (b) sets forth some common danger situations.

The organization's and the industry's histories of compliance violations and the nature of the organization's business are significant risk factors. Other things being equal, organizations that have engaged in past violations may be more likely to commit future violations than organizations with no history of violations. A heightened risk of violations may also be observed in particular industries due to factors such as the corrupt culture of the industry or the nature of the goods or services involved.

Compensation arrangements for employees in sensitive positions are a risk factor. If, for example, salespeople are incentivized to make sales but are not subject to penalty if the transactions they arrange turn out to be fraudulent or illegal, they have an incentive to engage in a higher level of questionable sales activities. Similarly, agents who are rewarded for arranging contracts but who suffer no risk of sanction if the contracts turn out to be procured by improper payments may be more likely to engage in impermissible conduct than are agents whose compensations are based in part on compliance with anti-corruption laws.

Changes in product lines or business activities can pose heightened compliance risks. When an organization enters into a new area, it may be unfamiliar with the applicable rules and regulations, and the officials responsible for the new area may be unfamiliar with regulatory expectations. Similarly, changes in applicable regulations pose compliance risks because employees of the organization may be unfamiliar with revised requirements, and control systems may not have kept pace with legal change.

Compliance systems may include procedures for the manual override of controls to account for unusual or unfamiliar circumstances. Manual overrides enhance the risk of compliance breakdowns, since a person may perform an override to cover misconduct rather than to facilitate

legitimate business needs. Accordingly, procedures for manual override should be accompanied by controls against abuse.

When the organization conducts substantial foreign activities, the compliance risk assessment should include consideration both of the requirements of foreign law and the potential for improper payments to foreign officials. The latter issue, in turn, depends in part on the risk environment of the foreign country in question. When assessing corruption risk, the chief compliance officer may consider publicly available risk measures such as Transparency International's Corruption Perceptions Index.

Many organizations use the services of vendors to assist in their core operations. These arrangements often provide significant benefits but also carry compliance risks, since organizations may be exposed to liability for violations by the vendor. The organization should consider these risks when designing its compliance program. It may manage the risks through provisions in vendor contracts, giving the organization audit rights or rights to terminate contracts if the vendor is found to present unacceptable risks. Similar compliance problems may arise in connection with relations with agents, customers, or remote participants in the organization's supply chain.

c. The organization's compliance risk assessment is a central part of a compliance program, and accordingly should be embodied in an appropriate medium. Larger organizations should record the risk assessment in writing and subject it to periodic review and revision as new risks become manifest or old risks fade in importance.

d. The chief compliance officer's risk assessment may, as appropriate, be informed by assessments performed by others such as the chief risk officer, the chief legal officer, the risk committee of the board of directors, or internal or external audit. However, because of its specialized nature and the need for assurance regarding the effectiveness of the process, compliance risk assessment should not be wholly performed elsewhere in the organization.

REPORTERS' NOTE

a. *Importance of risk assessments.* On the importance of risk assessments in the compliance function, see U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(c) (U.S. SENTENCING COMM'N 2016) (organizations should periodically assess the risk of violations and take appropriate steps to reduce the risk). Government regulators frequently stress the importance of compliance risk assessments. See, e.g., Thomas Baxter, Executive Vice President and General Counsel, Federal

Reserve Bank of New York, Compliance – Some Thoughts About Reaching the Next Level (Feb. 9, 2015).

b. Changes in laws. See Lori A. Richards, Director, Office of Compliance Inspections and Examinations, Securities and Exchange Commission, Incentivizing Good Compliance, 2008 Willamette Securities Regulation Conference, Willamette University College of Law (Oct. 30, 2008), https://www.sec.gov/news/speech/2008/spch103008lar.htm ("[W]e often find that firms are not aware of compliance obligations with respect to new rules. It sometimes takes time for people to learn about and understand their obligation.").

c. Contractual terms with counterparties. The compliance function increasingly involves a host of representations, commitments, rights, and obligations contained in contractual agreements with counterparties, in areas as diverse as vendor risk management and supply-chain due diligence. See Scott Killingsworth, The Privatization of Compliance, RAND Center for Corporate Ethics and Governance Symposium White Paper Series, Symposium on "Transforming Compliance: Emerging Paradigms for Boards, Management, Compliance Officers, and Government" (2014). The DOJ has promoted the usage of contractual terms to limit counterparty risk exposure through deferred prosecution agreements. United States v. Total, S.A., Deferred Prosecution Agreement, No. 13-CR-239, C1-C6 (E.D. Va. May 29, 2013).

d. Recidivism. Another risk that organizations should address in their compliance programs is the possibility that employees who have once engaged in misconduct will do so again. The United States Sentencing Guidelines call for an organization to exclude from its executive ranks people known to have "engaged in illegal activity or other conduct inconsistent with an effective ethics and compliance program." U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(3) (U.S. SENTENCING COMM'N 2016).

e. Vendor risk. Guidance on managing vendor risk is contained in Federal Reserve Board Supervisory Letter No. SR 13-19, Guidance on Managing Outsourcing Risk (Dec. 5, 2013); Office of the Comptroller of the Currency Bulletin No. 2013-29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013); Federal Deposit Insurance Corporation Letter No. FIL-44-2008, Third-Party Risk: Guidance for Managing Third-Party Risk (June 6, 2008); Federal Reserve Bank of New York, Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks (Oct. 1999); Consumer Financial Protection Bureau Bulletin No. 2012-03, Service Providers (Apr. 13, 2012).

§ 5.08. Compliance Advice

(a) The compliance function should stand ready to provide advice to employees and agents on how to behave in a compliant and ethical way.

(b) The advice described in subsection (a) may be provided by a compliance officer, a legal officer, or some other appropriate person. The identity of the person providing such

advice and the mechanism through which it is provided depend on the facts and circumstances.

(c) Employees or agents who rely on such advice in good faith should be protected against retaliation or punishment by the organization if the advice given proves to be mistaken.

Comment:

a. Compliance has evolved over the past decades from being a "watchdog" function—charged with seeking out misconduct—to including an important advisory and counseling element. The compliance function should maintain a repository of information about proper responses to challenging or ambiguous situations, and should stand ready to provide advice to employees and agents on how to behave in a compliant and ethical way.

b. As with other aspects of the compliance function, there is no "one size fits all" formula for how compliance-related advice should be provided, or by whom. The identity of the person providing such advice and the mechanism through which it is provided necessarily depend on the facts and circumstances surrounding each organization.

c. Compliance-related advice is only useful if it is credible. Moreover, organizations should reward employees or agents who reach out in good faith to seek such advice. Accordingly, organizations should not retaliate or punish employees or agents who in good faith act in reliance on such advice if the advice given proves to be mistaken.

REPORTERS' NOTE

a. *Advice.* See Office of the Comptroller of the Currency, The Director's Book: Role of Directors for National Banks and Federal Savings Associations (July 2016) ("The bank should have an ethics officer, bank counsel, or some other individual from whom employees can seek advice regarding ethics questions."). The role of the compliance officer has been recognized as a versatile one in which advice and counsel on topics indirectly affected by compliance or ethics is provided. Even when compliance is not concerned, a compliance perspective can serve to strengthen the compliance culture and provide a diverse perspective on certain business matters. See International Finance Corporation, World Bank Group, *Risk Culture, Risk Balance, and Balanced Incentives* (Aug. 2015) (recognizing an additional role of the compliance function in advising the board and committees on risk and other business operations); Michele DeStefano, *Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 10 HASTINGS BUS. L.J. 71, 95 n.100 (2014) ("Chief compliance officers also advise on business and reputational risks.")

§ 5.09. Compliance Monitoring [RESERVED]

§ 5.10. Training and Education

(a) The compliance function should include training and other educational activities regarding the compliance obligations of the organization and its employees and agents.

(b) The compliance function should make appropriate compliance training available to all employees. Compliance training should include advising the board of directors and senior managers on applicable laws, rules, and standards.

(c) The appropriate form of training depends on the facts and circumstances surrounding each organization, including its size, its complexity, the nature of the business line's activity, the compliance risk posed, the level of sophistication and experience of the employees involved, and the legal requirements for training of personnel.

Comment:

a. Training and education are keys to effective compliance programs. Accordingly, an important part of the compliance function's responsibilities is educational: compliance officers or third parties acting subject to their supervision should instruct others in the organization about how to fulfill the obligations associated with their roles. Compliance training may be integrated with other instructional programs carried on by or for the organization.

Because training programs do not have an immediate and measurable impact on the bottom line, they may be tempting candidates for cutbacks when an organization's profits are thin. While compliance training should not be exempt from the need to "tighten the belt" in lean times, organizations should resist the temptation to reduce training expenditures too readily, because the long-term costs of doing so may outweigh any short-term cost savings.

Training can be performed in-house or by third-party vendors. When selecting a training vendor, a company should confirm that the proposed service provider is qualified in the area of instruction, familiar with compliance functions and processes, and able to incorporate the organization's specific requirements into the training. It may be prudent for the organization to memorialize its training activities in order to preserve a record of its efforts in the event of later enforcement actions.

b. Training should be provided to all employees whose actions create a significant compliance risk for the organization. When feasible, live, in-person training may be more effective

than training conducted by means of videos, online programs, or written materials. Live training also confers additional potential advantages: it provides an opportunity for senior officials to demonstrate their personal commitment to compliance (by attending training sessions), and may generate valuable information in the form of comments made by employees during training sessions. Persons occupying leadership positions need not be experts in the law but should have some familiarity with the requirements applicable to their organizations. Thus, training for the organization's senior leaders should generally cover laws, rules, and standards, including updates on current developments.

In many organizations, no single office has the substantive expertise to manage the training needed for compliance in such diverse areas as tax, occupational safety and health, export controls, foreign corrupt practices, antitrust, and other areas. For these organizations, the compliance function should be charged with assuring that each of the organization's risk-specific activities conducts compliance training for employees whose responsibilities could affect compliance in that category of risk.

c. Compliance training and education activities should take account of the nature of the organization, the sophistication of its employees, and other matters. In appropriate cases, videos or online training modules may be effective training media. The compliance function may disseminate written documents such as compliance manuals or practice guidelines, or responses to individual requests for advice. Whatever the format employed, training that is more interesting and that contains concrete examples is more likely to be remembered. Training materials should also take account of language barriers: for example, materials written in English may be of little help when the affected employees are foreign nationals with minimal English skills.

REPORTERS' NOTE

a. *Generally.* For healthcare providers, the Department of Health & Human Services' Office of Inspector General has published a page of free compliance education materials and resources. Office of Inspector General, Department of Health & Human Services, The Compliance Resource Portal, https://www.oig.hhs.gov/compliance/compliance-resource-portal/.

b. *Language barriers.* The Department of Justice's and Securities and Exchange Commission's Resource Guide to the Foreign Corrupt Practices Act observes that "[r]egardless of how a company chooses to conduct its training . . . the information should be presented in a manner appropriate for the targeted audience, including providing training and training materials in the local language." See Department of Justice Criminal Division and Securities and Exchange

Commission Enforcement Division, A Resource Guide to the U.S. Foreign Corrupt Practices Act, https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

c. Employee sophistication. Within an organization, employees will likely vary in sophistication. Trainers should tailor their curriculum and level of rigor based on the sophistication of the employee or risk jeopardizing the efficacy of the training program. For executive officials who may have an understanding of regulatory requirements, training programs could be directed toward reinforcing other compliance risks; for newer employees whose introduction to the industry may be limited, compliance training may be directed at risk-awareness training and behavioral reinforcement.

d. Computer based training. For discussion of computer applications for compliance training, see, e.g., https://inspiredelearning.com/mobile/; https://elearningindustry.com/mobile-learning-tackles-compliance-training; https://www.traliant.com/blog/2017/08/10/traliant-announces-new-lms-app-for-compliance-training-managers/.

§ 5.11. Red Flags

(a) The compliance function should be alert to red flags of potential violations. Depending on the facts and circumstances, red flags can include but are not limited to:

(1) transactions with no apparent business purpose;

(2) sudden material changes in performance that cannot be explained by known causes;

(3) excessively complex structures;

(4) frequent failures to complete required paperwork;

(5) efforts to disguise the identity of customers or other counterparties;

(6) gifts or favors to customers or business partners, or family members of customers or business partners, that appear excessive in light of the customs of the industry;

(7) gifts or favors to government officials or to family members of government officials;

(8) unusual and persistent failures to take allowed vacations or time off; and

(9) unauthorized self-dealing or other conflicted activities by employees and agents.

(b) The presence of a red flag does not indicate that a violation has occurred.

(c) A compliance officer who knows of a red flag of a violation should undertake appropriate responsive actions.

Comment:

a. Employees and agents do not usually advertise their misconduct. It is uncommon for the chief compliance officer or his or her staff to observe misconduct directly. Unless information comes from an informant (see § 1.01(bb)), a compliance problem typically comes to the attention of management through signals indirectly indicating that misconduct may have occurred. These signals are often referred to as "red flags."

Red flags of compliance violations vary from industry to industry. Some occur frequently enough, however, as to warrant mention in these Principles. An example is a pattern of transactions with no identifiable business purpose. When no benign purpose can be discerned, a responsible compliance officer should entertain the possibility that the transactions in question are intended for an impermissible purpose. The compliance officer should ask the relevant business-line officer to explain the transactions, and, if no satisfactory explanation is forthcoming, should undertake other appropriate responsive actions.

Another danger sign is sudden material changes in performance that cannot readily be explained. Material changes ordinarily have an obvious explanation—a revision of accounting treatment, acquisition of a new business, a lost contract, and so on. When no such cause can be discerned, the chief compliance officer should consider whether the changes are due to circumstances that someone in the organization wishes to disguise.

Excessively complex structures can present red flags. Unless some rational purpose is ascertained for complex structures—limiting taxation, managing liability risk, organizing governance of activities, for example—the chief compliance officer should consider whether the structure in question serves a less benign purpose. Enron's financing transactions are a case in point. These arrangements were so complex that few outside the company understood them. It turned out that the complexity was masking a fraud that came to light only after the company had disguised its financial condition for years.

Frequent failures to complete required paperwork or to file reports indicate that the employees or agents in question are overworked or willing to cut corners in other respects. A larger concern is that paperwork requirements may be ignored because the person in question does not

want to alert a supervisor or control official of an impermissible activity in which he or she is engaged.

Efforts to disguise the identities of customers or other counterparties and excessive gifts to business partners raise the specter that undue influence is being exerted. These concerns are especially salient when the transaction involves a foreign country that presents a risk of official corruption.

Unusual and persistent failures to take allowed vacations or time off can be a red flag in situations where the employee's behavior could reflect an attempt to prevent others from learning details of their job performance.

Self-dealing and other conflicted behavior by senior executive officers are serious concerns. When self-dealing transactions occur frequently, or when the size of such transactions is large relative to the scale of the organization, the responsible compliance officer may have reason for worry that high-level officials are improperly enriching themselves at the organization's expense.

b. These or other red flags do not necessarily indicate that a violation has occurred. Such red flags, however, are a cause for further inquiry because they increase the risk that misconduct may be occurring within the organization.

c. A compliance officer who knows of a red flag of a violation should undertake appropriate responsive actions. If the violation is minor and unlikely to be repeated, the appropriate response could be to counsel the responsible party or undertake other informal actions. If a red flag signaling significant misconduct comes to the attention of the compliance function, compliance officers should engage in further inquiry. If such inquiry confirms suspicions or provides grounds for greater concern, the responsible compliance officer should undertake additional measures as appropriate.

REPORTERS' NOTE

a. *Gifts and high-pressure sales tactics.* See FINRA, Protecting Senior Investors: Report of Examinations of Securities Firms Providing "Free Lunch" Sales Seminars, Sept. 2007, http://www.finra.org/sites/default/files/Industry/p036814.pdf. FINRA Rule 3220 prohibits any member or person associated with a member, directly or indirectly, from giving anything of value in excess of $100 per year to any person where such payment is in relation to the business of the recipient's employer. The rule also requires members to keep separate records regarding gifts and gratuities. The rule seeks both to avoid improprieties that may arise when a member firm or its

associated persons give anything of value to an employee of a customer or counterparty and to preserve an employee's duty to act in the best interests of that customer.

b. Self-dealing and conflicts of interest. See, e.g., Carlo V. di Florio, Director, Office of Compliance Inspections and Examinations, Securities and Exchange Commission, Conflicts of Interest and Risk Governance, speech at the National Society of Compliance Professionals (Oct. 22, 2012), http://www.sec.gov/News/Speech/Detail/Speech/1365171491600 (providing a discussion of the inherent dangers related to conflicts of interest, outlining "numerous examples of conflicts leading to crisis," most notably the stock-market crash of 1929 and the demise of Drexel Burnham Lambert in 1990). Conflicts of interest may lead to an abdication of one's fiduciary duties, which may result in facing a stakeholder suit.

c. Failure to report red flags. Recognizing a red flag and failing to take remedial action may constitute a "dereliction of duty, a conscious disregard for one's responsibilities" and may put a board or its members at risk of liability. In re Walt Disney Co. Derivative Litig., 906 A.2d 27, 62 (Del. 2006).

§ 5.12. Escalation Within the Organization

(a) If a compliance officer knows that an employee or agent has engaged, or intends to engage, in illegal conduct or other impermissible activity that poses a significant risk to the organization or a third party if not corrected or remediated, he or she should act as reasonably necessary in the best interests of the organization.

(b) If the matter cannot be addressed in a timely manner within the scope of his or her authority, the chief compliance officer should refer the issue to an official who has the power to address the matter, including, when appropriate, the board of directors. Reporting up is not required if the effort would clearly be futile due to potential involvement in misconduct by higher level officials.

(c) If after undertaking the actions described in subsection (b), the chief compliance officer in good faith believes that the matter will not be satisfactorily addressed in an appropriate time within the organization and that the failure to address the matter poses a material threat to the organization's financial position or strategic objectives or to third parties, he or she may disclose the concerns to an appropriate government regulator.

Comment:

a. Compliance officials are responsible for controls over the risk of misconduct by an organization and its employees and agents. Accordingly, if an officer knows that an employee or agent has engaged or intends to engage in an impermissible activity that poses a significant risk if not corrected or remediated, he or she should take appropriate action. The chief compliance officer should act as is reasonably necessary in the best interests of the organization, in light of the circumstances and the facts then known.

b. The appropriate response by the responsible compliance officer depends on his or her authority. He or she may have the power to undertake effective corrective action directly without involving others. If the responsible compliance officer does not have the requisite authority, he or she should refer the matter to the appropriate official. Such officials could include, for example, the offending employee's supervisor, the head of the human-resources department, the organization's chief legal officer, an official responsible for relations with vendors or customers, or the official to whom the chief compliance officer reports. When appropriate, the chief compliance officer may report the issue to the board of directors—in a business corporation, a person such as the chair of the board audit committee. Reporting is not required if it would obviously be futile—for example, if the higher-level official is directly implicated in the misconduct.

REPORTERS' NOTE

a. *International comparison.* In the United Kingdom, compliance officers for institutions regulated by the Financial Conduct Authority have an obligation to "disclose appropriately any information of which the [regulators] would reasonably expect notice." Financial Conduct Authority, Statement of Principle 4. See United Kingdom Financial Conduct Authority, The Principles, https://www.imf.org/external/pubs/ft/scr/2016/cr16166.pdf.

b. *Escalation process.* The Financial Stability Board models the escalation process to: define clear consequences for noncompliance with escalation procedures; assess employee awareness of escalation processes and whether the environment is perceived as open to critical challenge; establish mechanisms for employees to elevate and report concerns when discomforted about products or practices, even when there is no specific allegation of wrongdoing; create appropriate whistleblowing procedures that are expected to be utilized by employees without any reprisal, to support effective compliance with the risk-management framework; clearly articulate, and follow in practice, the treatment of whistle blowers. FSB, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture 8 (April 2014).

The Office of the Comptroller of the Currency and others have similarly emphasized the importance and benefits of an efficacious escalation process. OCC, The Director's Book: Role of Directors for National Banks and Federal Savings Associations 64 (July 2016) ("Management also should ensure there is a mechanism for employees to confidentially raise concerns about illegal activities and violations. The mechanism also should allow employees to confidentially report circumvention of regulations or company policies."); Salz Review, Section 8.40, at 87 (Apr. 2013) ("Reluctance by staff to escalate issues, coupled with an expectation that employees needed to show that they could resolve problems themselves, rather than look to others to do so, created a culture that lacked openness."); International Finance Corporation, World Bank Group, *Risk Culture, Risk Balance, and Balanced Incentives* 4, 21 (Aug. 2015) ("There should be structured communication channels to ensure effective risk reporting within the bank and, where necessary, with external parties. The bank's employees should be encouraged to identify and report on existing and emerging risks through a clearly defined escalation process. Communication also helps inform the whole bank of the importance placed by top management on staff having the right risk culture…Employees should have a clear understanding of the channels and processes, as well as rights and protections, for raising risk issues, whether directly or anonymously.").

§ 5.13. Compliance Under Legal Uncertainty

(a) Unless the organization's rules of governance otherwise provide, the chief compliance officer is not responsible for resolving uncertainty in applicable rules or regulations.

(b) If the chief compliance officer deems it important to resolve a legal uncertainty in order to perform his or her responsibilities, he or she should ordinarily seek guidance from the chief legal officer or another qualified attorney. If such guidance is not available, the chief compliance officer should apply the most reasonable interpretation.

Comment:

a. Legal uncertainty can impose risks for organizations. If an organization resolves legal uncertainties against its interests but it later turns out that the law is more favorable, then the organization may lose profits it could have earned and also fail to provide goods or services to the public. On the other hand, if uncertainties are resolved in favor of the organization and are later interpreted differently by a court or agency, the organization may face enforcement actions, fines, and possible loss of reputation.

b. A person acting in the capacity of chief compliance officer is not an attorney for the organization and, unless the organization's governance rules otherwise provide, is not ordinarily

responsible for resolving legal uncertainty. He or she should ordinarily be entitled to rely on interpretations of applicable legal rules provided by the chief legal officer or another qualified attorney. If the chief compliance officer deems it important to resolve a legal uncertainty in order to perform his or her official responsibilities, and if appropriate under the organization's governance rules, he or she should seek guidance from the chief legal officer or other qualified attorney. If such guidance is not available, the chief compliance officer should apply the most reasonable interpretation. It is advisable that any interpretation of uncertain legal requirements be recorded in writing and preserved as a record of the organization.

REPORTERS' NOTE

a. Applicable scholarship. For analysis of the costs to organizations and the public that can arise when compliance organizations operating under legal uncertainty interpret the law in ways that unduly constrain their activities, see John P. Anderson, *Solving the Paradox of Insider Trading Compliance*, 88 TEMPLE L. REV. 273 (2016).

TOPIC 4

EMPLOYEES, AGENTS, AND COUNTERPARTIES

§ 5.14. Hiring of Employees, Retention of Agents, and Selection of Counterparties

(a) Unless otherwise indicated by the circumstances, the official charged with hiring employees or retaining agents should consider a candidate's background and history of compliance with applicable laws, regulations, and ethical norms. Candidates deemed to present an unacceptable risk of violations should not be hired or retained.

(b) The official tasked with selecting a vendor or supplier, or engaging in a transaction with a customer, should take into consideration the risk that misconduct by that vendor, supplier, or customer will be attributed to or otherwise result in harm to the organization. Prospective vendors, suppliers, or customers should not be dealt with if they present an unacceptable risk of misconduct that will result in harm to the organization.

Comment:

a. People who have committed violations in the past present a heightened risk of doing so again. Thus, an organization may appropriately take a person's history of violations into account when making a decision on whether to hire or retain that person. Candidates deemed to present an

unacceptable risk of violations should not be hired or retained. In some industries, applicable regulations prohibit the hiring of people who have committed acts of significant misconduct.

b. Misconduct by vendors, suppliers, or customers can harm organizations in a variety of ways. An unethical counterparty can defraud or otherwise impose costs on the organization. Misconduct by a vendor, supplier, or customer may be legally attributed to the organization. An organization may be penalized for dealing with counterparties who are unsuitable or legally off limits. Organizations may incur penalties for failing to undertake legal obligations imposed on them by virtue of their dealings with counterparties; an example is a financial institution's obligation to file suspicious activities reports in connection with questionable transactions. Organizations also face reputational costs if they are associated in the public eye with a counterparty who has engaged in compliance violations or who is perceived to be undesirable for other reasons. Because of these concerns, the official tasked with selecting a vendor, supplier, or customer should consider the risk that misconduct by such a party will be attributed to or otherwise result in harm to the organization. Vendors, suppliers, and customers should not be dealt with if they present an unacceptable risk of misconduct.

§ 5.15. Background Checks

In carrying out the activities contemplated in § 5.14, an organization may engage in background checks of potential employees, agents, or counterparties. Such background checks must comport with applicable legal restrictions, must not result in invidious discrimination, should be appropriate for the position in question, and should avoid intruding unnecessarily on reasonable expectations of privacy.

Comment:

a. In order to comply with the obligations of § 5.14, an organization will often find it desirable to investigate a candidate's background. The organization should ordinarily check the background of potential employees or agents whose wrongful conduct could pose a significant risk of harm to the organization. These inquiries may include communications with references, searches of criminal records, and credit checks. Additional checks may be appropriate for particular settings. For example, contractors with the United States may seek to confirm that employees are not excluded parties under the government's System for Award Management. Similarly, when conducting business in countries presenting corruption risk, an organization may

screen third-party business partners for criminal backgrounds, associations with government officials, and financial integrity.

Despite their value, background checks are subject to limitations. They must comport with legal restrictions and must not result in invidious discrimination against any person, and they should not intrude unnecessarily into a candidate's reasonable expectations of privacy. The use of criminal background checks may raise concerns about potentially discriminatory impacts on employment, to the extent that histories of arrests or convictions differ by race, gender, or other protected classifications. For this reason an organization should employ criminal background checks cautiously and should never use the result of these checks as a reason for disfavoring any employee or job candidate on grounds unrelated to his or her suitability for the position in question.

REPORTERS' NOTE

a. *Criminal background checks.* The Equal Employment Opportunity Commission (EEOC) has taken the position that the use of criminal background checks can constitute impermissible employment discrimination in violation of Title VII of the Civil Rights Act of 1964. See Equal Employment Opportunity Commission v. Dolgencorp, LLC, 249 F. Supp. 3d 890 (N.D. Ill. 2017); E.E.O.C. v. BMW Mfg. Co., LLC, 2015 WL 5431118 (D.S.C. July 30, 2015); BMW to Pay $1.6 Million and Offer Jobs to Settle Federal Race Discrimination Lawsuit, EEOC press release, September 8, 2015, https://www.eeoc.gov/eeoc/newsroom/release/9-8-15.cfm. For a decision critical of the EEOC's claims of employment discrimination based on the use of background checks, see EEOC v. Freeman, 961 F. Supp. 2d 783, 803 (D. Md. 2013), aff'd, 778 F.3d 463 (4th Cir. 2015) ("By bringing actions of this nature, the EEOC has placed many employers in the "Hobson's choice" of ignoring criminal history and credit background, thus exposing themselves to potential liability for criminal and fraudulent acts committed by employees, on the one hand, or incurring the wrath of the EEOC for having utilized information deemed fundamental by most employers.").

Several states impose limits on an employer's ability to ask about a job applicant's criminal history. In some states, employers are prohibited from asking about arrests that did not result in convictions; some allow inquiries into convictions only if the offense relates to the requirements of the job opening; some require employers to consider the background circumstances and mitigating factors in criminal convictions; some prohibit employers from inquiring into criminal histories until after the applicant has interviewed for the job or received a conditional job offer. See generally https:/www.nolo.com/legal-encyclopedia/state-laws-use-arrests-convictions-employment.html.

b. *Criminal records*. On criminal records generally, see JAMES JACOBS, THE ETERNAL CRIMINAL RECORD (Harv. U. Press 2015).

c. *Data analytics*. The EEOC held a meeting in 2016 about the use of big data in hiring decisions—also known as predictive analytics or talent analytics, which could equally be applied to weed out potentially problematic employees or agents using empirical data. See https://www.eeoc.gov/eeoc/newsroom/release/10-13-16.cfm

d. *Risks.* The American Civil Liberties Union warns that "[T]oo often [background checks] are used to inappropriately blacklist individuals who are thereby prevented from recovering from mistakes in their past," and that "[b]ackground checks often contain erroneous information that results in unfair treatment and are used without giving individuals the right to challenge or explain their contents." American Civil Liberties Union, Background Checks, https://www.aclu.org/issues/privacy-technology/workplace-privacy/background-checks.

§ 5.16. Compensation

(a) An employee's record of compliant or noncompliant behavior should be considered as a factor in setting his or her compensation.

(b) Bonuses and other nonsalary compensation for employees in a compliance function should be independent of the performance of any business line overseen by the employee and should be based in substantial part on the achievement of compliance-based objectives.

Comment:

a. While compensation is not the only driver of behavior within organizations, it is a powerful incentive. It is appropriate for organizations to use compensation systems as tools to encourage compliant behavior and discourage misconduct. This is particularly true in the case of senior executives; an organization may structure its compensation system so that the extent to which an executive meets compliance standards impacts the amount of that person's bonus, and failure to meet compliance standards results in reduction or voiding of such compensation.

b. Compensation for the chief compliance officer and his or her staff presents special problems. On the one hand, these individuals are part of the organization and share in its success or failure. It is appropriate that their compensation be adjusted, to some extent, to reflect the organization's overall performance. On the other hand, compensation for compliance officers should not create incentives to shirk on the job or pull their punches. Accordingly, compensation for employees in a compliance function should, if possible, be independent of the performance of any business line overseen, and performance measures should be based in substantial part on the

achievement of compliance-based objectives rather than on the objectives of the business lines or the organization as a whole. Where the compliance function oversees all business lines, or where the organization has only one business line, the organization may elect to pay compliance officers on a salary basis or otherwise to limit the amount of their incentive-based compensation.

REPORTERS' NOTE

a. *Adoption of positive incentives.* Many organizations have been slow to create positive incentives for compliant behavior. See, e.g., Incentive Programs and Compliance, A Survey by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association (April 2017), https://www.hcca-info.org/Portals/0/PDFs/Resources/Surveys/2017-incentives-programs-and-compliance-survey.pdf?ver=2017-05-08-124106-733.

b. *Clawbacks.* Clawbacks of deferred compensation are appropriate when a responsible official has egregiously violated an internal-control obligation and thereby contributed to a violation of an external or internal norm. See, e.g., United States v. HSBC Bank N.A., Deferred Prosecution Agreement, No. 12-CR-763 (E.D.N.Y. July 1, 2013) (reporting that the defendant clawed back bonuses from its chief compliance officer, the chief AML officer, and the chief executive officer).

c. *Confidentiality.* Financial penalties for misconduct may compromise the confidentiality of the organization's internal processes because the reasons for the penalty may become known. Some organizations may prefer not to place evidence of an employee's compliance breaches on the record out of concern that the file may be discovered and used against the organization in later adversarial proceedings. Michael Goldsmith & Chad King, *Policing Corporate Crime: The Dilemma of Internal Compliance Programs*, 50 VAND. L. REV. 1 (1997) (noting how compliance programs create the unanticipated dilemma of producing a paper trail, potentially discouraging complete candor or a comprehensive internal-control system). However, organizations should also consider the costs of not making a record of compliance violations. Without such a record, it may be difficult to impose discipline on the employee when further acts of misconduct occur. Beyond this, a policy of not recording compliance violations may contribute to an unhealthy culture that tends to minimize the importance and impact of violations. Additionally, the benefits of an effective system of internal controls may offset the fears of increased exposure to regulators or adversaries. These benefits may include a mitigated penalty for a violation or the decreased likelihood of committing costly violations. U.S. SENTENCING GUIDELINES MANUAL § 8C2.5(f)(1) (U.S. SENTENCING COMM'N 2016) (subtracting points from an organization's culpability score for having an effective compliance program).

d. *Incentives for compliant behavior.* For discussion and analysis, see, e.g., Joseph E. Murphy, Using Incentives in Your Compliance and Ethics Program (Society of Corporate Compliance and Ethics 2011), https://www.corporatecompliance.org/Portals/1/PDF/Resources/IncentivesCEProgram-Murphy.pdf; Lori A. Richards, Director, Office of Compliance Inspections and Examinations, Securities and Exchange Commission, Incentivizing

Good Compliance, 2008 Willamette Securities Regulation Conference, Willamette University College of Law (Oct. 30, 2008), https://www.sec.gov/news/speech/2008/spch103008lar.htm; International Finance Corporation, World Bank, *Risk Culture, Risk Balance, and Balanced Incentives* (Aug. 2015) ("The bank seeks the advice of its risk management and control design functions in the design and review of the incentive programs."), https://www.ifc.org/wps/wcm/connect/4e887b2e-5999-485e-95b1-428c157cfea6/IFC+Risk+Culture+Governance+Incentives+report.pdf?MOD=AJPERES. The Walker Report, published in the UK by the Chancellor of the Exchequer, Secretary of State for Business, Enterprise and Regulatory Reform, and the Financial Services Secretary to the Treasury recognizes remuneration as a mechanism for controlling risk, to discourage short-term risk-taking and encourage long-term responsibility by management. Chancellor of the Exchequer, A review of corporate governance in UK banks and other financial industry entities, Final recommendations 119 (Nov. 26, 2009), http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/d/walker_review_261109.pdf ("The remuneration committee should seek advice from the board risk committee on specific risk adjustments to be applied to performance objectives set in the context of incentive packages.").

e. Settlements of regulatory actions. Incentives for compliance are sometimes found in settlements of regulatory actions. See, e.g., Settlement Agreement with Mellon Bank, N.A., (Appendix A, Para. 6(c)) (Aug. 14, 2006), http://www.corporatecompliance.org/Resources/View/tabid/531/ArticleId/737/Settlement-Agreement-in-Mellon-Bank-Case.aspx ("Performance evaluation criteria and compensation should also be linked to specific steps taken by [senior executives] to support the compliance and ethics program (e.g., briefing "direct reports" on the code's application and the importance of raising compliance and ethics issues; ensuring that "direct reports" have completed required training).").

§ 5.17. Discipline

(a) In addition to setting compensation practices to incentivize compliant behavior, organizations should consider imposing nonmonetary discipline for violations.

(b) As in the case of monetary sanctions, the form of nonmonetary discipline should be commensurate with the gravity of the offense and consistent with the organization's stated policies and procedures.

(c) Nonmonetary sanctions should be based on clearly expressed and widely disseminated norms of conduct and should be administered within the organization on an evenhanded basis.

(d) The organization's decision whether to report misconduct should depend on the facts and circumstances, including the gravity of the offense, whether third parties have been

harmed by the misconduct, the likelihood of recidivism, the probable response of regulators, and fairness to parties involved.

Comment:

a. Compliance programs may be more effective when organizations impose nonmonetary as well as monetary penalties for violations by employees or agents. Forms of nonmonetary discipline can include termination, demotion, suspension, reassignment, probation, warnings, censures, and reporting of the individual's conduct to law-enforcement authorities. Nonmonetary sanctions may sometimes be required by applicable regulations; in such cases, the organization must conform to these legal requirements.

Even if an organization maintains confidentiality regarding penalties imposed in particular cases, it should generally inform its employees and agents about the consequences of misconduct. In this way everyone in the organization is placed on notice of the organization's reasonable expectations.

It is usually advisable for the organization to share reports of disciplinary cases with the legal department. Among other benefits, such sharing of information can provide the legal department with valuable information about the legal issues and risks facing the organization.

b. Organizations have a greater interest in deterring significant violations than minor ones; an employee or agent who commits a minor violation ordinarily represents a lesser threat than an employee who engages in significant misconduct. Accordingly, organizations should attempt to match the severity of the discipline with the significance of the offense. Organizations that engage in a "broken windows" style of compliance program, in which even minor offenses are sanctioned, should nevertheless attempt to administer punishments that are reasonably adjusted to reflect the severity of the offense.

c. Compliance programs are more effective if they receive "buy-in" from employees and agents. A disciplinary process that is administered in an unfair or biased way—or that is perceived as such within the organization—is likely to receive less respect and be less effective than one that is perceived as fair and impartial. It is important that such proceedings are and are perceived within the organization as conducted on an evenhanded and impartial basis, without favoring any person or group. Resolutions of disciplinary matters that preserve confidentiality can sometimes erode discipline if rumors circulate that high-level employees receive lighter penalties than lower-level

employees. This problem can be addressed, to some extent, by disclosing statistics on the number and type of disciplinary actions taken for various categories of compliance violations.

d. Organizations may face a difficult issue when deciding whether the results of disciplinary proceedings will be reported to the authorities or otherwise made available to third parties (unless law or regulation mandate this reporting). On the one hand, there is a public interest in preventing "bad apple" employees from leaving one organization after being found to have engaged in misconduct, only to wind up in another organization where they do the same thing. On the other hand, organizations may be appropriately sensitive to the privacy interests of the employee involved and may not wish to bring potentially career-ending consequences upon an individual whose misconduct may have been part of a broader pattern of failures of people and systems of internal control. Organizations should balance these and other factors when determining whether and to what extent to reveal disciplinary actions against their employees or agents.

e. The recommendations contained in this section should be interpreted in conformity with the American Law Institute's Restatement of Employment Law (AM. LAW INST. 2015).

REPORTERS' NOTE

a. *Incentives for compliant behavior.* See U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(6) (U.S. SENTENCING COMM'N 2016). In considering specific factors for the evaluation of a corporate compliance program, the Justice Department looks to "Incentives and Disciplinary Measures" taken by the company in the face of misconduct. Measured factors include: management accountability, a company's disciplinary record relating to the specific conduct, who participated in the disciplinary decisions, whether the disciplinary actions were applied fairly and consistently across the organization, and how the company has incentivized compliant behavior and accounted for potential negative implications of company incentives and rewards. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs, https://www.justice.gov/criminal-fraud/page/file/937501/download.

b. *Fairness in administration of discipline.* See Remarks of Leslie R. Caldwell, Assistant Attorney General for the Criminal Division (Oct. 1, 2014), http://www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-22nd-annual-ethics ("Too often, we see situations where low level employees who may have implemented the bad conduct are fired, but their boss, who saw what they were doing and did nothing—and maybe even the [sic] directed the conduct—is left in place. This should not happen. . . . Leaving in place senior managers who sanction bad behavior sends a very wrong message about the company's true commitment to compliance and ethics.")

c. *Proportionality*. See Financial Stability Board, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture 1 (April

2014) (emphasizing that a sound risk culture requires that "all limit breaches, deviations from established policies, and operational incidents are thoroughly followed up with proportionate disciplinary actions when necessary.").

d. *Facts and circumstances.* The nature of a disciplinary action should be contingent on the facts and circumstances of a given case of misconduct. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. n.5 (U.S. SENTENCING COMM'N 2016) ("[T]he form of discipline that will be appropriate will be case specific.").

TOPIC 5. INTERNAL REPORTING

TOPIC 6. THIRD-PARTY SERVICE PROVIDERS

TOPIC 7. INVESTIGATIONS

TOPIC 8. COMPLIANCE BEYOND THE ORGANIZATION

TOPIC 9. ETHICS AND SOCIAL RESPONSIBILITY

TOPIC 10. SPECIAL CONSIDERATIONS FOR NONPROFITS AND INTERNATIONAL FIRMS

APPENDIX
BLACK LETTER OF TENTATIVE DRAFT NO. 1

§ 1.01. Definitions

For purposes of these Principles, the terms set forth herein shall mean the following:

(a) Board of Directors. The individual or group exercising final authority over an organization's internal decisions.

(b) Chief Audit Officer. The head of an organization's internal-audit department.

(c) Chief Compliance Officer. The head of an organization's compliance department.

(d) Chief Executive Officer. The senior-most executive official in an organization.

(e) Chief Legal Officer. The head of an organization's legal department.

(f) Chief Risk Officer. The head of an organization's risk-management department.

(g) Code of Ethics. A written statement that embodies and formalizes the requirements and recommendations of an organization's ethical standards and its code of conduct.

(h) Compliance. Adherence to applicable laws, regulations, rules, or internal requirements.

(i) Compliance Function. The operations, offices, personnel, and activities within an organization that carry out its compliance responsibilities.

(j) Compliance Monitor. An independent third party responsible for assuring compliance with rules or regulations, or with the requirements of agreements settling civil or criminal enforcement actions.

(k) Compliance Officer. An employee working in a professional capacity within an organization's compliance department.

(l) Compliance Policies and Procedures. A statement approved by the board of directors that sets forth an organization's philosophy and general approach to compliance issues.

(m) Compliance Program. A set of specific rules, procedures, authorities, standards, practices, and requirements that implement the compliance policies and procedures within an organization.

(n) Compliance Risk. The risk that an organization will experience financial or reputational losses or legal sanctions or other negative consequences because of its unwillingness or failure to follow laws, regulations, its code of ethics, its ethical standards, or applicable industry codes of conduct, or to cooperate appropriately with regulators.

(o) Deferred Prosecution Agreement. [RESERVED]

(p) Deterrence. [RESERVED]

(q) Duty of Care. The duty to act on an informed and prudent basis with respect to the affairs of an organization.

(r) Duty of Loyalty. The duty not to act in one's own interest, or in the interest of another, to the detriment of the best interests of an organization.

(s) Enforcement Officials. Officials who bring enforcement actions on behalf of a government.

(t) Enterprise Risk Management. [RESERVED]

(u) Ethical Standards. The set of principles, grounded in concerns of morality or the public good, which an organization adopts and declares to be applicable to its employees or agents.

(v) Executive Management. The senior officers of an organization or some subset of such officers.

(w) External Control. A function performed by persons outside an organization that is designed to provide reasonable assurance regarding the achievement of objectives relating to compliance and risk management.

(x) First Line of Defense. An organization's operational managers.

(y) Governance. The process by which decisions relative to compliance and risk management are made within an organization.

(z) Governance Map. A specification assigning responsibility for internal control to persons within an organization.

(aa) Independent. Not part of or subject to the control of any other organization or office and not subject to any influence or conflict that would prevent an organizational actor from fulfilling his or her role on an organization's behalf.

(bb) Informant. A person who reports to an organization's officials about possible wrongful activities by an organization and its employees or agents.

(cc) Inherent Risk. [RESERVED]

(dd) Internal Audit. An internal assurance activity designed to assess whether operations or processes are functioning as designed and whether internal controls are operating effectively.

(ee) Internal-Audit Plan. The policies, procedures, and practices employed by an organization to carry out the task of internal audit.

(ff) Internal-Audit Function. The operations, offices, personnel, and activities within an organization that carry out the task of internal audit.

(gg) Internal Control. A process, implemented by an organization's board of directors, executive management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to compliance and risk management.

(hh) Internal-Control Officer. The chief legal officer, chief risk officer, chief compliance officer, chief audit officer, any of their subordinates, or any other employee charged with carrying out an internal-control function.

(ii) Knowledge. Substantial certainty about a particular fact or state of affairs. Knowledge can be inferred from the circumstances.

(jj) Mandate. A binding obligation imposed by a final judgment or settlement agreement in an enforcement action. [RESERVED]

(kk) Material. Significant, qualitatively or quantitatively, or both, to an organization's reputation, effective functioning, or financial position.

(ll) Misconduct. Any violation of a criminal statute, civil statute, regulation, or mandatory internal rule or standard.

(mm) Nonprosecution Agreement. [RESERVED]

(nn) Organization. A corporation, partnership, limited-liability company, limited-liability partnership, limited-liability limited partnership, professional corporation, business trust, nonprofit corporation, public-benefit corporation, charitable foundation, or other legally constituted entity.

(oo) Organizational Culture. The norms, assumptions, perspectives, and beliefs that guide and govern behavior within an organization.

(pp) Principles. These Principles of the Law, Compliance, Risk Management, and Enforcement.

(qq) Prosecutor. [RESERVED]

(rr) Regulator. [RESERVED]

(ss) Residual Risk. [RESERVED]

(tt) Risk Appetite. [RESERVED]

(uu) Risk-Appetite Statement. [RESERVED]

(vv) Risk Assessment. [RESERVED]

(ww) Risk Capacity. [RESERVED]

(xx) Risk Culture. [RESERVED]

(yy) Risk Limit. [RESERVED]

(zz) Risk Management. [RESERVED]

(aaa) Risk-Management Framework. [RESERVED]

(bbb) Risk-Management Function. [RESERVED]

(ccc) Risk-Management Program. [RESERVED]

(ddd) Risk Tolerance. Acceptable variation in performance, whether exceeding or falling short of the target business objective. [RESERVED]

(eee) Second Line of Defense. The offices and individuals within an organization charged with monitoring the first line of defense to ensure that its functions and processes are properly designed, in place, and operating as intended.

(fff) Third Line of Defense. Internal audit, an independent, objective assurance, and consulting activity designed to add value and improve an organization's operations.

(ggg) Tone. A publicly communicated set of values and norms, expressed in behaviors as well as words.

(hhh) Tone at the Top. The tone set by the board of directors and executive management as to an organization's ethical standards and guiding values.

(iii) Whistleblower. [RESERVED]

§ 2.01. Subject Matter

These Principles set forth recommendations of best practice for internal control within organizations and external control by regulators, prosecutors, and judges.

§ 2.02. Objectives

These Principles are intended to promote the following objectives:

(a) fostering compliant, ethical, and risk-aware conduct by organizations and their employees and agents; and

(b) enhancing the effectiveness of internal and external controls.

§ 2.03. Characteristics of the Organization

The application of these Principles depends on the facts and circumstances of the organization, which include the following factors, among others:

(a) size;

(b) legal form;

(c) complexity;

(d) geographic scope;

(e) the nature of its business or affairs;

(f) for-profit or not-for-profit status;

(g) history of its compliance violations;

(h) existing obligations arising from settlements of criminal, regulatory, or private enforcement proceedings against it and its employees or agents;

(i) the nature and extent of the regulations applicable to the organization and its business; and

(j) compliance and other risk factors peculiar to its industry or sector.

§ 2.04. Interpretation

These Principles should be interpreted in light of the objectives set forth in § 2.02 and the facts and circumstances of the organization listed in § 2.03.

§ 2.05. Nonliability

Unless otherwise specifically stated, no recommendation contained in these Principles should be considered as indicating that the law will or should impose liability for conduct that fails to conform to the recommendation.

§ 3.01. Governance in Compliance and Risk Management

Governance is essential to achieving effective compliance and risk management in an organization. Organizations should have flexibility in designing their compliance and risk-management governance.

§ 3.02. Governance Actors

The primary governance actors for compliance and risk management in an organization are its board of directors, executive management, and internal-control officers.

§ 3.03. Governance Map for Compliance and Risk Management

It is a best practice for an organization to establish a governance map for compliance and risk management.

§ 3.04. Coordination of Compliance and Risk Management in Affiliated Organizations

In a group of affiliated organizations, depending upon the structure of that group and legal and practical constraints, the parent organization or another affiliate may find it advisable to coordinate compliance and risk management for the group.

§ 3.05. Governance Accommodations for Organizational Circumstances

An organization should structure the governance of its internal-control functions of compliance, risk management, and internal audit to reflect its size, legal form, industry-specific requirements, nonprofit status, potential harm caused by a violation or a failure of, or deviation from, an internal-control program, or other circumstances.

§ 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.

§ 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.

§ 3.08. Board of Directors' Oversight of Compliance, Risk Management, and Internal Audit

(a) As part of its supervision of the organization's business or affairs, the board of directors must oversee the organization's compliance, risk-management, and internal-audit functions.

(b) The oversight in subsection (a) should include the following responsibilities:

(1) to be informed of the major legal obligations of, and the main values in the code of ethics for, the organization, its employees, and agents;

(2) to review and approve the organization's compliance program and code of ethics, any material revisions thereto, and their implementation;

(3) to be informed of the material risks to which the organization is or will likely be exposed;

(4) to review and approve the organization's risk-management framework and risk-management program, any material revisions thereto, and their implementation;

(5) to review and approve the internal-audit plan for compliance and risk management, and any material revisions thereto, and be reasonably informed of the results of the internal audit of these internal-control functions;

(6) to be reasonably informed of the staffing and resources allocated by executive management to the internal-control departments of compliance, risk management, and internal audit, and to satisfy itself that the staffing and resources are adequate and that the departments are sufficiently independent

and have the appropriate authority to perform their respective internal-control responsibilities;

(7) to approve the appointment, terms of employment, and dismissal of the chief compliance officer, the chief risk officer, and the chief audit officer;

(8) to communicate regularly with these internal-control officers;

(9) to meet at reasonable intervals with executive management and each of the appropriate internal-control officers to review the effectiveness of, inadequacies in, and any necessary changes to the internal-control function headed by that officer;

(10) to confer with executive management, the chief legal officer, and the appropriate internal-control officer or officers:

(A) to address any material violation or failure of the compliance program and code of ethics, material deviation from or failure of the risk-management program, or material failure in the internal audit of compliance and risk management, and

(B) to approve or ratify any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation, failure, or deviation; and

(11) with the assistance of the chief legal officer, the appropriate internal-control officer or officers, outside legal counsel, or outside consultants:

(A) to direct its own investigation of any material violation or failure of the compliance program and code of ethics, material deviation from or failure of the risk-management program, or material failure in the internal audit of compliance and risk management,

(B) to resolve upon any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such violation, failure, or deviation, and

(C) to direct executive management to develop a plan of action for responding to any future such violation, failure, or deviation.

(c) Subject to subsection (a) and if authorized under the law governing the organization, the board of directors, in its discretion, may delegate to a group or committee of its members, to a joint committee of directors and executives, or to executive management the power to perform one or more of the responsibilities set forth in subsection (b).

§ 3.09. Delegation of Oversight Responsibilities by the Board of Directors to a Committee or Group of its Members

(a) If the board of directors elects to delegate any of its oversight responsibilities under § 3.08 to a committee or group of its members, this committee or group should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority over them and to any reservation made by the board in the delegation.

(b) The members constituting any such committee or group should:

(1) be independent; and

(2) have the background or experience in compliance and risk management, as the case may be, to be able, individually and, when appropriate, collectively, to fulfill their delegated responsibilities.

(c) Any such committee or group should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's or group's judgment, such engagement is appropriate.

(d) Any such committee or group may elect to have a written charter specifying its purpose, duties, functions, structure, procedures, and member requirements or limitations.

(e) Any such committee or group should regularly report to the board of directors on the exercise of its delegated responsibilities.

§ 3.10. Compliance and Ethics Committee

(a) The board of directors, in its discretion, may elect to delegate to a compliance and ethics committee, or to another committee or committees, part or all of its oversight of compliance and ethics in the organization. This committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should:

(1) be independent; and

(2) have the background or experience in compliance and ethics to be able, individually and, when appropriate, collectively, to fulfill their delegated responsibilities.

(b) The compliance and ethics committee should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's judgment, such engagement is appropriate.

(c) The compliance and ethics committee may elect to operate with a written charter specifying the committee's purpose, responsibilities, functions, structure, procedures, and member requirements or limitations.

(d) The compliance and ethics committee's oversight in subsection (a) should include one or more of the following responsibilities:

(1) to be informed of the major legal obligations of, and the main values in the code of ethics for, the organization, its employees, and agents;

(2) to review and approve the compliance program and the code of ethics, any material revisions thereto, and their implementation;

(3) to be reasonably informed of the staffing and resources allocated by executive management to the compliance department and to satisfy itself that they are adequate and that the department is sufficiently independent and has the appropriate authority to perform its responsibilities;

(4) to approve the appointment, terms of employment, and dismissal of the chief compliance officer;

(5) to communicate regularly with the chief compliance officer;

(6) to meet at reasonable intervals with executive management and the chief compliance officer to review the effectiveness of, inadequacies in, and any necessary changes to the organization's compliance function;

(7) to confer with executive management, the chief compliance officer, and the chief legal officer:

(A) to address any material violation or failure of the compliance program or code of ethics, and

(B) to approve or ratify any material disciplinary or remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation or failure;

(8) to confer with executive management, the chief compliance officer, and the chief legal officer about:

(A) any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and code of ethics in ensuring compliance with them, and

(B) the adequacy of such disclosure or reporting;

(9) to confer with executive management or any other board committee to explore whether the organization's practices, particularly those involving compensation, are adequately aligned with the compliance program and the code of ethics;

(10) to receive and to respond to communications made pursuant to the organization's procedures for confidential internal reporting of a violation or failure of the compliance program and the code of ethics, and to meet at reasonable intervals with the chief legal officer and the chief compliance officer to review the effectiveness of, inadequacies in, and any necessary changes to these procedures;

(11) with the assistance of the chief legal officer, the chief compliance officer, outside legal counsel, or outside consultants, to direct its own investigation of any material violation or failure of the compliance program and the code of ethics, including any violation or failure communicated under the organization's procedures for confidential internal reporting; and

(12) to report regularly to the board of directors on the responsibilities delegated to it.

§ 3.11. Risk Committee

(a) The board of directors, in its discretion, may elect to (or, if required by law, must) delegate to a risk committee, or to another committee or committees, part or all of its oversight of risk management in the organization. This committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should:

(1) be independent; and

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

(b) The risk committee should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's judgment, such engagement is appropriate.

(c) The risk committee may elect to operate with a written charter specifying its purpose, duties, functions, structure, procedures, and member requirements or limitations.

(d) The risk committee's oversight in subsection (a) should include one or more of the following responsibilities:

(1) to be informed of the material risks to which the organization is or will likely be exposed;

(2) to review and approve the organization's risk-management framework and risk-management program, any material revisions thereto, and their implementation;

(3) to be reasonably informed of the staffing and resources allocated by executive management to the risk-management department and to satisfy itself that they are adequate and that the department is sufficiently independent and has the appropriate authority to perform its responsibilities;

(4) to approve the appointment, terms of employment, and dismissal of the chief risk officer;

(5) to communicate regularly with the chief risk officer;

(6) to meet at reasonable intervals with executive management and the chief risk officer to review the effectiveness of, inadequacies in, and any necessary changes to the organization's risk-management function;

(7) to confer with executive management, the chief legal officer, and the chief risk officer:

(A) to address any material deviation from or failure of the risk-management program, and

(B) to approve or ratify any material disciplinary or remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such deviation or failure;

(8) to confer with executive management, the chief legal officer, and the chief risk officer about:

(A) any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the material risks to which the organization is or may be exposed and the effectiveness of the risk-management program in addressing these risks, and

(B) the adequacy of such disclosure or reporting;

(9) to confer with executive management or any other board committee to explore whether the organization's practices, particularly those involving compensation, are adequately aligned with the risk-management framework;

(10) with the assistance of the chief legal officer, the chief risk officer, outside legal counsel, or outside consultants, to direct its own investigation of any material deviation from or failure of the risk-management program; and

(11) to report regularly to the board of directors on the responsibilities delegated to it.

§ 3.12. Role of the Audit Committee in Compliance and Risk Management

(a) The board of directors, in its discretion, may elect to delegate to an audit committee, or to another committee or committees, part or all of its oversight of the internal audit of compliance and risk management in the organization. The committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should be:

(1) independent; and

(2) have the background or experience in internal audit to be able, individually and, when appropriate, collectively, to fulfill their delegated responsibilities.

(b) The audit committee should be reasonably satisfied that, given the organization's circumstances, it has adequate resources to carry out its delegated responsibilities, including funds to engage its own legal counsel and other advisors and consultants when, in the committee's judgment, such engagement is appropriate.

(c) The audit committee may elect to operate with a written charter specifying the committee's purpose, responsibilities, functions, structure, procedures, and member requirements or limitations.

(d) The audit committee's oversight in subsection (a) should include one or more of the following responsibilities:

(1) to review and approve the internal-audit plan for compliance and risk management, and any material revisions thereto;

(2) to be reasonably informed of the staffing and resources allocated by executive management to the internal-audit department and to satisfy itself that they are adequate and that the department is sufficiently independent and has the appropriate authority to perform its responsibilities;

(3) to approve the appointment, terms of employment, and dismissal of the chief audit officer;

(4) to communicate regularly with the chief audit officer on the organization's internal-control environment, including its compliance and risk management;

(5) to meet at reasonable intervals with executive management and the chief audit officer to review the effectiveness of, inadequacies in, and any necessary changes to the organization's internal-audit function;

(6) to confer with executive management, the chief legal officer, and the chief audit officer:

(A) to address any material failure in the internal audit of compliance and risk management, and

(B) to approve or ratify any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such failure;

(7) to review, in consultation with the chief audit officer and, if applicable, the external auditor, the results of the internal audit and, if applicable, those of the external audit, as both pertain to compliance and risk management, and, in light of that review:

(A) to consider the effectiveness of and inadequacies in the organization's compliance program, code of ethics, and risk-management framework and program, and any necessary changes to them, and

(B) to evaluate any material violation or failure of the compliance program and the code of ethics, material deviation from or

failure of the risk-management framework and program, or material failure in the internal audit of compliance and risk management that the internal or external audit revealed, and the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization as it pertains to compliance and risk management;

(8) to meet with executive management, the chief compliance officer, the chief risk officer, the compliance and ethics committee, the risk committee, or any other board committee that is concerned with compliance and risk management to discuss any conclusions at which it arrived from the processes stated in subsection (d)(7);

(9) with the assistance of the chief legal officer, the chief audit officer, outside legal counsel, or outside consultants, to direct its own investigation of any material failure of the internal audit;

(10) to perform the responsibilities of the compliance and ethics committee and the risk committee, as provided in §§ 3.10 and 3.11, if the board elects to delegate those responsibilities to the audit committee; and

(11) to report regularly to the board of directors on the responsibilities delegated to it.

§ 3.13. The Role of the Compensation Committee in Compliance and Risk Management

(a) If the board of directors elects to establish a compensation committee, that committee should consult periodically with any other committee of the board of directors having oversight of compliance and risk management:

(1) to consider its views as to whether the organization's compensation policies and practices under the purview of the compensation committee adequately support or undermine the organization's compliance program, code of ethics, and risk-management framework and program; and

(2) to discuss with it how these policies and practices should be revised to provide this support if the other committee believes that such revision is appropriate.

(b) The compensation committee should also report regularly to the board of directors on the revisions to the organization's compensation policies and practices that result from this consultation.

§ 3.14. Executive Management of Compliance and Risk Management

(a) As part of its management of the organization's business or affairs, executive management should direct the implementation of effective compliance, risk management, and internal audit in the organization.

(b) Specifically, the responsibilities of executive management under subsection (a) should include the following:

(1) to be informed of the major legal obligations applicable to, and the main values in the code of ethics for, the organization, its employees, and agents;

(2) in collaboration with, among others, the organization's chief compliance officer, to direct the formulation and implementation of the compliance program and the code of ethics, and any material revisions thereto;

(3) to be informed of the material risks to which the organization is or will likely be exposed;

(4) in collaboration with, among others, the organization's chief risk officer, to direct the formulation and implementation of the risk-management framework and risk-management program, and any material revisions thereto;

(5) to provide support to the chief audit officer who implements an internal-audit plan for compliance and risk management, and any material revisions thereto, and to be informed of the results of the internal audit of these internal-control functions;

(6) to ensure that the internal-control departments of compliance, risk management, and internal audit are adequately staffed, have adequate resources, are sufficiently independent, and have the appropriate authority to perform their respective internal-control responsibilities;

(7) subject to the approval of the board of directors, or a board committee, to appoint and dismiss, and to determine the terms of employment of, the chief compliance officer, the chief risk officer, and the chief audit officer;

(8) to communicate regularly with these internal-control officers;

(9) to meet at reasonable intervals with each of these internal-control officers to assess the effectiveness of and to identify inadequacies in the internal-control function headed by that officer, and to authorize, and to direct the implementation of, any necessary changes to it;

(10) to confer with the chief legal officer and the appropriate internal-control officer:

(A) to learn about any material violation or failure of the compliance program or the code of ethics, any material deviation from or failure of the risk-management program, or any material failure of the internal audit of compliance and risk management, and

(B) to resolve upon any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such violation, failure, or deviation; and

(11) accompanied by the appropriate internal-control officer, to meet with the board of directors, or a board committee:

(A) to obtain its approval for the compliance program and the code of ethics, the risk-management framework and risk-management program, and the internal-audit plan for compliance and risk management, and any material revisions thereto,

(B) to report on their implementation,

(C) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the internal-control function headed by the accompanying internal-control officer,

(D) to notify it of any material violation or failure of the compliance program or code of ethics, any material deviation from or failure of the risk-management program, or any material failure of the internal audit of compliance and risk management, and to propose for approval or to identify for ratification any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation, failure, or deviation, and

(E) to confer about any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them, or the material risks to which the organization is or may be exposed and the effectiveness of the risk-management program in addressing them, and the adequacy of such disclosure or reporting.

§ 3.15. Chief Compliance Officer

(a) An organization should elect to have a chief compliance officer ("CCO") who is responsible for the compliance function and, if feasible, does not have other operational responsibilities.

(b) The CCO's responsibilities should include the following:

(1) for the purposes of formulating, implementing, and testing the organization's compliance program and code of ethics:

(A) to be well informed of the legal obligations applicable to, and the values in the code of ethics for, the organization, its employees, and agents,

(B) together with compliance officers and as directed by executive management, to conduct a compliance-risk assessment, and to formulate and implement the compliance program and the code of ethics, and any revisions thereto, in response to that assessment, and

(C) to oversee compliance officers' regular testing and reassessment of the compliance program and the code of ethics for effectiveness and inadequacies;

(2) to manage the compliance department, which includes making recommendations to executive management about its staffing and resources, and to decide upon the hiring, dismissal, compensation, work conditions, placement within the organization, and reporting lines of compliance officers and other compliance personnel;

(3) to oversee communication about the compliance program and the code of ethics throughout the organization and the compliance training conducted for the board of directors, executive management, employees, and agents;

(4) to advise the board of directors, any board committee, executive management, and other organizational actors about whether a course of action, transaction, practice, or other organizational matter complies with the compliance program and the code of ethics, and to oversee compliance officers' provision of compliance advice in the organization;

(5) for the purposes of monitoring compliance with the compliance program and the code of ethics, administering confidential internal reporting and investigating violations:

(A) to initiate and oversee the monitoring done by compliance officers to ensure that the organization, its employees, and agents follow the compliance program and the code of ethics, and, if delegated these responsibilities under the compliance program,

(B) to administer the organization's procedures for confidential internal reporting of violations of the compliance program and the code of ethics, and

(C) in consultation with the chief legal officer, to direct the investigation of any actual or potential violation of the program and the code detected by the monitoring or by the procedures for confidential internal reporting and to report the results of the investigation to the appropriate organizational actor;

(6) to be the organization's liaison with regulators on its compliance program and code of ethics;

(7) to communicate regularly with the board of directors, any board committee responsible for compliance oversight, and executive management about the compliance program and the code of ethics;

(8) to meet at reasonable intervals with executive management to report on the effectiveness of and inadequacies in the compliance function and to recommend any necessary changes;

(9) to confer with executive management:

(A) to notify it of any material violation or failure of the compliance program or the code of ethics, and

(B) to recommend any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such violation or failure; and

(10) to accompany executive management to meet with the board of directors, or a board committee responsible for compliance oversight, or to meet outside the presence of executive management at the request of the board or its committee, or at the CCO's own request, for the following purposes:

(A) to obtain its approval for the compliance program and the code of ethics, and any material revisions thereto,

(B) to report on their implementation,

(C) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the compliance function,

(D) to notify it of any material violation or failure of the compliance program or the code of ethics and to propose for approval or to identify for ratification any material disciplinary and remedial

measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation or failure, and

(E) to confer about any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them, and the adequacy of such disclosure or reporting.

§ 3.16. Chief Risk Officer

(a) An organization should elect to have a chief risk officer ("CRO") who is responsible for the risk-management function and, if feasible, does not have other operational responsibilities.

(b) The CRO's responsibilities should include the following:

(1) for the purposes of formulating, implementing, and testing the organization's risk-management framework and risk-management program:

(A) to be well informed of the material risks (other than legal and compliance risks, of which the CRO should be reasonably informed) to which the organization is or will likely be exposed,

(B) together with risk officers and as directed by executive management, to conduct a risk assessment and to formulate and implement the risk-management framework and risk-management program, and any revisions thereto, in response to that assessment, and

(C) to oversee risk officers' regular testing and reassessment of the framework and program;

(2) to manage the risk-management department, which includes making recommendations to executive management about its staffing and resources, and to decide upon the hiring, dismissal, compensation, work conditions, placement within the organization, and reporting lines of risk officers and other risk-management personnel;

(3) to oversee communication about the risk-management framework and program throughout the organization and the risk-management training conducted for the board of directors, executive management, employees, and agents;

(4) to advise the board of directors, any board committee, executive management, and other organizational actors about whether an organization's course of action, transaction, practices, including those involving employee compensation, or other organizational matters comply and are adequately aligned with the risk-management framework and program, and to oversee risk officers' provision of risk-management advice in the organization;

(5) for the purpose of monitoring compliance with the risk-management program and investigating deviations or failures:

(A) to initiate and oversee the monitoring done by risk officers to ensure that the organization, its employees, and agents follow the risk-management program and to identify and assess new risks, and

(B) if delegated this task under the risk-management program, in consultation with the chief legal officer, to oversee the investigation of any actual or potential deviations from or failures in the program detected by the monitoring and to report the results of the investigation to the appropriate organizational actor;

(6) to be the organization's liaison with regulators on its risk-management program;

(7) to communicate regularly with the board of directors, any board committee responsible for risk oversight, and executive management about the risk-management program;

(8) to meet at reasonable intervals with executive management to report on the effectiveness of and inadequacies in the risk-management function and to recommend any necessary changes;

(9) to confer with executive management:

(A) to notify it of any material deviation from or failure of the risk-management program, and

(B) to recommend any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such deviation or failure; and

(10) to accompany executive management to meet with the board of directors, or a board committee responsible for risk-management oversight, or to meet outside the presence of executive management at the request of the board or its committee, or at the CRO's request, for the following purposes:

(A) to obtain its approval for the risk-management framework and program, and any material revisions thereto,

(B) to report on their implementation,

(C) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the risk-management function,

(D) to notify it of any material deviation from or failure of the risk-management program and to propose for approval or to identify for ratification any material disciplinary and remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such deviation or failure, and

(E) to confer about any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the material risks to which the organization is or may be exposed and the effectiveness of the risk-management program in addressing them, and the adequacy of such disclosure or reporting.

§ 3.17. Chief Audit Officer

(a) An organization should have a chief audit officer ("CAO") who is responsible for the internal-audit function and does not have other operational responsibilities.

(b) The CAO's compliance and risk-management responsibilities should include the following:

(1) for the purposes of formulating, implementing, and testing the organization's internal-audit plan:

(A) to be informed of the major legal obligations applicable to, and the main values in the code of ethics for, the organization, its employees, and agents and of the material risks to which the organization is or will be exposed,

(B) together with internal auditors and with the support of executive management, to formulate and implement an internal-audit plan that includes compliance and risk management within its assessment of the organization's internal-control environment, and any revisions to that plan, and

(C) to oversee internal auditors' regular testing and reassessment of the plan;

(2) to manage the internal-audit department, which includes making recommendations to executive management about its staffing and resources, and to decide upon the hiring, dismissal, compensation, work conditions, placement within the organization, and reporting lines of the internal auditors and other internal-audit personnel;

(3) to be the organization's liaison with regulators on its internal audit;

(4) to communicate regularly with the board of directors, the board audit committee, any other board committee responsible for compliance or risk-management oversight, and executive management about the internal-control environment for compliance and risk management;

(5) to meet at reasonable intervals with executive management to report on the effectiveness of and inadequacies in the internal-audit function,

including the internal-audit plan for compliance and risk management, and to seek approval for any material modifications;

(6) to confer with executive management:

(A) to notify it of any material failure of the internal audit of compliance and risk management, and

(B) to recommend any material disciplinary and remedial measures that will be taken, including any reporting to a regulator that will be made, in response to such failure;

(7) to confer with executive management and, when appropriate, the chief compliance officer and the chief risk officer:

(A) to report on the results of the internal audit of compliance and risk management, particularly on the effectiveness of and inadequacies in the compliance function and the risk-management function, and to recommend any necessary changes,

(B) to notify them of any material violation or failure of the compliance program and the code of ethics and of any material deviation from or failure of the risk-management framework and program that the internal audit revealed,

(C) to identify the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization for compliance or risk management, and

(D) to recommend remedial measures to address such cause or causes; and

(8) to accompany executive management to meet with the board of directors, the board audit committee, or any other board committee responsible for compliance or risk-management oversight, or to meet outside the presence of executive management at the request of the board or its committee, or at the CAO's request, for the following purposes:

(A) to obtain its approval for the internal-audit plan for compliance and risk management, and any material revisions,

(B) at reasonable intervals to report on the effectiveness of, inadequacies in, and any necessary changes to the internal-audit function, including the internal-audit plan for compliance and risk management,

(C) to notify it of any material failure of the internal audit of compliance and risk management, and to propose for approval or to identify for ratification any material disciplinary or remedial measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such failure,

(D) to report on the implementation and the results of the internal audit of compliance and risk management, particularly on the effectiveness of and inadequacies in the compliance function and the risk-management function, and to recommend any necessary changes, and to provide assurance on the internal-control environment of the organization for compliance and risk management, and

(E) to notify it of any material violation or failure of the compliance program and the code of ethics and of any material deviation from or failure of the risk-management framework and program that the internal audit revealed, to identify the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization for compliance and risk management, and to recommend remedial measures to address such cause or causes.

§ 3.18. Compliance and Risk-Management Responsibilities of Chief Legal Officer

(a) An organization should have a chief legal officer ("CLO") who is primarily responsible for all legal advice to organizational actors.

(b) The CLO should have the following compliance and risk-management responsibilities:

(1) to provide advice on a regular basis and as requested to the board of directors, any board committee, executive management, and internal-

control officers with respect to the legal obligations of the organization, its employees, and agents, the risks arising from noncompliance with them, and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them;

(2) to advise the board of directors, any board committee, executive management, and the appropriate internal-control officer about:

(A) any mandatory or discretionary public disclosure of, or any mandatory or discretionary reporting to a regulator relating to, the major legal obligations and ethical standards of the organization, its employees, and agents and the effectiveness of the compliance program and the code of ethics in ensuring compliance with them, and the material risks to which the organization is or may be exposed and the effectiveness of the risk-management framework and program in addressing them, and

(B) the adequacy of such disclosure or reporting; and

(3) unless otherwise directed by the board:

(A) to advise the board of directors, any board committee, executive management, and the appropriate internal-control officer on, and to conduct the investigation of, any material violation or failure of the compliance program or the code of ethics, any material deviation from or failure of the risk-management program, or any material failure of the internal audit, and

(B) to advise them on any remedial or disciplinary measures that will be or have been taken, including any reporting to a regulator that will be or has been made, in response to such violation, failure, or deviation.

§ 3.19. Compliance and Risk-Management Responsibilities of the Human-Resources Officer

(a) An organization may elect to have a human-resources officer ("HRO") who is responsible for the human-resources function and, if feasible, does not have other operational responsibilities.

(b) The HRO's compliance and risk-management responsibilities should include the following:

(1) in collaboration with the chief compliance officer, chief legal officer, and chief risk officer and directed by executive management, to formulate policies and procedures that support the compliance program, the code of ethics, and the risk-management framework and program of the organization, for:

(A) the hiring, retention, compensation, performance evaluation, and promotion of employees, including conducting background checks and related personnel testing, and

(B) the status of employees under investigation and the discipline of employees, including their suspension or termination;

(2) to advise executive management, the chief compliance officer, chief legal officer, and chief risk officer on the implications of personnel decisions resulting from employees' violations of the compliance program and the code of ethics and their deviations from the risk-management program;

(3) to administer the organization's policies and procedures for nonretaliation against employees who use the organization's procedures for confidential internal reporting and to report any evidence of retaliation to the appropriate organizational actor; and

(4) to report to the chief compliance officer and the chief legal officer any actual or potential violation of employment-related law and regulation and of the organization's code of ethics and, if delegated this task, in consultation with the chief legal officer, to oversee the investigation of such violation and to report the results of the investigation to the appropriate organizational actor.

§ 3.20. Multiple Responsibilities of Internal-Control Officers

(a) Because of its size, operations, or resources, or because of other circumstances and if permitted by law, an organization may elect to have an internal-control officer be responsible for multiple internal-control functions or for non-internal-control operations.

(b) If subsection (a) applies, the organization should put in place safeguards to ensure the effectiveness of the internal-control officer, including the following:

(1) Executive management concludes that the internal-control officer can effectively execute the multiple responsibilities assigned;

(2) The internal-control officer is not given operational or other responsibilities that would create a disabling conflict of interest that would undermine the officer's effective accomplishment of the internal-control responsibilities; and

(3) There are in place organizational procedures to deal with any conflicts of interest (other than those disabling ones that would be excluded under subparagraph (2) above) that would arise from the assignment of multiple responsibilities to the internal-control officer.

§ 3.21. Outsourcing, Use of Technology, and Engagement of Third-Party Service Providers

(a) Because of its size, operations, or resources, or because of other circumstances and if permitted by law, an organization may outsource an internal-control function to a third party. The organizational actor who has direct responsibility for the internal-control function that is being outsourced and who approves the outsourcing remains responsible for it.

(b) If permitted by law, an internal-control officer may use technology and engage professionals, consultants, or other third-party service providers to perform, or to assist in, the responsibilities of the internal-control function overseen by that officer, including evaluating the adequacy and effectiveness of the function.

(c) When subsection (b) applies:

(1) the internal-control officer remains responsible for the internal-control function; and

(2) policies and procedures should provide that the internal-control officer shall evaluate and regularly reassess the effectiveness of the technology and shall supervise the performance of any professional, consultant, or other third-party service provider to whom an internal-control responsibility has been delegated.

§ 5.01. Nature of the Compliance Function

The compliance function is the set of operations, offices, personnel, and activities within the organization that carry out its compliance responsibilities.

§ 5.02. Goals of the Compliance Function

Goals of the compliance function include the following:

(a) providing input on the effective strategic management of the organization;

(b) deterring misconduct by employees, agents, or others whose actions can be attributed to the organization;

(c) enforcing the organization's code of ethics;

(d) investigating and identifying violations of the law;

(e) establishing and maintaining a culture of ethics and compliance within the organization; and

(f) lowering the organization's expenses by preventing legal violations in a cost-effective manner.

§ 5.03. General Compliance Activities of Organizations

An organization should do the following with respect to compliance:

(a) undertake reasonable measures to ensure that employees and agents comply with the requirements of the law and applicable norms when acting on behalf of the organization;

(b) conduct appropriate investigations when made aware of credible evidence of significant violations of law or of the organization's compliance policy or code of ethics;

(c) undertake reasonable remedial measures to correct identified violations;

(d) be honest and candid towards regulators, prosecutors, and other responsible government officials, both in required reporting and in discretionary communications; and

(e) preserve books, records, and other information pertinent to potential legal violations, except pursuant to general, previously announced, legally authorized, and consistently performed document disposal and retention policies.

§ 5.04. Enterprise Compliance

Subject to § 2.03, the compliance function should be supervised or managed on an enterprise-wide basis.

§ 5.05. Elements of an Effective Compliance Function

Elements of an effective compliance function include:

(a) a compliance program;

(b) support and oversight from the organization's board of directors;

(c) effective management;

(d) adequate funding, staffing, and other resources;

(e) incentives for compliant behavior; and

(f) procedures for independent validation.

§ 5.06. Compliance Program

The organization's compliance program should be reasonably designed to prevent and detect violations of internal and external laws and norms. It should:

(a) be governed by written rules and procedures approved by the board of directors;

(b) be informed by an assessment of risk to the organization;

(c) be based at least in part on underlying principles rather than standardized procedures;

(d) assign responsibility for compliance within the organization;

(e) be impartially and fairly administered;

(f) provide reliable and timely advice to employees regarding their compliance obligations;

(g) be effectively communicated to affected employees;

(h) include appropriate compliance training for employees, agents, and members of the board of directors;

(i) include procedures for internal reporting of violations;

(j) include procedures for monitoring employee conduct;

(k) include procedures for investigating violations;

(l) include procedures for disciplining violations;

(m) create appropriate incentives for compliant behavior and disincentives for violations;

(n) be regularly assessed for effectiveness and updated as necessary; and

(o) be periodically reviewed and reaffirmed by the organization's senior executives and board of directors.

§ 5.07. Compliance Risk Assessment

(a) When deciding how to allocate resources provided for the compliance function, the chief compliance officer should undertake a compliance risk assessment.

(b) Depending on the facts and circumstances, factors relevant to the compliance risk assessment may include:

(1) the nature of the organization's business;

(2) the industry's history of violations;

(3) the organization's history of violations;

(4) compensation arrangements for executives and employees;

(5) whether the organization has introduced a new product line or entered into a new business activity;

(6) whether there has been a change in applicable laws;

(7) whether internal controls are subject to manual override;

(8) the extent of the organization's foreign activities;

(9) the organization's exposure to compliance violations by agents, vendors, customers, or supply-chain counterparties;

(10) regulatory enforcement priorities; and

(11) the probable impact of compliance violations on the organization's reputation.

(c) Any risk assessment performed pursuant to subsection (a) should, if feasible and appropriate, be:

(1) in writing;

(2) evaluated both in terms of the absolute level and the trend of compliance risk; and

(3) reviewed and, if advisable, revised on a periodic basis and be subject to revision as new risks become apparent or old ones subside.

(d) In performing the risk assessment pursuant to subsection (a), the chief compliance officer should make an independent judgment about the compliance risks facing the organization but should also take account of the views of others within the organization, particularly the chief legal officer.

§ 5.08. Compliance Advice

(a) The compliance function should stand ready to provide advice to employees and agents on how to behave in a compliant and ethical way.

(b) The advice described in subsection (a) may be provided by a compliance officer, a legal officer, or some other appropriate person. The identity of the person providing such advice and the mechanism through which it is provided depend on the facts and circumstances.

(c) Employees or agents who rely on such advice in good faith should be protected against retaliation or punishment by the organization if the advice given proves to be mistaken.

§ 5.09. Compliance Monitoring [RESERVED]

§ 5.10. Training and Education

(a) The compliance function should include training and other educational activities regarding the compliance obligations of the organization and its employees and agents.

(b) The compliance function should make appropriate compliance training available to all employees. Compliance training should include advising the board of directors and senior managers on applicable laws, rules, and standards.

(c) The appropriate form of training depends on the facts and circumstances surrounding each organization, including its size, its complexity, the nature of the business line's activity, the compliance risk posed, the level of sophistication and experience of the employees involved, and the legal requirements for training of personnel.

§ 5.11. Red Flags

(a) The compliance function should be alert to red flags of potential violations. Depending on the facts and circumstances, red flags can include but are not limited to:

(1) transactions with no apparent business purpose;

(2) sudden material changes in performance that cannot be explained by known causes;

(3) excessively complex structures;

(4) frequent failures to complete required paperwork;

(5) efforts to disguise the identity of customers or other counterparties;

(6) gifts or favors to customers or business partners, or family members of customers or business partners, that appear excessive in light of the customs of the industry;

(7) gifts or favors to government officials or to family members of government officials;

(8) unusual and persistent failures to take allowed vacations or time off; and

(9) unauthorized self-dealing or other conflicted activities by employees and agents.

(b) The presence of a red flag does not indicate that a violation has occurred.

(c) A compliance officer who knows of a red flag of a violation should undertake appropriate responsive actions.

§ 5.12. Escalation Within the Organization

(a) If a compliance officer knows that an employee or agent has engaged, or intends to engage, in illegal conduct or other impermissible activity that poses a significant risk to the organization or a third party if not corrected or remediated, he or she should act as reasonably necessary in the best interests of the organization.

(b) If the matter cannot be addressed in a timely manner within the scope of his or her authority, the chief compliance officer should refer the issue to an official who has the power to address the matter, including, when appropriate, the board of directors. Reporting up is not required if the effort would clearly be futile due to potential involvement in misconduct by higher level officials.

(c) If after undertaking the actions described in subsection (b), the chief compliance officer in good faith believes that the matter will not be satisfactorily addressed in an appropriate time within the organization and that the failure to address the matter poses a material threat to the organization's financial position or strategic objectives or to third parties, he or she may disclose the concerns to an appropriate government regulator.

§ 5.13. Compliance Under Legal Uncertainty

(a) Unless the organization's rules of governance otherwise provide, the chief compliance officer is not responsible for resolving uncertainty in applicable rules or regulations.

(b) If the chief compliance officer deems it important to resolve a legal uncertainty in order to perform his or her responsibilities, he or she should ordinarily

seek guidance from the chief legal officer or another qualified attorney. If such guidance is not available, the chief compliance officer should apply the most reasonable interpretation.

§ 5.14. Hiring of Employees, Retention of Agents, and Selection of Counterparties

(a) Unless otherwise indicated by the circumstances, the official charged with hiring employees or retaining agents should consider a candidate's background and history of compliance with applicable laws, regulations, and ethical norms. Candidates deemed to present an unacceptable risk of violations should not be hired or retained.

(b) The official tasked with selecting a vendor or supplier, or engaging in a transaction with a customer, should take into consideration the risk that misconduct by that vendor, supplier, or customer will be attributed to or otherwise result in harm to the organization. Prospective vendors, suppliers, or customers should not be dealt with if they present an unacceptable risk of misconduct that will result in harm to the organization.

§ 5.15. Background Checks

In carrying out the activities contemplated in § 5.14, an organization may engage in background checks of potential employees, agents, or counterparties. Such background checks must comport with applicable legal restrictions, must not result in invidious discrimination, should be appropriate for the position in question, and should avoid intruding unnecessarily on reasonable expectations of privacy.

§ 5.16. Compensation

(a) An employee's record of compliant or noncompliant behavior should be considered as a factor in setting his or her compensation.

(b) Bonuses and other nonsalary compensation for employees in a compliance function should be independent of the performance of any business line overseen by the employee and should be based in substantial part on the achievement of compliance-based objectives.

§ 5.17. Discipline

(a) In addition to setting compensation practices to incentivize compliant behavior, organizations should consider imposing nonmonetary discipline for violations.

(b) As in the case of monetary sanctions, the form of nonmonetary discipline should be commensurate with the gravity of the offense and consistent with the organization's stated policies and procedures.

(c) Nonmonetary sanctions should be based on clearly expressed and widely disseminated norms of conduct and should be administered within the organization on an evenhanded basis.

(d) The organization's decision whether to report misconduct should depend on the facts and circumstances, including the gravity of the offense, whether third parties have been harmed by the misconduct, the likelihood of recidivism, the probable response of regulators, and fairness to parties involved.