Submitted by the Council to the membership of
The American Law Institute
for consideration at the 2021 Annual Meeting on May 17-18 and June 7-8, 2021.

THE AMERICAN LAW INSTITUTE

Principles of the Law
Compliance and Enforcement for Organizations

Tentative Draft No. 2

(April 23, 2021)

SUBJECTS COVERED

The Executive Office
The American Law Institute
4025 Chestnut Street
Philadelphia, PA 19104-3099
Telephone: (215) 243-1626 • Fax: (215) 243-1636
E-mail: ali@ali.org • Website: http://www.ali.org

As of the date on its cover, this draft had not been considered by the membership of The American Law Institute and therefore may not represent the position of the Institute on any of the issues with which it deals. Any action taken by the membership with respect to this draft may be ascertained by consulting the ALI website or the Proceedings of the Annual Meeting.

The American Law Institute

Principles of the Law
Compliance and Enforcement

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
Vanderbilt Hall # 411G
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
Vanderbilt Hall # 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
Mondale Hall # 418
Minneapolis, MN 55455-0400
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 and Enforcement for Organizations

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

KATHERINE L. ADAMS, Apple Inc., Cupertino, CA
DANIEL ALTER, New York State Department of Financial Services, Mount Vernon, NY
MIRIAM H. BAER, Brooklyn Law School, Brooklyn, NY
JEFF BENJAMIN, Avon Products Inc. (retired), New York, NY
JOHN THEODORE BOESE, Fried, Frank, Harris, Shriver & Jacobson, Washington, DC
LESLIE R. CALDWELL, Latham & Watkins, San Francisco, CA
GEORGE S. CANELLOS, Milbank, New York, NY
SABINE ANNA CHALMERS, BT Group, London, England
STEPHEN M. CUTLER, Simpson Thacher & Bartlett, New York, NY
LEE G. DUNST, Gibson Dunn, New York, NY
PAUL L. FRIEDMAN, U.S. District Court, District of Columbia, Washington, DC
STACEY PUTNAM GEIS, Earthjustice, San Francisco, CA
JOHN GLEESON, Debevoise & Plimpton, New York, NY
COURT GOLUMBIC, Goldman Sachs & Co., New York, NY
SEAN J. GRIFFITH, Fordham University School of Law, New York, NY
YANNICK HAUSMANN, Zurich Insurance Group Ltd., Zurich, Switzerland
MICHAEL HELD, Federal Reserve Bank of New York, New York, NY
ANDREW D. HENDRY, Pinehurst, NC
ANDREW HINTON, Google, Mountain View, CA
JACK B. JACOBS, Young, Conaway, Stargatt & Taylor, Wilmington, DE
ERIKA A. KELTON, Phillips & Cohen, Washington, DC
JEFFREY H. KNOX, Simpson Thacher & Bartlett, Washington, DC
WILLIAM E. KOVACIC, George Washington University School of Law, Washington, DC
JULES B. KROLL, K2 Intelligence, New York, NY
IRIS LAN, Washington, DC
DONALD C. LANGEVOORT, Georgetown University Law Center, Washington, DC
DOUGLAS M. LANKLER, Pfizer Inc., New York, NY
DAVID G. LEITCH, Bank of America, Charlotte, NC
LEWIS J. LIMAN, U.S. District Court, Southern District of New York, New York, NY
MARTIN LIPTON, Wachtell, Lipton, Rosen & Katz, New York, NY
RAYMOND J. LOHIER, JR., U.S. Court of Appeals, Second Circuit, New York, NY
LORI A. MARTIN, WilmerHale, New York, NY
JAMES MCDONALD, U.S. Commodity Futures Trading Commission, Division of Enforcement, Washington, DC
DENIS J. MCINERNEY, Davis Polk & Wardwell, New York, NY
JUDITH A. MILLER, Chevy Chase, MD
DOUGLAS K. MOLL, University of Houston Law Center, Houston, TX
ROBERT H. MUNDHEIM, Shearman & Sterling, New York, NY
BRIAN E. NELSON, LA 2028, Los Angeles, CA

ERNEST PATRIKIS, Industrial and Commercial Bank of China, New York, NY
JED S. RAKOFF, U.S. District Court, Southern District of New York, New York, NY
MYTHILI RAMAN, Covington & Burling, Washington, DC
KATHRYN S. REIMANN, Citigroup Inc. (retired), New York, NY
DOUGLAS R. RICHMOND, Aon Professional Services, Kansas City, MO
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
LAUREEN E. SEEGER, American Express, New York, NY
CHARLES V. SENATORE, Fidelity Digital Asset Services, Boston, MA
KAREN PATTON SEYMOUR, Sullivan & Cromwell, New York, NY
KENNETH S. SIEGEL, Senestech, Phoenix, AZ
NEAL R. SONNETT, Neal R. Sonnett, P.A., Miami, FL
LAURA STEIN, Mondelez International, Lafayette, 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 and Enforcement for Organizations
(as of April 22, 2021)

JERRY L. ANDERSON, Des Moines, IA
JOSÉ F. ANDERSON, Baltimore, MD
CHRISTOPHER EDWARD APPEL, Washington, DC
JOHN B. ATTANASIO, Irving, TX
MICHAEL F. AYLWARD, Boston, MA
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, Austin, 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, Phoenix, AZ
JOHN G. BUCHANAN III, Washington, DC
JOHN P. BURTON, Santa Fe, NM
GREGORY P. BUTRUS, Birmingham, AL
IVONNE CABRERA, Downers Grove, IL
FABRIZIO CAFAGGI, Florence, Italy
J. WILLIAM CALLISON, Denver, CO
RUEBEN C. CÁSAREZ, 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
PENELOPE L. CHRISTOPHOROU, New York, NY
KATHLEEN CLARK, Washington, DC
ANNE E. COHEN, New York, NY
DAVID A. COLLINS, Chicago, IL
PAMELA CRAVEN, New York, NY
ROBERT A. CREAMER, Cambridge, MA
THOMAS L. CUBBAGE III, Plano, TX
CHRISTOPHER SCOTT D'ANGELO, Philadelphia, PA
ALICIA J. DAVIS, Ann Arbor, MI
KIMBERLY A. DEMARCHI, Tempe, AZ
BRACKETT B. DENNISTON III, Boston, MA
MELANIE DIPIETRO, Greensburg, PA
ANTHONY E. DIRESTA, Washington, DC
ALYSSA A. DIRUSSO, Birmingham, AL
TOBIAS A. DORSEY, Silver Spring, MD
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
ROGER A. FAIRFAX JR., Washington, DC
BORIS FELDMAN, Palo Alto, CA
JEAN K. FITZSIMON, Philadelphia, PA
JOSEPH Z. FLEMING, Miami, FL
IVAN K. FONG, Saint Paul, MN
SUSAN S. FORTNEY, Fort Worth, TX
ANNE C. FOSTER, Wilmington, DE
C. ALLEN FOSTER, Washington, DC
VERNON L. FRANCIS, Philadelphia, PA
TAMAR FRANKEL, Boston, MA
MEREDITH FUCHS, Washington, DC
THOMAS P. GALLANIS, Iowa City, IA
BRANDON L. GARRETT, Durham, NC
CAROL ROSE GOFORTH, Fayetteville, AR
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, Chicago, IL
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
CHRISTINA MICHELLE HOUSTON, Wilmington, DE

JOHN E. IOLE, Pittsburgh, PA
MELISSA B. JACOBY, Chapel Hill, NC
KRISTIN N. JOHNSON, Atlanta, GA
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, Arlington, VA
DAVID N. KRAGSETH, Philadelphia, PA
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
SYBIL H. LANDAU, New York, NY
STEWART M. LANDEFELD, Seattle, WA
PAUL A. LEBEL, Williamsburg, VA
JOHN LINARELLI, Central Islip, NY
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, Washington, DC
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
WALFRIDO J. MARTINEZ, New York, NY
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
JOHN J. MCGREGOR, Fresno, CA
JAMES C. MCKAY JR., Washington, DC
DOUGLAS EARL MCLAREN, Washington, DC
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
DONNA M. NAGY, Bloomington, IN
JOEL W. NOMKIN, Phoenix, AZ
VANCE K. OPPERMAN, Minneapolis, MN
BARAK ORBACH, Tucson, AZ
JOHN EDWARD OSBORN, Chadds Ford, PA
COLIN OWYANG, Rutland, VT
ERIC J. PAN, Bethesda, MD
JACQUELINE A. PARKER, New York, NY
WENDY L. PATRICK, San Diego, CA
WILLIAM J. PERLSTEIN, Washington, DC
JOY LAMBERT PHILLIPS, Gulfport, MS
A. ROBERT PIETRZAK, New York, NY
JACK W. PIROZZOLO, Boston, MA
ELLEN S. PODGOR, Gulfport, FL
DONALD J. POLDEN, San Jose, 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, Chicago, IL
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
JACOB H. ROOKSBY, Spokane, WA
ROD J. ROSENSTEIN, Washington, DC
JEREMY LEDGER ROSS, Seattle, WA
KENNETH ROSS, Midway, UT
VICTORIA P. ROSTOW, Washington, DC
IRMA S. RUSSELL, Shawnee Mission, KS
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
D. GORDON SMITH, Provo, UT
DOUGLAS G. SMITH, Chicago, IL
MARY L. SMITH, Lansing, IL
NICHOLAS F. B. SMYTH, Pittsburgh, PA
DAVID V. SNYDER, Washington, DC
D. DANIEL SOKOL, Gainesville, FL
PETER Y. SOLMSSEN, Abiquiu, NM
DAVID E. STERNBERG, New York, NY
RHEA C. STEVENS, Pearland, TX
H. MARK STICHEL, Baltimore, MD
ELIZABETH S. STONG, Brooklyn, NY
ANDREW H. STRUVE, San Diego, 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
LUCY L. THOMSON, Washington, DC
ETHAN V. TORREY, Washington, DC
PETER D. TROOBOFF, Washington, DC
DANIEL E. TROY, Chevy Chase, MD
FREDERICK TUNG, Boston, MA
THOMAS A. TUPITZA, Erie, PA
E. PETER URBANOWICZ, Dallas, TX
ANDREW VERSTEIN, Los Angeles, CA
FREDERICK WILLIAM (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

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. L. 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.

TABLE OF CONTENTS

Section *Page*

PART ONE

GENERAL PROVISIONS

CHAPTER 1

DEFINITIONS

PART TWO

COMPLIANCE

CHAPTER 4

COMPLIANCE RISK MANAGEMENT

TOPIC 1
COMPLIANCE RISK MANAGEMENT IN GENERAL

TOPIC 2
GENERAL CONSIDERATIONS IN COMPLIANCE RISK MANAGEMENT

TOPIC 3
SPECIFIC COMPLIANCE-RISK-MANAGEMENT ACTIVITIES

CHAPTER 5

THE COMPLIANCE FUNCTION

TOPIC 3
SPECIFIC COMPLIANCE ACTIVITIES

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 INTERNATIONAL FIRMS

PART THREE

ENFORCEMENT

CHAPTER 6

CRIMINAL, CIVIL, AND ADMINISTRATIVE ENFORCEMENT AGAINST INDIVIDUALS AND COMPANIES FOR CORPORATE MISCONDUCT

TOPIC 1

DEFINITIONS

TOPIC 2

PRINCIPLES COMMON TO ENFORCEMENT BY PROSECUTORS AND CIVIL-ENFORCEMENT OFFICIALS

PART TWO
COMPLIANCE

CHAPTER 4
COMPLIANCE RISK MANAGEMENT

Introductory Note: This Chapter is about compliance risk management. Organizations manage compliance risk in the context of, and as part of their broader management of, all the risks they face. Organizations also have compliance functions, and their management of compliance risk will be integrally involved with that function. This Chapter references an organization's broader risk-management and compliance endeavors when appropriate. Given that Chapter 5 expressly deals with the compliance function, this Chapter focuses more on compliance risk in relation to the organization's overall risk management, characterizing compliance risk management as a type and part of risk management when appropriate.

TOPIC 1
COMPLIANCE RISK MANAGEMENT IN GENERAL

§ 4.01. Nature of Compliance Risk and Compliance Risk Management

(a) An organization should manage compliance risk in a manner appropriate for its attributes and circumstances.

(b) An organization should manage compliance risk through or in coordination with its risk-management function and risk-management program, and through or in coordination with its compliance function and compliance program.

Comment:

a. Definition of compliance risk. Compliance risk is the risk that an organization will experience financial, operational, or reputational losses, legal sanctions, or other negative consequences because of its unwillingness or failure to follow laws, regulations, rules, its code of ethics, its ethical standards, or legally applicable or otherwise binding industry codes of conduct, or to cooperate appropriately with regulators. See § 1.01(n).

b. Definition of compliance risk management. Compliance risk management is the processes, practices, and activities by which an organization manages its compliance risk. See § 1.01(o).

c. Compliance risk management as part of risk management. An organization's compliance risk management is part of its overall risk management. An organization's risk management is the processes, practices, and activities by which its risk is identified, assessed, prioritized, avoided, prevented, reduced, shared, transferred, monitored, mitigated, and otherwise responded to, or accepted, and the monitoring and review of those processes, practices, and activities. See § 1.01(xx).

d. Coordination with compliance function and compliance program; relationship to risk management. An organization's compliance risk management should be coordinated or integrated with its compliance function and its compliance program. See §§ 5.01–511. An organization's compliance risk management should be coordinated or integrated with its risk management, including, as appropriate, its risk-management program, risk-management function, and risk-management framework.

e. Compliance risk management differs in different organizations. An organization's compliance risk management should reflect its particular attributes and circumstances, which include the organization's size, complexity, and resources, and its assessment of the compliance risks it faces and anticipates that it may face. See § 4.03.

f. Compliance risk as risk of certain negative consequences. Compliance risk includes the risk of negative consequences for an organization's unwillingness or failure to follow laws, regulations, rules, or legally applicable or otherwise binding industry codes of conduct, or to cooperate appropriately with regulators. It also includes the risk of negative consequences from an organization's unwillingness or failure to follow its code of ethics or its ethical standards. See § 5.26, §§ 5.34–5.35, and § 6.08. The negative consequences include negative financial, operational, reputational, and legal consequences.

g. Residual compliance risk. An organization cannot completely eliminate its compliance (or other) risks; it will necessarily face residual risk, including residual compliance risk. See § 4.13.

h. Compliance risk distinguished from other risks. Compliance risk management differs from management of an organization's other risks, most notably its strategic risks, the risks that an organization expressly takes on to achieve its strategy and business objectives. On strategic risks, see § 4.04, Comment *d*. Both types of risk are inevitable and cannot be eliminated. But compliance risk is downside risk; the organization manages it by seeking to minimize it to the extent feasible. By contrast, strategic risks are both upside and downside risks; an organization does not seek only to minimize strategic risk.

i. Risk appetite and risk tolerance. As part of its overall risk management, an organization's risk-management function sets its risk appetite (the type and level of risk it is willing to assume to achieve its strategy and business objectives), its risk tolerance (the maximum amount of residual risk it is willing to bear), and determines its risk capacity (the maximum amount of risk it is able to assume in the pursuit of its strategy and business objectives). See § 1.01(ss) (risk appetite), §1.01(uu) (risk capacity), and § 1.01(bbb) (risk tolerance).

j. Risk appetite and risk tolerance for compliance risk. An organization may have a risk appetite and risk tolerance for compliance risk, in order to guide it both in designing and executing its compliance risk management and in assessing the residual compliance risk that it will accept.

k. An organization's choices regarding levels of risk. As to risks other than compliance risks, an organization may conclude that given its risk appetite, risk tolerance, and risk capacity, and the particular risks and aggregate level of risk it faces, it should take on more risk. However, the organization may not make such a conclusion with respect to compliance risk. An organization may not choose to take on more compliance risk because its risk appetite, risk tolerance, or risk capacity for the organization or for particular risks within the organization allows for or contemplates taking on more risk, nor may an organization decide that a compliance risk event that has come to pass (a compliance failure) is within its risk tolerance. Rather, if there has been a compliance failure, the organization must respond in an appropriate manner, including remediating the effects of the event itself as well as reviewing its risk management and making any adjustments that it determines are warranted.

l. Need for qualitative measurement. Compliance risk is often difficult to measure quantitatively. Compliance risk management thus makes significant use of qualitative measures.

REPORTERS' NOTES

a. Definition of risk. Risk has been defined as "[t]he possibility that events will occur and affect the achievement of strategy and business objectives." COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT–INTEGRATING WITH STRATEGY AND

PERFORMANCE 167 (2017). The term also importantly includes downside risk, "the possibility that an event will occur and *adversely affect* the achievement of objectives." COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, INTERNAL CONTROL–INTEGRATED FRAMEWORK 4 (2013) (emphasis added). Risk management generally deals with both upside and downside risks. But compliance risk, and its risk management, more straightforwardly concern downside risk.

b. Risk vs. uncertainty. Under a formal, narrow definition of risk, possible outcomes, whether bad or good, and their associated probabilities, are known, and thus, risk can be computed mechanically. But risk management importantly also involves "uncertainty," "[t]he state of not knowing how or if potential events may manifest." COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT–INTEGRATING WITH STRATEGY AND PERFORMANCE 168 (2017).

Frank Knight articulated the distinction between risk and uncertainty as follows:

> Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated. The term "risk," as loosely used in everyday speech and in economic discussion, really covers two things which, functionally at least, in their causal relations to the phenomena of economic organization, are categorically different. … The essential fact is that "risk" means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far reaching and crucial differences in the bearings of the phenomenon depending on which of the two is really present and operating. … It will appear that a measurable uncertainty, or "risk" proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect an uncertainty at all. We shall accordingly restrict the term "uncertainty" to cases of the non-quantitative type.

FRANK H. KNIGHT, RISK, UNCERTAINTY AND PROFIT 19-20 (1921). See also JOHN KAY & MERVYN KING, RADICAL UNCERTAINTY: DECISION-MAKING BEYOND THE NUMBERS (2021).

Thus, the risks an organization faces cannot be computed mechanically, nor can risk management be largely a mechanical task. While the results of a large number of purely financial bets can be computed with precision, for many other kinds of risks, including risks that arise from the actions of third parties or nature, reputational risks, newly emerging risks such as cybersecurity risks, and risks of remote but catastrophic events, the "computation" is quite different—and often more difficult. The use of concepts that are in some contexts amenable to relatively mechanical computation and aggregation may mask the level of discretion and judgment that risk computation entails. This is a particularly important point for compliance risk, much of which does not lend itself well to mechanical computations.

c. Risk-management frameworks generally. Compliance risk is part of the broader endeavor of risk management. An important treatment of risk management was published 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. In 2017, COSO released its updated enterprise risk-management framework. COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT–INTEGRATING WITH STRATEGY AND PERFORMANCE (2017). Another prominent framework is the International Organization of Standardization's *ISO 31000:2018, Risk Management Guidelines*, https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

d. Definition of enterprise risk management. Many organizations, especially large or more complex organizations, manage their risks on an enterprise-wide basis. COSO's 2017 *Enterprise Risk Management–Integrating with Strategy and Performance* defines "enterprise risk management" 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." COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT–INTEGRATING WITH STRATEGY AND PERFORMANCE 44 (2017). See also EY, NEXT-GENERATION ENTERPRISE RISK MANAGEMENT, ADVANCING STRATEGY AND PERFORMANCE IN LIGHT OF THE COSO 2017 REFRESH (2017), https://pdf4pro.com/cdn/next-generation-enterprise-risk-management-ey-e2960.pdf.

e. Risk management for financial institutions. Other organizations—some private and some governmental—have issued principles, reports, and other guidance on risk management. A significant amount of this guidance is focused on risk management in financial institutions, much of which is management of compliance risk.

See, e.g., INST. OF INT'L FIN., FINAL REPORT OF THE INSTITUTE OF INTERNATIONAL FINANCE'S COMMITTEE ON MARKET BEST PRACTICES: PRINCIPLES OF CONDUCT AND BEST PRACTICE RECOMMENDATIONS (2008), https://www.iif.com/publication/regulatory-report/global-finance-leaders-release-comprehensive-proposals-strengthen; BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK (2011), http://www.bis.org/publ/bcbs195.pdf; FIN. STABILITY BD., PRINCIPLES FOR AN EFFECTIVE RISK APPETITE FRAMEWORK (2013), http://www.fsb.org/wp-content/uploads/r_131118.pdf.

The Federal Reserve's guidance on board effectiveness in large financial institutions addresses risk management. See Bd. of Governors of the Fed. Rsrv. Sys., SR 21-3/CA 21-1, *Supervisory Guidance on Board of Directors' Effectiveness* (February 26, 2021), https://www.federalreserve.gov/supervisionreg/srletters/SR2103.htm, and https://www.federalreserve.gov/supervisionreg/srletters/SR2103a1.pdf. See also OFF. OF THE COMPTROLLER OF THE CURRENCY, DIRECTOR'S BOOK; ROLE OF DIRECTORS FOR NATIONAL BANKS AND FEDERAL SAVINGS ASSOCIATIONS 51-71 (2020), https://www.occ.gov/publications-and-resources/publications/banker-education/files/pub-directors-book.pdfguidance, addressing risk governance.

f. Reports on risk-management failures. Interest in risk management increased significantly after several major corporate-governance, oversight, and reporting lapses in the early 2000s. Several companies collapsed, arguably in significant part because of their failure to manage risk properly, importantly including compliance risk. Other organizations have suffered severe negative consequences from poor management of compliance and other risks. For instructive case studies, see GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 799-825 (3d ed. 2020).

One report describing an organization's risk management and other failings is ANTHONY SALZ & RUSSELL COLLINS, SALZ REVIEW: AN INDEPENDENT REVIEW OF BARCLAYS' BUSINESS PRACTICES (2013), https://online.wsj.com/public/resources/documents/SalzReview04032013.pdf. Other reports include UBS's *Shareholder Report on UBS's Write-Downs* (Apr. 18, 2008), http://maths-fi.com/ubs-shareholder-report.pdf, ANTON VALUKAS, JENNER & BLOCK, REPORT TO BOARD OF DIRECTORS OF GENERAL MOTORS COMPANY REGARDING IGNITION SWITCH RECALLS (2014) (redacted), https://www.aieg.com/wp-content/uploads/2014/08/Valukas-report-on-gm-redacted2.pdf, and ANTON VALUKAS, JENNER & BLOCK, LEHMAN BROTHERS HOLDINGS INC. CHAPTER 11 PROCEEDINGS EXAMINER'S REPORT (2010), https://jenner.com/lehman. In another report, the U.K. Financial Services Authority analyzed shortcomings at a Scottish bank which led to a government bailout. FIN. SERVS. AUTH., THE FAILURE OF THE ROYAL BANK OF SCOTLAND (2011), https://www.fca.org.uk/publication/corporate/fsa-rbs.pdf. See also MARGARET WOODS, ASTON UNIV., REPORTING AND MANAGING RISK: A LOOK AT CURRENT PRACTICE AT TESCO, RBS, LOCAL AND CENTRAL GOVERNMENT, Chartered Institute of Management Accountants, Research Executive Summary Series Volume 6, Issue 8 (2010), https://www.cimaglobal.com /Documents/Thought_leadership_docs/R267%20Manage%20risks.pdf. In yet another report, a congressional committee addressed an organization's aircraft model that was involved in fatal crashes. MAJORITY STAFF OF H. COMM. ON TRANSP. & INFRASTRUCTURE, 116TH CONG., FINAL REPORT ON THE DESIGN, DEVELOPMENT & CERTIFICATION OF THE BOEING 737 MAX (2020), https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf. The report, the Final Committee Report on the Boeing MAX 737, is at https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737 %20MAX%20Report%20for%20Public%20Release.pdf. On Jan. 7, 2021, the United States and Boeing entered into a deferred prosecution agreement relating to matters discussed in the report, with Boeing agreeing to pay $2.5 billion in penalties and reimbursements. See *Deferred Prosecution Agreement between the United States of America and the Boeing Company,* U.S. District Court, N.D. Texas, https://www.justice.gov/opa/press-release/file/1351336/download.

A report not focused on a particular organization's failure is the Senior Supervisors' Group's *Risk Management Lessons from the Global Banking Crisis of 2008* (Oct. 21, 2009), https://www.sec.gov/news/press/2009/report102109.pdf. The report is written by the financial supervisory authorities of Canada, France, Germany, Japan, Switzerland, and the United Kingdom. The report's transmittal letter sets forth some areas of weakness that are highlighted therein: "the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm; compensation programs that conflicted with the control objectives of the firm; inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel."

SENIOR SUPERVISORS' GRP., RISK MANAGEMENT LESSONS FROM THE GLOBAL BANKING CRISIS OF 2008 (2009), https://www.sec.gov/news/press/2009/report102109.pdf.

Another report that focuses heavily on compliance risk-management failures in financial institutions is the final report of the Financial Crisis Inquiry Commission, formed to examine the causes of the financial crisis that began in 2007–2008. FIN. CRISIS INQUIRY BD., FINANCIAL CRISIS INQUIRY REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON THE CAUSES OF THE FINANCIAL AND ECONOMIC IN THE UNITED STATES (2011), https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf.

g. Compliance risk management and definitions. While the management of compliance risk has long been an important component of risk management, compliance risk management, referred to as such, is increasingly generating its own commentary and guidance. In November 2020, the Committee on Sponsoring Organizations of the Treadway Commission released a report, *Compliance Risk Management: Applying the COSO ERM Framework*. The report defined compliance risks as "those risks relating to possible violations of applicable laws, regulations, contractual terms, standards, or internal policies where such violation could result in direct or indirect financial liability, civil or criminal penalties, regulatory sanctions, or other negative effects for the organization or its personnel." Id at 1. Another definition of compliance risk is "the threat posed to an organization's financial, organizational, or reputational standing resulting from violations of law, regulations, codes of conduct, or organizational standards of practice." DELOITTE & TOUCHE LLP, BUILDING WORLD-CLASS ETHICS AND COMPLIANCE PROGRAMS: MAKING A GOOD PROGRAM GREAT 12 (2018), https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Building-world-class-ethics-and-compliance-programs.pdf. As the field evolves, different definitions can be expected, with some broader than others; for instance, breaches of contract terms might be within some definitions and not within others. A contract breach has been viewed by some theorists as simply a willingness to pay the penalties associated with the breach—and desirable under some circumstances. See generally Gregory Klass, *Efficient Breach*, *in* THE PHILOSOPHICAL FOUNDATIONS OF CONTRACT LAW 362-387 (Gregory Klass, George Letsas & Prince Saprai eds., 2014).

h. Compliance risk beyond law and regulatory violations. COSO's *Compliance Risk Management: Applying the COSO ERM Framework*, noted that its use of the term "compliance risk" includes "any risk that is either directly associated with a law or regulation or is compliance-related in that it is associated with other standards, organizational policies, or ethical expectations and guidelines." COMM. ON SPONSORING ORGANIZATIONS OF THE TREADWAY COMM'N, COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK (2010), https://www.coso.org/Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf. See also the Organizational Sentencing Guidelines, which state that in order to have an effective compliance program, an organization must (1) "exercise due diligence to prevent and detect criminal conduct" and (2) "*otherwise promote an organizational culture that encourages ethical conduct* and a commitment to compliance with the law." U.S. SENT'G

GUIDELINES MANUAL § 8B2.1 (U.S. SENT'G COMM'N 2013) (emphasis added), quoted in § 6.08, Reporters' Note *b*.

i. Federal Reserve definition of compliance risk. The Federal Reserve has defined compliance risk as "the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations applicable to the banking organization (applicable rules and standards)." Bd. of Governors of the Fed. Rsrv. Sys., SR 8-08/CA 08-11, Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles (2008), https://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.

j. Relationship between risk management and compliance risk. A letter from the Board of Governors of the Federal Reserve on the relationship between risk management generally and compliance risk states that:

> While the guiding principles of sound risk management are the same for compliance as for other types of risk, the management and oversight of compliance risk presents certain challenges. For example, quantitative limits reflecting the board of directors' risk appetite can be established for market and credit risks, allocated to the various business lines within the organization, and monitored by units independent of the business line. Compliance risk does not lend itself to similar processes for establishing and allocating overall risk tolerance, in part because organizations must comply with applicable rules and standards. Additionally, existing compliance risk metrics are often less meaningful in terms of aggregation and trend analysis as compared with more traditional market and credit risk metrics. These distinguishing characteristics of compliance risk underscore the need for a firmwide approach to compliance risk management and oversight for large, complex organizations. A firmwide compliance function that plays a key role in managing and overseeing compliance risk while promoting a strong culture of compliance across the organization is particularly important for large, complex organizations that have a number of separate business lines and legal entities that must comply with a wide range of applicable rules and standards.

Id.

k. Compliance risks as distinguished from other risks. Robert S. Kaplan and Anette Mikes set forth a risk taxonomy that distinguishes compliance risks, strategic risks, and external risks. The first category largely encompasses misbehavior by employees or managers. Kaplan and Mikes also use the term "preventable" for this category. The second largely encompasses risks that the organization must take on to pursue and achieve its strategy. Kaplan and Mikes describe these risks, also called "strategy" risks, as ones the organization takes in order to obtain a higher return; they characterize these risks as "not inherently undesirable." The third, "external risks", largely encompasses actions or events that are mostly or completely outside of the organization's influence or control, such as regulatory changes, actions by competitors, or natural disasters. See generally Robert S. Kaplan & Anette Mikes, *Managing Risks: A New Framework*, HARV. BUS. REV. (June 2012), https://hbr.org/2012/06/managing-risks-a-new-framework. There is also a classification by a Blue Ribbon Commission of the National Association of Corporate Directors. NACD AND THE CENTER OF BOARD LEADERSHIP AND ITS ALLIANCE PARTNERS, THE REPORT OF THE NACD BLUE RIBBON COMMISSION ON RISK GOVERNANCE: BALANCING RISK AND REWARD (2009). https://www.nacdonline.org/insights/publications.cfm?ItemNumber=675. The commission lists the following categories or classifications: governance risks; critical-enterprise risks; board-approval risks; emerging and nontraditional risks; and business-management risks; a category that includes reporting risks, operational risks, financial risks, human-resources risks, and compliance and reputational risks. Id. at 22-23. Three authors provide a detailed listing of specific types of risks: hazard risks, financial risks, strategic risks, and operations risks. William G. Shenkir, Thomas L. Barton & Paul L. Walker, *Enterprise Risk Management: Lessons from the Field*, *in* ENTERPRISE RISK MANAGEMENT 446 (John Fraser & Betty Simkins eds., 2010).

l. The history of risk management. Several authors provide histories of risk management. H. Felix Kloman, *A Brief History of Risk Management*, *in* ENTERPRISE RISK MANAGEMENT 19 (John Fraser & Betty Simkins eds., 2010); Georges Dionne, *Risk Management: History, Definition, and Critique*, 16 RISK MGM'T & INS. REV. 147 (2013); and Betty Simkins & Steven Ramirez, *Enterprise-Wide Risk Management and Corporate Governance*, 39 LOY. U. CHI. L.J. 571 (2008). Peter Bernstein's *Against the Gods: The Remarkable Story of Risk* recounts the history of the concept of risk. "The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than a whim of the gods and that men and women are not passive before nature. Until human beings discovered a way across that boundary, the future was a mirror of the past or the murky domain of oracles and soothsayers who held a monopoly over knowledge of anticipated events." PETER BERNSTEIN, AGAINST THE GODS: THE REMARKABLE STORY OF RISK 2 (1996).

m. Enterprise risk management as distinguished from risk management. In their history of enterprise risk management, Betty Simkins and Steven Ramirez contrast the new, enterprise-based paradigm with an older one, albeit still in use, in which risk management is fragmented and done in silos, ad hoc, and narrowly focused on "insurable and financial risks." Betty Simkins & Steven A. Ramirez, *Enterprise-Wide Risk Management and Corporate Governance*, 39 LOY. U. CHI. L.J. 571 (2008). The enterprise risk-management paradigm integrates risk management throughout, and within, the organization. The task is ongoing such that some matters are reviewed on a scheduled basis, while others are reviewed continuously, but at all times, risk is being managed as needed, and risk management is broadly focused on all "business risks and opportunities." Id. at 581. Thus, the concept of "enterprise risk management" often refers to risk management that is not just enterprise-wide, but also has these other features. For another history of enterprise risk management, see Kristin N. Johnson & Steven A. Ramirez, *New Guiding Principles: Macroprudential Solutions to Risk Management Oversight and Systemic Risk Concerns*, 11 U. ST. THOMAS L.J. 386 (2014).

§ 4.02. Goals of Compliance Risk Management

The goals of compliance risk management include:

(a) managing and to the extent feasible, minimizing the organization's compliance risk in a cost-effective manner;

(b) establishing, maintaining, promoting, and demonstrating the organization's commitment to an effective risk culture, including as it pertains to compliance risk;

(c) preserving value for the organization, including by minimizing the costs associated with compliance risk; and

(d) adding value, by ensuring that the organization's strategy and business objectives, major decisions, and its overall risk management are informed by considerations relating to compliance risk.

Comment:

a. Cost-effective management of compliance risk. An organization's compliance risk management should seek to manage compliance risk cost-effectively, and in a manner appropriate to the organization's particular attributes and circumstances.

b. Compliance risk cannot be eliminated. It is impossible to eliminate compliance risk. An organization should aim to reduce compliance risk as much as it reasonably and in good faith concludes is feasible, and accept the residual compliance risk only after a reasoned and deliberate assessment that doing so is appropriate. See § 4.13.

c. Risk culture to be conducive to effective risk management. An organization's risk culture should be conducive to effective risk management, including compliance risk management. See §§ 3.07 and 4.06. An effective risk culture can have positive effects across an organization. While risk culture is one component of organizational culture, an effective risk culture can positively affect the organizational culture as a whole.

d. Preserving organizational value as goal. A traditional goal of risk management generally, including compliance risk management, is to preserve the value of the organization, including by minimizing the effects of downside risks that the organization faces.

e. Adding value as potential benefit. Beyond avoiding losses caused by ineffective risk management and thereby preserving value, adding value is a potential benefit of risk management, including compliance risk management. In particular, the organization should benefit from taking compliance risk into account in setting and modifying its strategy and business objectives, and in considering significant changes and decisions.

REPORTERS' NOTES

a. Benefits of risk management. Risk management, including compliance risk management, provides potential benefits to an organization, including cost-effective management of risk, overall cost savings and better capital allocation, benefits to competitive position and attractiveness to investors, increased predictability of results and costs, and better preparation for low-probability catastrophic risks. See generally COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT–INTEGRATING WITH STRATEGY AND PERFORMANCE 13 (2017) (in the context of enterprise risk management), and INST. OF INT'L FIN., FINAL REPORT OF THE IIF COMMITTEE ON MARKET BEST PRACTICES: PRINCIPLES OF CONDUCT AND BEST PRACTICE RECOMMENDATIONS: FINANCIAL SERVICES INDUSTRY RESPONSE TO THE MARKET TURMOIL OF 2007-2008, 38 (2008). For a general survey, also in the context of enterprise risk management, on how risk management has fared and what it might yield, see MARK BEASLEY, BRUCE BRANSON & BONNIE HANCOCK, THE STATE OF RISK OVERSIGHT: AN OVERVIEW OF ENTERPRISE RISK MANAGEMENT PRACTICES (7th ed. 2016), https://erm.ncsu.edu/az/erm/i/chan/library/AICPA_ERM_Research_Study_2016.pdf.

b. Risk management as adding value. The traditional articulation of the rationale for risk management has focused on preserving value and avoiding downside risks. The increasing emphasis on risk management since the 2007–2008 financial crisis was sparked by the significant losses and other adverse effects the crisis caused. But subsequent articulations have increasingly considered risk management as also potentially adding value. For a study providing evidence of the potential value creation effects of risk management, see Torben Juul Andersen & Oliviero Roggi, *Strategic Risk Management and Corporate Value Creation, in* THE ROUTLEDGE COMPANION TO STRATEGIC RISK MANAGEMENT (Torben Juul Andersen ed., 2014).

Many of the discussions as to value-adding have expressly considered enterprise risk management. Enterprise risk management has been described as allowing an organization to make better decisions and assume a level of risk more in line with the organization's values and priorities. Robert Kaplan and Anette Mikes discuss the relationship between an organization's value preservation and enhancement and its enterprise risk management in *Risk Management—the Revealing Hand*, 28 J. APPL. CORP. FIN. 8 (2016) (discussing the "greater internal clarity," which can lead to "better decision-making"). Indeed, as stated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), "[e]nterprise risk management is no longer focused principally on preventing the erosion of value and minimizing risk to an acceptable level. Rather, it is viewed as integral to strategy setting and the identification of opportunities to create and maintain value. Instead of simply focusing on reducing risk to a target state, enterprise risk management becomes a dynamic and integral part of the managing [sic] an entity throughout the value chain." COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, ENTERPRISE RISK MANAGEMENT–INTEGRATING WITH STRATEGY AND PERFORMANCE 15 (2017), https://www.coso.org/Documents/COSO-ERM-FAQ-September-2017.pdf. According to COSO, the benefits of enterprise risk management include that it can increase positive outcomes and advantages, increase the range of opportunities management has available, improve resource deployment, identify and manage enterprise-wide risks, and reduce negative surprises and performance variability. Id. at 37-38. See also Jim DeLoach, *A Value-Based Approach to Risk Management*, CORPORATE COMPLIANCE INSIGHTS (Sept. 3, 2015), https://www.corporatecomplianceinsights.com/a-value-based-approach-to-risk-management. Much of what is referred to potentially falls within the purview of compliance risk management.

c. Compliance risk management as adding value. Beyond the general benefits of risk management, compliance risk management can be value-adding in various ways. Integrating risk management, notably compliance risk management, into an organization's strategy-setting and articulation of its business plan helps the organization make choices that reflect the full spectrum of risks and opportunities it faces. It also focuses the organization on risk minimization throughout its execution of its business plan. Integrating compliance risk-management concerns into the organization's hiring, training, compensation, and discipline of its employees, and, more broadly, the organization's consideration of its strategy, business objectives, and business plan, can help the organization better understand the relationship between its risks and its opportunities, and better present itself to relevant constituencies. See also COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK 7-14 (2020), https://www.coso.org/Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf; Rebecca Chasen, *Creating Value Through Compliance Modernization,* RISK & COMPLIANCE J. (May 16, 2017), https://deloitte.wsj.com/riskandcompliance/2017/05/16/creating-value-through-compliance-modernization/; and DELOITTE, COMPLIANCE RISK MANAGEMENT POWERS PERFORMANCE (2018), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-compliance-risk-management-powers-performance.pdf. Indeed, COSO's report on Compliance Risk Management states that compliance "should be considered as a business objective of the organization." Id at 12.