THE GOVERNING AUTHORITY'S RESPONSIBILITIES IN COMPLIANCE AND RISK MANAGEMENT, AS SEEN IN THE AMERICAN LAW INSTITUTE'S DRAFT PRINCIPLES OF COMPLIANCE, RISK MANAGEMENT, AND ENFORCEMENT

James A. Fanto[*]

ABSTRACT

This Essay discusses the project on compliance and risk management of the American Law Institute in relation to the governance of compliance and risk management in an organization. It identifies several important governance issues and debates that have emerged in the drafting process. These issues are (i) the appropriate role of what the project calls the "highest legal authority" in compliance and risk management and (ii) the related topic of to whom internal control officers, particularly the chief compliance officer and the chief risk officer, report. While discussing the importance of, and the project's approach to, these issues, the Essay emphasizes that the project provides flexibility to organizations, which reflects the diversity of organizational practice on these, and other, governance issues.

TABLE OF CONTENTS

INTRODUCTION

As an academic, I follow the compliance and risk management professions and developments in these fields,[1] but I do not practice in them. Thus, when

* Gerald Baylin Professor of Law, Brooklyn Law School. This Essay is based upon a panel presentation titled "It's Only Dicta—*Caremark*'s Impact on Compliance, Risk Management, and Governance," at the 2017 Temple Law Review Symposium, held on October 26, 2017. The symposium was titled "The *Caremark* Decision at 21: Corporate Compliance Comes of Age—What Does the Future Hold?"

1. I began to write about compliance primarily because of my work on the regulation of broker-dealers. *See* NORMAN S. POSER & JAMES A. FANTO, BROKER-DEALER LAW & REGULATION (4th ed. 2007).

presenting at the Temple Law Review Symposium in October 2017, I talked about issues related to the governance of compliance and risk management from an academic perspective. This perspective complemented the presentations of others who understand significant issues in compliance and risk management as practitioners. In particular, I discussed the governance of compliance and risk management in relation to a project of The American Law Institute (ALI) with which I am involved. This Principles of Law project, titled Compliance, Enforcement, and Risk Management for Corporations, Nonprofits, and Other Organizations and referred to hereinafter as the ALI Compliance Project, involves, among other things, formulating principles of compliance and risk management.[2]

It might be useful to situate the ALI Compliance Project by explaining why it is appropriate to articulate these principles now. Ever since Chancellor Allen delivered the *In re Caremark International Inc. Derivative Litigation* decision,[3] compliance has become a recognized internal control function in many organizations.[4] The growth and establishment of compliance in organizations is due to a complex interaction among judges, regulators, prosecutors, and the organizations themselves.[5] As discussed by others in this conference,[6] Delaware courts, beginning with *Caremark*, have held that the board of a corporation has the responsibility to ensure that management has established a reasonable system to prevent and to detect violations of the law or regulation.[7] The Delaware judges drew support partly from the Sentencing Guidelines for Organizations promulgated by the U.S. Sentencing Commission.[8] Under the Guidelines, a firm that was criminally liable because of crimes committed by its employees could receive credit in its sentencing if that firm had an effective compliance and ethics program as defined by the Guidelines.[9] In addition, on the

2. *See* PRINCIPLES OF THE LAW: COMPLIANCE, ENFORCEMENT, AND RISK MANAGEMENT FOR CORPORATIONS, NONPROFITS, AND OTHER ORGANIZATIONS (AM. LAW INST., Preliminary Draft No. 3, 2017) [hereinafter, ALI COMPLIANCE PROJECT]. This project is still underway and not finalized as of the publication of this Essay. Thus, its principles, which I discuss below, remain preliminary and subject to change.

3. *See* 698 A.2d 959 (Del. Ch. 1996).

4. *See* Miriam Hechler Baer, *Governing Corporate Compliance,* 50 B.C. L. REV. 949, 965–72 (2009) (highlighting the growth of compliance and the reasons for it, including *Caremark*).

5. *See id.* at 958–79 (discussing these different influences in the growth of compliance).

6. *See generally* Symposium, *The* Caremark *Decision at 21—Corporate Compliance Comes of Age*, 90 TEMP. L. REV. 597 (2018).

7. *See, e.g.*, *Caremark*, 698 A.2d at 970 ("[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 . . . ."); *see also* Stone v. Ritter, 911 A.2d 362, 365 (Del. 2006) (accepting that board's oversight obligation includes the responsibility to ensure that the corporation has a compliance function adequate for the organization).

8. *See Stone*, 911 A.2d at 370 (approving the *Caremark* standard); *Caremark,* 698 A.2d at 969 (discussing the U.S. SENTENCING GUIDELINES MANUAL ch. 8 (U.S. SENTENCING COMM'N 1991)).

9. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (U.S. SENTENCING COMM'N 2016) (laying out the elements of an effective compliance and ethics program); *id.* § 8C2.5(f) (discussing the effect of a compliance program in determining the organization's culpability score for a calculation of a fine to be assessed).

basis of their governing statutes, regulators required organizations under their authority to have a compliance function.[10] For example, in 2004 the Securities and Exchange Commission (SEC) required registered investment advisers to have a compliance program with a chief compliance officer (CCO).[11] In an entirely different domain, the Office of Inspector General for the Department of Health and Human Services directed hospitals to have a compliance program managed by a CCO.[12]

To guide organizations in their response to this judicial and regulatory activity, scholars and practitioners have developed codes, best practices, and guidelines regarding the duties of compliance officers and the structure of compliance programs.[13] Today many organizations have compliance programs administered by a CCO or by a person in the organization in charge of its compliance activities.[14]

Risk management has also gained attention in the legal community, although by following a different path from compliance.[15] In financial institutions, which need to manage their credit and market risks, risk management has been a subject of operational and business attention for some time.[16] The practice of risk management received considerable legal attention, again primarily in financial institutions, because of the financial crisis of 2007–2008.[17] This crisis was regarded as an event that exposed defective risk-management practices in large financial institutions, which contributed to their failure or near failure and to the near collapse of the financial system.[18]

10. *See infra* notes 11–12.

11. *See* Compliance Programs of Investment Companies and Investment Advisers, 68 Fed. Reg. 74,714, 74,715 (Dec. 24, 2003) (codified at 17 C.F.R. pts. 270, 275, 279) (setting forth, among other things, Rule 206(4)-7 to this effect).

12. *See* Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,989 (Feb. 23, 1998) (providing this requirement and guidance for hospitals).

13. *See* INT'L ORG. FOR STANDARDIZATION, NO. 19600, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES (1st ed. 2014) [hereinafter COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES] (laying out the elements of a compliance program by an organization designed to standardize compliance practices). An early, ambitious, and useful effort to put compliance into principles was that done by the National Center for Preventive Law. NAT'L CTR. FOR PREVENTIVE LAW, CORPORATE COMPLIANCE PRINCIPLES (1996). It set forth twenty compliance principles, *id.* at 1–42, and gave over one-hundred pages of examples drawn from how compliance worked in practice in corporations at that time. *Id.* at 44–147.

14. *See, e.g.*, Sean J. Griffith, *Corporate Governance in an Era of Compliance*, 57 WM. & MARY L. REV. 2075, 2101–02 (2016) (describing the growth of compliance departments headed by CCOs).

15. *See infra* notes 16–23 and accompanying text.

16. See ANTHONY SAUNDERS & MARCIA MILLON CORNETT, FINANCIAL INSTITUTIONS MANAGEMENT: A RISK MANAGEMENT APPROACH 168–75 (6th ed. 2008) for a discussion of financial institutions' management of their credit and market risks, among others. *See generally* Anette Mikes, *Chief Risk Officers at Crunch Time: Compliance Champions or Business Partners?*, 2 J. RISK MGMT. FIN. INSTITUTIONS 7 (2008) (discussing of the growth of risk management).

17. *See infra* notes 19–20 and accompanying text.

18. *See* James Fanto, *Anticipating the Unthinkable: The Adequacy of Risk Management in Finance and Environmental Studies*, 44 WAKE FOREST L. REV. 731, 739–45 (2009) (discussing problems in risk management leading up to the crisis).

Following the crisis there was litigation raising the issue about the responsibility of the board of a public company for the company's risk-management practices and program, just as *Caremark* had done for compliance.[19] The Dodd-Frank Act, passed in response to the crisis,[20] directed federal banking regulators to develop risk-management standards for large bank holding companies to adopt.[21] Thus, in bank regulation, risk management became a subject of law and regulation.[22] As in the case of compliance, this judicial, legal, and regulatory activity then motivated efforts by private actors to develop recommended risk management practices and governance.[23]

In light of all of this activity in both compliance and risk management, the ALI considered it timely to look at the standards that have emerged from these legal and advisory developments, as well as the practice of compliance and risk management, in order to see whether general principles of the law could be articulated.[24] In its work, the ALI typically identifies law-related fields that might be ready for this kind of summation or rationalization and then assembles experts to conduct it.[25] In this case, the resulting principles are intended to

19. *See, e.g.*, *In re* Goldman Sachs Grp., Inc. S'holder Litig., C.A. No. 5215–VCG, 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."); *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 124–26 (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); *see also* G20/OECD, PRINCIPLES OF CORPORATE GOVERNANCE 56 (2015) (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" are required under Principle VI.D.7).

20. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111–203, 124 Stat. 1376 (2010). For background on Dodd-Frank, see MICHAEL S. BARR ET AL., FINANCIAL REGULATION: LAW AND POLICY 63 (1st ed. 2016).

21. *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. pt. 30, app. D (2017) (providing guidelines on risk management).

22. *See id.*

23. One of the most notable examples of this activity was accomplished by the Treadway Commission, which promulgated guidance on risk management throughout an organization, which was known as enterprise risk management or "ERM." *See, e.g.*, COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT: ALIGNING RISK WITH STRATEGY AND PERFORMANCE (2016) [hereinafter ENTERPRISE RISK MANAGEMENT]. International organizations contributed to this activity. *See* INT'L ORG. FOR STANDARDIZATION, NO. 31000, RISK MANAGEMENT—PRINCIPLES AND GUIDELINES 12 (1st ed. 2009) (providing principles and guidelines for risk management).

24. Professor Geoffrey Miller of New York University Law School, who is the chief reporter on the ALI Compliance Project, was responsible for proposing it to the American Law Institute. *Distilling the Law: American Law Institute Again Taps NYU Law Faculty to Oversee Publications on Key Areas of Practice*, NYU L. NEWS (Dec. 12, 2014), http://www.law.nyu.edu/news/ideas/american-law-institute [perma: http://perma.cc/R7PV-3ZCL].

25. As it observes on its website, the "American Law Institute is the leading independent organization in the United States producing scholarly work to clarify, modernize, and improve the law." *See About ALI*, AM. L. INST., http://www.ali.org/about-ali/ [perma: http://perma.cc/7MH6-VFPU] (last visited July 14, 2018).

provide guidance to legislators, regulators, industry bodies, and organizations about the basic elements of compliance and risk management and the structure and duties of compliance and risk-management programs. The ALI thus began the ALI Compliance Project, which is now in its third year of drafting.[26]

Because one of the main topics of this symposium is governance of compliance and risk management in an organization, I shall discuss the ALI Compliance Project in relation to that subject. In essence, governance means who is responsible for compliance and risk management in an organization and, in particular, who makes the key decisions on these subjects.[27] In other words, governance is about issues like the decisionmaking authority, duties, and reporting lines of organizational actors for compliance and risk management.[28]

Given the limitations of time and space, it is not possible in this Essay to cover all the compliance and risk management governance issues that we are considering and treating in the ALI Compliance Project. We are also still drafting our principles and receiving detailed comments on them from members of our advisory and consultative committees.[29] It may be useful at this point to identify several important issues and debates that have emerged in the drafting process. This exposition might also demonstrate the potential usefulness of the ALI Compliance Project regarding the governance of compliance and risk management that could benefit from the Project's suggested resolution.[30]

The issues discussed below focus on (i) the appropriate role of what the Project calls the "highest legal authority" in compliance and risk management and (ii) the related topic of to whom internal control officers, particularly the CCO and the chief risk officer (CRO), report. The role of the highest legal authority, which is the "individual or group exercising final authority over an organization's internal decisions,"[31] such as the board of directors of an

26. The conference where this Essay was presented was scheduled near the annual meeting of the ALI Compliance Project's advisory committee and consultative committee for a discussion of the draft principles. As the ALI describes the project, this "project will address the need for a set of recommended standards and best practices on the law of compliance and risk management." *Compliance, Enforcement, and Risk Management for Corporations, Nonprofits, and Other Organizations*, AM. L. INST., http://www.ali.org/projects/show/compliance-enforcement-and-risk-management-corporations-nonprofits-and-other-organizations/ [perma: http://perma.cc/Z6VC-MUBZ] (last visited July 14, 2018).

27. Indeed, in our most current draft, we say the following: "1.01(v) Governance. The process by which decisions relative to risk management and compliance are made within an organization." ALI COMPLIANCE PROJECT, *supra* note 2, § 1.01(v).

28. *See id.* § 3.01 (discussing the functions of governance).

29. Under the ALI project structure, an advisory committee is a selected group of ALI members and others who are tasked with offering comments on and reviewing a particular project, often because they have expertise in the subject matter. A consultative committee is composed of only ALI members who have expressed interest in the project and attend committee meetings to offer their views on a project's drafts. *See Project Life Cycle*, AM. L. INST., http://www.ali.org/projects/project-life-cycle/ [perma: http://perma.cc/FF57-BTHB] (last visited July 14, 2018).

30. The difficulty of formulating principles in this domain is exacerbated by the fact that we are trying to offer principles that would apply to both for-profit and not-for-profit organizations and both large and small organizations. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 2.02 cmt. a.

31. *Id.* § 1.01(x).

organization, is important to specify. After all, the duties of the highest legal authority was the subject of *Caremark*[32] and is often treated by regulation and in practical guidance.[33] As discussed below, the challenge of the ALI Compliance Project is articulating the duties of the highest legal authority while recognizing that its role is primarily reactive. Senior executives, with the help of internal control officers, design and propose compliance and risk-management programs to the highest legal authority for its approval.[34] In light of the authority's traditionally reactive role on these matters, it is important to identify the compliance and risk-management issues where, under our recommendation, the highest legal authority should take an active role. As I shall also highlight and as might be expected, this active role is evidenced by the use of specialized compliance and risk-management committees of the highest legal authority.[35]

The second issue, reporting by internal control officers, is clearly related to the first because the highest legal authority often exercises its oversight of compliance and risk management through its access to and reports from these officers.[36] This issue raises a governance matter because reporting has several meanings, from providing information to being subject to the authority of an organizational actor.[37] For example, internal control officers might provide information to the highest legal authority while also doing the same for senior executives who direct their activities in the organization.[38] How internal control officers balance these reporting responsibilities is explored further below.

The Essay will proceed as follows. Section I provides, as necessary background, a brief account of the growth of compliance and risk management and the basic elements of compliance and risk-management programs. Section II discusses the responsibilities of the highest legal authority in compliance and risk management and explores the approach that the ALI Compliance Project takes in dealing with issues arising from the authority's oversight of these domains. Section III then raises the issue of reporting by internal control officers and explains, and justifies, the tentative design of this reporting recommended by the Project.

I. COMPLIANCE AND RISK MANAGEMENT

Before talking about the specifics of the governance of compliance and risk management, it is useful to specify what exactly the fields of compliance and risk

32. *See In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996).

33. *See* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 8 (setting out the responsibilities of the governing body in compliance); *infra* notes 95–99 (providing examples from regulators).

34. See *infra* text accompanying notes 101–06 for examples of the responsibilities of management in developing and executing compliance and risk management programs.

35. *See infra* text accompanying notes 100–09.

36. *See infra* text accompanying notes 155–66.

37. See *infra* Section IV for a discussion of the methods employed by the highest legal authority to conduct a risk-management program.

38. See *infra* text accompanying notes 112–16 for a description of the roles of CCOs and CROs.

management are. Compliance is essentially an internal control function of an organization that is designed to ensure that the organization, its employees, and other agents comply with laws, regulations, applicable professional or industry standards, and the organization's ethical standards.[39] Typically, although not exclusively, this internal control function is represented by a compliance department, which is composed of compliance officers directed by the CCO.[40] The compliance department ensures that organizational actors comply with their legal and other obligations through the organization's compliance program, which sets forth the ways in which the department helps the organization and its employees achieve compliant conduct.[41]

Before outlining the basic elements of a compliance program, it may be helpful to say a few more words about why organizations need a compliance function.[42] In general, organizations are concerned that they will have liability because a wrongful act or crime is committed by one of their employees or agents acting on its behalf.[43] This organizational liability has its origins in tort and agency laws, which place liability upon an organization for tortious conduct done by its agents, particularly its employees.[44] The paradigmatic doctrine of organizational liability is respondeat superior.[45] This tort law doctrine, which criminal law adopted, provides that, in specific contexts, an organization may be criminally liable if an agent acting in the organization's business or affairs engages in criminal conduct.[46] In their early years, moreover, federal government agencies typically borrowed the common law doctrines of organizational liability in their own enforcement actions so that they could reach the firms where misconduct had occurred, in addition to prosecuting the violator.[47] In some cases, to supplement these common law doctrines, Congress

39. *See* GEOFFREY P. MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 3 (2d ed. 2017) ("'Compliance' refers to the processes by which an organization polices its own behavior to ensure that it conforms to applicable rules and regulations.").

40. *See* Griffith, *supra* note 14, at 2102–02.

41. Professor Miller defines a compliance program as "the mechanisms that an organization uses to ensure compliance, and the procedures that it employs when possible instances of noncompliance are discovered." MILLER, *supra* note 39, at 201. In an important rationalization of compliance, the Internal Standard Organisation referred to the mechanisms as "processes." COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 19.

42. The reasons have already been alluded to above. *See supra* text accompanying notes 4–9 for a discussion of the reasons for organizations to implement a compliance program.

43. *See* Griffith, *supra* note 14, at 2082–83 (describing this issue).

44. *See infra* note 45.

45. *See* RESTATEMENT (THIRD) OF AGENCY § 7.03 (AM. LAW INST. 2006) (stating the general liability of principal for actions of its agent); *cf. id.* § 7.05 cmt. a (explaining that this liability arises from the tort law concept that a person who is in a special relationship with another owes third parties a duty of reasonable care with respect to the foreseeable risks posed by that relationship).

46. *See* Samuel W. Buell, *The Blaming Function of Entity Criminal Liability*, 81 IND. L.J. 473, 491–500 (2006) (discussing the origins of the use of this liability in criminal law).

47. *See, e.g.*, Task Force on Broker-Dealer Supervision & Compliance of the Comm. on Fed. Regulation of Sec., *Broker-Dealer Supervision of Registered Representatives and Branch Office Operations*, 44 BUS. LAW. 1361, 1363–64 (1989) (discussing the initial legal theories for imposing supervisory liability upon broker-dealers by the Securities and Exchange Commission).

gave the government agencies express statutory power to prosecute firms and managerial employees for their failure to supervise employees and other agents if the latter violated laws or regulations.[48] Through the imposition of supervisory liability regulators effectively made firms use their resources and personnel (that is, supervisors) to ensure their employees' compliance with the applicable law and regulations.[49]

Given the risk of organizational liability, organizations thus need a firm function to keep track of all the legal obligations applicable to an organization and its employees and to specify how conduct can be done so as to comply with these obligations.[50] This need has grown as the obligations have proliferated, particularly in highly regulated industries.[51] The compliance department, led by the CCO and staffed with compliance officers, became that firm function, even if in early days and still in some organizations today it is undertaken by organizational actors who are not compliance officers.[52] Moreover, firms have been encouraged to establish compliance departments because, in some cases, having an effective compliance and supervisory system is a defense to organizational liability.[53] For example, the U.S. Sentencing Guidelines provide organizations with relief in sentencing if they have an effective (and Guidelines-specified) compliance and ethics program.[54] To take another example, a broker-dealer can escape supervisory liability if it establishes supervisory procedures, which direct its supervisors how to oversee the firm's brokers, and a supervisory system, which provides for adequate supervisory staffing and resources to implement the procedures, and if it then puts the system into effect.[55]

48. For a discussion of how this occurred with respect to broker-dealers under the federal securities laws, see James A. Fanto, *The Vanishing Supervisor*, 41 J. CORP. L. 117, 134–43 (2015) [hereinafter Fanto, *Vanishing Supervisor*] (discussing 15 U.S.C. § 78o(b)(4)(E) (2012), which imposed supervisory liability upon broker-dealers and defenses to that liability).

49. *See, e.g.*, Fanto, *Vanishing Supervisor*, *supra* note 48, at 138–39 (discussing how the Securities and Exchange Commission determined that it needed firm personnel to help with the enforcement of laws in broker-dealers). Organizational liability thus promotes "internal," as opposed to "external," enforcement of the law. *See* MILLER, *supra* note 39, at 197–228 (discussing "Internal Enforcement").

50. See MILLER, *supra* note 39, at 197–228 (his chapter on "Internal Enforcement").

51. *See* Kirsten Grind & Emily Glazer, *Nuns with Guns: The Strange Day-to-Day Struggles Between Bankers and Regulators*, WALL ST. J. (May 30, 2016, 10:39 PM), http://www.wsj.com/articles/nuns-with-guns-the-strange-day-to-day-struggles-between-bankers-and-regulators-1464627601 [perma: http://perma.cc/6PMT-V9FV] (discussing the proliferation of regulations affecting banks).

52. *See* John H. Walsh, *A History of Compliance*, *in* MODERN COMPLIANCE: BEST PRACTICES FOR SECURITIES & FINANCE 5, 5–62 (David H. Lui & John H. Walsh eds., 2015) (reviewing the history of compliance in the financial sector).

53. *See* Fanto, *Vanishing Supervisor*, *supra* note 48, at 134–43 (discussing the defense).

54. See *supra* note 9 and accompanying text for a discussion of the effect of a compliance program on an organization's liability under the U.S. Sentencing Guidelines.

55. *See* 15 U.S.C. § 78o(b)(4)(E) (2012) (providing this defense to supervisory liability for broker dealers). For a discussion of the SEC's interpretation of the elements of this defense, see James A. Fanto, *Surveillant and Counselor: A Reorientation in Compliance for Broker-Dealers*, 2014 BYU L. REV. 1121, 1179–80 [hereinafter Fanto, *Surveillant and Counselor*].

Indeed, Congress and regulatory agencies today require regulated firms to have a compliance program and specify in detail the program's requirements.[56] For example, in the regulation of swap dealers under Dodd-Frank, Congress required the dealers to have a compliance program and outlined what the program must involve.[57] The regulator assigned authority over this kind of firm (the SEC for security-based swap dealers and the Commodity Futures Trading Commission (CFTC) for swap dealers) then establishes in more detail through its regulation the required elements of the program.[58] In effect, as this example shows, compliance programs have become so standardized that Congress or a regulator can confidently enumerate their features.[59]

There are several basic elements of most compliance programs, which is a way of setting forth the typical responsibilities of compliance officers. Compliance officers draft the compliance policies and procedures, which explain, sometimes in considerable detail and in a step-by-step way, how employees and other agents are to conduct their activities in the organization in accordance with the applicable laws, regulations and ethical standards.[60] The policies outline the general purpose of or need for these standards of conduct, and the procedures provide the detailed guidance.[61] Naturally, these policies and procedures must be geared to the organization's activities and its particular risks of noncompliance, which means that they must be drafted to respond to a compliance risk assessment.[62] They must also be constantly updated and changed to reflect legal and other developments in these activities.[63] Supervisory policies and procedures guide supervisors in their supervision of the employees and might well be a part of the compliance policies and procedures.[64] Compliance officers also train and educate board members, executives, managers, employees, and agents in all these procedures.[65] This education includes activities promoting the

56. *See infra* notes 57–58.

57. *See* 15 U.S.C. § 78o-10(k)(1) (requiring each security-based swap dealer and participant to have a CCO).

58. *See* 17 C.F.R. § 3.3(a) (2017) (CFTC's implementing rule); 17 C.F.R. § 240.15Fk-1(a) (2017) (SEC's implementing rule).

59. *See* MILLER, *supra* note 39, at 197–220 (laying out some of the basic elements of compliance programs, such as establishing compliance policies and procedures, doing background checks, conducting training and monitoring and doing investigations).

60. *See* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 12 (listing these and other responsibilities of the compliance function in paragraph 5.3.4).

61. *See* MILLER, *supra* note 39, at 197, 201.

62. *See* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 7 (referring to paragraph 4.6 entitled the "Identification, analysis and evaluation of compliance risks").

63. *See, e.g.*, Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,993 (Feb. 23, 1998) (listing the CCO's responsibilities to include overseeing and monitoring implementation of the compliance program and periodically revising it).

64. *See* John H. Walsh, *Right the First Time: Regulation, Quality, and Preventive Compliance in the Securities Industry*, 1997 COLUM. BUS. L. REV. 165, 189–91 [hereinafter Walsh, *Right the First Time*] (describing compliance and supervisory procedures).

65. *See* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 12 (noting in paragraph 5.3.4 that the "compliance function . . . shall be responsible for . . . providing or organizing on-going training support for employees to ensure that all relevant employees are trained on a regular

organization's ethical standards that help define its culture.[66] The officers, moreover, monitor compliance with the procedures, which involves oversight and surveillance of the organization's employees and activities; today this often involves electronic surveillance.[67] If, in the course of this surveillance, compliance officers come upon a potential breach of the procedures, which could be a legal violation or a violation of firm ethical standards, they may investigate it and, if necessary, remedy it and refer the violator to the appropriate authority in the organization.[68] In the alternative, compliance officers may leave this kind of investigatory matter to the legal department, which can exercise attorney-client and other privileges in conducting an investigation.[69] Compliance officers also advise employees and others in the organization about the compliance implications of their decisions, particularly in borderline or "grey" areas where the procedures do not define well what compliant conduct is.[70] Finally, an important part of a compliance program is that it is regularly tested and audited to ensure that it is effective and that any problems in it are corrected.[71]

As noted, risk management did not emerge from a particular body of law. Instead, it was originally a financial practice dealing with the management of credit and market risks in the commercial banking sector.[72] As also noted above, risk management acquired a legal significance when it became legally mandated in large financial firms.[73] Risk management has arguably gone farther than

basis").

66. *See id.* at 16–17 (discussing compliance culture in paragraph 7.3.2.3).

67. *See* James Fanto, *Dashboard Compliance: Benefit, Threat, or Both?*, 11 BROOK. J. CORP. FIN. & COM. L. 1, 11–12 (2016) (explaining compliance monitoring and its current automation); *see also* KPMG, LEVERAGING TECHNOLOGICAL INNOVATION TO ESTABLISH A MORE EFFECTIVE REGULATORY ECOSYSTEM 3 (2017) (arguing for the need for "Regulation Technology" in firms so that they can become more efficient in compliance).

68. *See* COMM. OF SPONSORING ORGS OF THE TREADWAY COMM'N, INTERNAL CONTROL—INTEGRATED FRAMEWORK 150 (2012) [hereinafter INTERNAL CONTROL—INTEGRATED FRAMEWORK] (noting that collaboration between legal or 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").

69. *See* Michele DeStefano, *Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 10 HASTINGS BUS. L.J. 71, 122 (2014) (discussing this limitation on CCO's conducting an investigation).

70. *See* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 12 (explaining in paragraph 5.3.4, that one of the tasks of the compliance function is "providing objective advice to the organization on compliance-related matters"); *see also* Fanto, *Surveillant and Counselor*, *supra* note 55, at 1163 (discussing "internal" compliance, which includes providing advice).

71. This is done by the compliance officers themselves, *see* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 25 (paragraph 9.2), and also by the internal auditors. *See* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 151 ("The scope of internal auditing is typically expected to include oversight, risk management, and internal control, and assisting the organization in maintaining effective control by evaluating their [sic] 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.").

72. *See supra* text accompanying note 15–16.

73. *See supra* text accompanying note 21.

compliance in becoming an established part of organizations.[74] Indeed, it has become a dominant paradigm through which organizations assess conduct and has even influenced compliance.[75] Under the enterprise risk management (ERM) approach,[76] all risks facing an organization, whether in its activities or from outside, are identified and measured.[77] The organization then determines whether it can eliminate particular risks or amounts of risk, leaving residual risks.[78] The organization decides its "risk appetite"—the level of residual risk that is acceptable to it—and ensures that its risks stay within that risk appetite.[79] In other words, a given amount of risk is acceptable in most business activities.[80] Risk management, as well as ERM, is a disciplined way for an organization to conduct its activities and affairs in light of the ever-present risks.[81]

If an organization were to use this risk-management approach in compliance, it would identify the laws and regulations applicable to an organization and its actors and the organizational activities where there would be the greatest number of legal violations, generally those of a serious nature.[82] It would then try to prevent, or at least reduce the number of, these violations by putting most of its compliance resources in those areas.[83] However, organizational actors cannot publicly assert, as they would for nonlegal risks, that they accept or tolerate a certain number of legal violations in the organization's activities, even if they realize that a compliance program cannot prevent *all* violations.[84] Public authorities, such as regulators and prosecutors, expect them to espouse no tolerance for legal risks.[85]

The elements of a risk-management program, which a CRO and risk officers would administer, are similar in general format to those of the

74. *See* MILLER, *supra* note 39, at 710–17 (discussing risk management's history and establishment in organizations of all kinds).

75. *See id.* at 710.

76. *See* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 10 (defined as "[t]he culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value").

77. *See id.* at 62–68.

78. *See id.* at 69.

79. *See* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 17–20 (outlining this approach of understanding an organization's "risk profile," setting its "risk appetite" and dealing with variation in performance); *see also* MILLER, *supra* note 39, at 745–49 (discussing risk appetite and identification and acceptance of residual risk).

80. ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 17–20.

81. *See id.* at 6–7.

82. *See* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 17–20.

83. *Id.*

84. *See* MILLER, *supra* note 39, at 720 (noting that violations are part of operational risk); *id.* at 749 (observing, in an example, that a certain number of these violations are part of residual risk). It appears that organizations are trying to create risk appetites for non-financial risks, like compliance, and that compliance risk is one of their chief areas of concern. *See, e.g.*, EY, RETHINKING RISK MANAGEMENT: BANKS FOCUS ON NON-FINANCIAL RISKS AND ACCOUNTABILITY 35–36 (2015) (discussing "risk appetite").

85. *See* MILLER, *supra* note 39, at 711.

compliance program. With the assistance of senior executives, risk officers conduct an intensive evaluation of the risks facing their organization and assess their probability of occurrence.[86] At this point they would present the information to the organization's governing body, with a proposal from senior management about which risks and levels of risk could be eliminated, which are the residual risks, and which of such residual risks are acceptable for the organization to incur.[87] This would be the organization's risk appetite, typically embodied in a risk appetite statement.[88] With the risk appetite statement as a guidepost, the risk officers enact controls so that the organization's risks are managed so as to stay within the limits or parameters of the risk appetite statement.[89] As in the case of compliance, the risk officers instruct organizational actors about the risk limits, monitor the actors' compliance with these limits, provide advice on risk-management issues, and investigate any violations of the risk-management program. In addition, they must periodically test the risk-management program and update it to take account of new, emerging risks or of an enhancement of existing ones.[90]

As the reference to actions of risk officers, senior management, and the governing authority make clear, governance is an essential part of compliance and risk-management programs. These programs assign responsibility for compliance and risk management in an organization and set forth a chain of command for compliance and risk-management decisionmaking and responsibilities. Indeed, the classical tripartite view of internal control has much to do with governance.[91] Under this view, internal control officers like compliance officers and risk officers design and administer compliance and risk-management programs, organizational actors do their business in accordance with these programs, and internal auditors verify that both the officers and actors are conducting themselves in line with the programs and that the programs

86. *See* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 44–46.

87. *See* ABA Section of Bus. Law, Comm. on Corp. Laws, *Corporate Director's Guidebook—Sixth Edition*, 66 BUS. LAW. 975, 986, 998–1000 (2011).

88. *See* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 47–50; *see also* ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 998 (discussing a public company board's expected understanding a firm's risk profile and its management of risks). Board risk oversight has traditionally been the task of the board audit committee. *See, e.g.*, NYSE, 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.").

89. *See, e.g.*, BASEL COMM. ON BANKING SUPERVISION, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS ¶ 107 (2014) (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" in paragraph 107); *see also* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 53–59.

90. *See* ENTERPRISE RISK MANAGEMENT, *supra* note 23, at 100–01 (discussing monitoring ERM and improving it). Risk officers also oversee the communication to all organizational actors concerning risks and the organization's risk limits and controls. *See id.* at 90–92; *see also* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 149.

91. *See* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 145–52 (describing the internal control duties of the main governance actors).

themselves are effective.[92]

II. THE ROLE OF THE HIGHEST LEGAL AUTHORITY AND ITS COMMITTEES

A crucial governance issue in compliance and risk management is the role of the organization's highest legal authority in these internal control functions. The highest legal authority is the generic name for the supreme governing body in an organization, like the board of directors in a public company or a board of trustees in a large not-for-profit.[93] It is now well established that this authority must oversee the organization's compliance and risk management programs just as it oversees and supervises all organizational activities.[94] This is the import of *Caremark*, at least for compliance: the board of directors must ensure, as part of its duty of care, that a company has a compliance program adequate for its circumstances.[95] Regulators and other government authorities have affirmed, or reaffirmed, this oversight responsibility of the highest legal authority.[96] Under the U.S. Sentencing Guidelines, referenced as support by the Court of Chancery in *Caremark*,[97] an organization may receive credit in sentencing for its compliance and ethics program if, among other things, the highest legal authority has oversight responsibility over it.[98] In numerous industries, regulators require that the board or its equivalent of the regulated organization approve the establishment of a compliance and risk-management program.[99]

The central inquiry, then, becomes identifying the elements of this oversight responsibility or, put another way, explaining how the governing authority would exercise this responsibility. At the very least, as *Caremark* suggests, the governing authority must ensure that the senior executives of an organization establish compliance and risk-management programs adequate for the organization's circumstances.[100] But how exactly this allocation of responsibilities of the authority and the executives works is an important

92. *See id.* at 147.

93. *See supra* note 31.

94. *See, e.g.*, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 8 (setting forth the compliance responsibilities of the governing body).

95. *See, e.g.*, *In re* Caremark Int'l Inc. Derivative Litig., 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 . . . .").

96. *See infra* notes 97–99.

97. *See Caremark*, 698 A.2d at 969.

98. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(A) (U.S. SENTENCING COMM'N 2016).

99. *See, e.g.*, 17 C.F.R. § 270.38a-1 (2017) (mandating board approval of the compliance program of a registered investment company, as well as those of its advisors and service providers); 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 large financial institutions by their boards); 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 health-care board's responsibility for oversight of compliance).

100. *See Caremark*, 698 A.2d at 970.

governance issue. This is, not surprisingly, a focus of the ALI Compliance Project. We recognize that, in all but the smallest organizations, the members of the governing authority are generally outsiders to the functioning of the organization and thus different from the senior executives.[101] We understand that a typical organizational practice has senior executives, assisted by the internal control officers, formulate, and propose for approval by the governing authority, the compliance and risk-management programs.[102] As in many other organizational matters, the governing authority is thus reacting to, and expected to consider and ultimately to approve or disapprove, the proposals.[103] This makes sense because, under the law of most organizations, the governing authority oversees, and does not direct or manage, the organization's business or affairs.[104]

Certainly, the governing authority should not just passively accept executives' proposals on compliance and risk management; their fiduciary duty demands more.[105] Without expecting the governing authority's members to rethink the compliance program proposal, on the basis of their own experience and of the information provided to them, they should actively evaluate the proposal and be convinced that it makes sense for the organization. To do this they should have the background, experience or education, or receive advice, to understand the legal obligations to which the organization and its employees and other agents are subject. Advice could come from the general counsel, the CCO, or outside compliance experts. Each could provide an understanding of the design of an appropriate compliance program for organizations comparable to their own.[106] Therefore, an issue for the ALI Compliance Project is to have a

101. *See* ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 1005 (making this point). There may be some overlap, of course, as in the case of public companies where the chair of the board is often the chief executive officer.

102. *See* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 150–52 (discussing these responsibilities); *see also* KPMG, THE COMPLIANCE JOURNEY: BOOSTING THE VALUE OF COMPLIANCE IN A CHANGING REGULATORY CLIMATE 5 (2017) (discussing the breakdown of responsibilities).

103. *See, e.g.*, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 8 (observing that the governing body formally approves the compliance policy, and top management makes sure that the commitment to compliance is realized in the organization).

104. *See, e.g.*, MODEL BUS. CORP. ACT § 8.01(b) (AM. BAR ASS'N 2016) ("[A]ll corporate powers shall be exercised by or under the authority of, the business and affairs of the corporation shall be managed by or under the direction, and subject to the oversight, of its board of directors.").

105. *See* Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006) (noting that liability can attach to directors where "(a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention").

106. *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 general counsel's role in providing information to directors and executives on legal risks); *see also* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(A) (U.S. SENTENCING COMM'N 2016) (stating that an "organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program").

principle on the expected background and education (and continuing education) of the members of the governing authority so that they will have the competence to evaluate knowledgeably management's proposed compliance program.[107]

A similarly engaged governing authority should approve the risk-management program.[108] Indeed, one would expect that the members of the authority would be considerably involved in risk management because, given their backgrounds as senior executives of other organizations, they are likely to have a good understanding of business and operational risks,[109] and because they have had to propose risk appetites and limits for their own organization.[110] As in the case of compliance, the members of the authority are likely to draw upon the expertise of the organization's risk specialist, the CRO, and outsider advisors, such as risk consultants, as well as their own experience, in performing their risk-oversight role.[111] There is likely to be, or should be, a vigorous debate between governing authority members and executives over the risk-management program. The kinds and levels of risk that an organization accepts and manages are intertwined with its affairs, business, strategies and their ultimate success, whereas the management of legal risks through the compliance program, while important, is just one part of the overall ERM strategy.[112]

Other than to review and approve the compliance and risk management programs, what else should be demanded of the governing authority in these domains? Compliance and risk management programs must have adequate staffing and resources so that they can be put into effect, and the CCO and the CRO must be sufficiently independent of the organization's activities and have the necessary authority to implement the programs so that the activities are effectively controlled. Staffing, allocation of resources, and authority are managerial matters, but as part of its oversight responsibility, the governing authority should be reasonably satisfied that the resources are adequate to make

107. This principle is currently in Section 3.06. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.06 cmt. c. It should be noted here that programs exist for new public-company directors, some in affiliation with universities, which covers such issues as board oversight. *See, e.g.*, *Directors Consortium*, STAN. U. GRADUATE SCH. OF BUS., http://www.gsb.stanford.edu/exed/directors/ [perma: http://perma.cc/RSE8-A2CL] (last visited July 14, 2018).

108. *See supra* notes 12–14 and accompanying text. After the financial crisis, there has been considerable focus worldwide on a board's oversight responsibilities with respect to an organization's risk management. *See, e.g.*, G20/OECD, *supra* note 19, at 56 (noting that "the board should retain final responsibility for oversight of the company's risk management system"); *see also* 17 C.F.R. § 229.407(h) (2017) (mandating that all public companies "disclose the extent of the board's role in the risk oversight of the" company).

109. *See, e.g.*, ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 986, 998 (describing a board's understanding of a firm's risk profile and its management of risks); *id.* at 987 (describing an individual director's understanding of a firm's kinds of risk).

110. *See supra* text accompanying notes 78–81.

111. *See* NAT'L ASS'N OF CORP. DIRS., REPORT OF THE NACD BLUE RIBBON COMMISSION ON RISK GOVERNANCE: BALANCING RISK AND REWARD 10–11 (2009) (discussing use of independent consultants).

112. *See supra* note 76–80 and accompanying text.

the programs effective.[113] The authority of internal control officers in an organization is also typically within senior management's domain.[114] The CCO and the CRO should have the power to administer their programs, which at the very least means obtaining information about the organization's business or affairs so that they can monitor them in accordance with the programs. Therefore, when senior executives bring the compliance and risk management programs to the governing authority for its approval, the authority has to be satisfied that the CCO, the CRO and the other compliance and risk officers will have the necessary organizational authority.[115] In addition, the authority's review and approval of the compliance and risk-management programs is not just a one-time decision. Rather, the governing authority should review the effectiveness of the programs, at an interval that it should determine but at least yearly, and inquire of senior executives and of the CCO and the CRO whether they see the need for and would propose any revisions to them.[116]

Internal control officers must be independent so that they can engage in their work free of undue influence from those conducting the organization's business, whom the officers are monitoring and who may resist the restrictions imposed upon them by the compliance or risk-management programs.[117] Independence is also related to the issue whether an internal control officer can wear two hats, an internal control one and an operational one.[118] The ALI

113. *See, e.g.*, U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C) (U.S. SENTENCING COMM'N 2016) (noting that the person 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"); ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 1000 ("Boards should also ensure the compliance program has adequate resources and authority to perform its function."). The ALI Compliance Project does this through section 3.07(a)(6). *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.08(a) ("[T]he authority should . . . [b]e familiar with the staffing and resources allocated by executive management to the internal-control functions of compliance, risk management, and internal audit and satisfy itself that the functions are sufficiently independent and have appropriate authority to perform their respective internal control responsibilities . . . .").

114. The issue of authority can raise questions about the liability of internal control officers for legal violations occurring in an organization. *See, e.g.*, Fanto, *Surveillant and Counselor*, *supra* note 55, at 1179–80 (discussing supervisory liability of compliance officers in broker-dealers).

115. *See supra* note 86.

116. *See, e.g.*, U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(5)(B) (an organization with an effective compliance and ethics program "evaluate[s] periodically the effectiveness of the organization's compliance and ethics program"); BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 99, 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."); ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 999 (discussing a public company board's review of the compliance program and its effectiveness). The ALI Compliance Project does this through Section § 3.08(a)(9). *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.09(a)(9).

117. COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 11 (stating in paragraph 5.3.3(e) 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).

118. *See* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 95–96 (discussing

Compliance Project takes the position, echoed in regulation,[119] that having a person conduct both internal control and other organizational responsibilities is permissible (other than internal audit responsibilities),[120] but is not recommended in large organizations that, because of their size and complexity, require specialized internal control officers.[121] The governing authority's contribution to internal control officers' independence is, at a minimum, twofold: (i) it approves the hiring and dismissal of the officers,[122] and (ii) it has a direct line of communication with the officers because they regularly report to it.[123]

generally the separation of control functions from others in an organization).

119. *See, e.g.*, FIN. INDUS. REGULATORY AUTH., FINRA MANUAL § 3130 supplementary material .08 (2008), http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=6286 [perma: http://perma.cc/J87E-FJVG] ("The requirement to designate one or more chief compliance officers does not preclude such persons from holding any other position within the member [organization], 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.").

120. *See* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 151 ("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.").

121. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.20(a) ("By reason of its size, limited resources or operations, or in other circumstances, an organization may elect to have an internal control officer be responsible for multiple internal-control functions or for non-internal-control operations."); *see also* BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS ¶ 28 (2005) [hereinafter BASEL COMM., COMPLIANCE AND THE COMPLIANCE FUNCTION] ("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."); INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 149 (providing support for this approach, stating "[i]n large and complex organizations, specialized compliance professionals can be helpful in defining and assessing controls for adherence to both external and internal requirements"). *But see* Donald C. Langevoort, *Monitoring: The Behavioral Economics of Corporate Compliance with Law*, 2002 COLUM. BUS. L. REV. 71, 100–03 (discussing the factors that an organization may consider in adopting a compliance function that is not the most independent).

122. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.08(a)(7). There is considerable support for this approach. For example, 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) (2017). The U.S. Commodity Futures Trading Commission's regulations of futures commission merchants, swap dealers, and major swap participants allow either the board of directors or a senior officer to appoint, remove, and determine the compensation of the chief compliance officer. *See* 17 C.F.R. § 3.3(a) (2017); *see also* BASEL COMM., COMPLIANCE AND THE COMPLIANCE FUNCTION, *supra* note 121, ¶ 27 (recommending that the board of directors of a large banking institution be informed about the hiring and departure of the chief compliance officer and the reasons for that departure).

123. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.08(a)(8) (discussing lines of communication); *see also* COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 11 (requiring that the governing body and top management have a compliance function with "clear and unambiguous support from and direct access to the governing body and top management" in paragraph 5.3.3(d)(2)); Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed.

The first allows the governing authority to check that appropriate people are being hired for these positions, that they are properly compensated, and that they are not dismissed because of management's desire to hide internal control problems or deficiencies in the organization.[124] The second contributes to the independence by allowing the internal control officers to discuss their concerns directly with the governing authority, unfiltered and uninfluenced by senior executives.[125] It also enables the authority to engage in ongoing oversight, in addition to periodically approving the proposals of senior executives, with respect to compliance and risk management and to be better prepared to make their supervisory decisions on these subjects.[126]

The highest legal authority is also responsible when there has been a material violation or failure of the compliance program or a material failure of or deviation from the risk-management program. "Material" would have to be defined, but, in the compliance area, it could involve, among other things, legal violations, or a pattern of legal violations, occurring in the organization that could have significant criminal or civil repercussions for the organization.[127] In risk management, material deviations or failures would be those actions beyond the organization's risk appetite, limits, or controls that could threaten the organization's business and financial position.[128] There are likely two ways for these matters to be presented to the governing authority. In the one, which relies upon the governance hierarchy, internal control officers detect the violation, failure, or deviation and bring it to the CCO or CRO, who alerts senior executives.[129] The executives, with the advice of the CCO and CRO, then resolve upon a course of action, which could include discipline of the employees involved, remedial measures to fix the problem, and possibly reporting to a regulator or to other government authorities.[130] The governing authority would approve, modify, or ratify the recommended course of action, in consultation

Reg. 8,987, 8,993 (Feb. 23, 1998) (requiring that the CCO report to the hospital's governing body, CEO, and compliance committee). The U.S. Sentencing Guidelines make this reporting by the CCO to the highest legal authority and to "high-level personnel" an element of an effective compliance program. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2)(C) (U.S. SENTENCING COMM'N 2016).

124. *See supra* note 117.

125. *See* MICHAEL D. GREENBERG, RAND CORP., TRANSFORMING COMPLIANCE: EMERGING PARADIGMS FOR BOARDS, MANAGEMENT, COMPLIANCE OFFICERS, AND GOVERNMENT 24–25 (2014) (discussing the importance of this reporting).

126. *See* Walsh, *Right the First Time*, *supra* note 64, at 236 (discussing generally the value of this reporting in financial firms like broker-dealers and investment advisers).

127. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 1.01(hh) (defining "material" as "[s]ignificant to an organization's reputation, effective functioning, or financial position").

128. *See* ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 999 (explaining that the 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") (emphasis added)).

129. The ALI Compliance Project takes this approach. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.08(a)(10) (directing the highest legal authority to confer with executive management).

130. *See id.*

with the CCO or CRO and outside consultants, if need be.[131] If the material violation, failure, or deviation implicated senior executives themselves or their management, the governing authority may learn of the problem through the direct reporting of internal control officers that was discussed above or through a system of anonymous reporting.[132] In these kinds of cases, which could involve a management crisis, the governing authority would have to determine the appropriate response to the material violation, failure, or deviation.[133]

In the ALI Compliance Project, we recognize that it is a well-established practice for a governing authority to delegate its oversight of internal control to one of its committees.[134] This practice has the benefit of allowing a group of members of the governing authority to develop expertise in that area, which enhances the authority's oversight of it.[135] An important question for us is whether to recommend that organizations establish specialized committees for the oversight of compliance and risk management. For public companies, under stock exchange rules and corporate practice, these tasks have often fallen to its audit committee that oversees a company's financial reporting and thus the internal and external auditors, who also audit compliance and risk-management programs, in addition to the company's preparation of financial reports.[136] However, the typical audit committee is likely to be considerably overworked,[137] and stock exchange rules permit it to delegate certain of its duties, like the oversight of compliance, to another board committee.[138]

131. *See id.* (directing the highest legal authority to approve or ratify remedial measures); *see also* BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 99, at *8 ("The board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by senior management.").

132. This could occur through reporting in a confidential hotline for whistleblowers. In public companies, the audit committee is generally tasked with this responsibility to administer the hotline. *See* NYSE, *supra* note 88, § 303A.07(b).

133. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.08(a)(11) & cmt. i (demonstrating that the ALI Compliance Project has this approach as one alternative for the governing authority). *See generally* NAT'L ASS'N OF CORP. DIRS., *supra* note 111, at 40 (discussing "crisis management plan" for governing authorities or boards).

134. Years ago, the ALI's Principles of Corporate Governance recognized 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 powers, subject to the board's ultimate responsibility for oversight over the matter. *See* PRINCIPLES OF CORP. GOVERNANCE: ANALYSIS AND RECOMMENDATIONS § 3.02 & cmt. j (AM. LAW INST. 1994) (describing delegation of powers); *see also* MODEL BUS. CORP. ACT § 8.25(d) & cmt. (AM. BAR ASS'N 2016) (permitting such delegation and discussing the practice). The ALI Compliance Project includes this power for the governing authority. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.08(b).

135. This positive side of delegation must be balanced with the interest in not reducing the responsibilities of the entire board. *See* MODEL BUS. CORP. ACT § 8.25 cmt.

136. *See* ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 998–1000 (discussing use of committees in risk management and compliance); *id.* at 1015–19, 1021–22 (describing audit committee's responsibilities, which include oversight of internal audit and compliance).

137. *See, e.g.*, KPMG'S AUDIT COMM. INST., 2015 GLOBAL AUDIT COMMITTEE SURVEY 4 (2015) (discussing the increasingly difficult nature of the audit committee's workload).

138. *See* ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 998–1000 (noting

The ALI Compliance Project considers it useful to give organizations frameworks for their compliance committee and risk committees.[139] There are models for these kinds of committees from different domains, particularly, although not exclusively, from the regulation of large commercial banks and financial groups.[140] With the assistance of the CCO or the CRO, as the case may be, and its own advisors, a committee would engage in the general oversight of compliance or risk management that the governing authority performs, as discussed above.[141] However, because of its specialized mission, a compliance or risk committee could be more extensively involved with the particular internal control function, without usurping the role of senior executives.[142] For example, this kind of committee might approve any public disclosure and reporting to regulators about compliance or risk management, apart from the reporting associated with material violations, failures or deviations.[143] It could also consult formally or informally with other committees on matters affecting compliance or risk management. For example, the ALI Compliance Project recommends that each committee meet with the organization's compensation committee, which has oversight of the compensation practices of the organization, in order to discuss how these practices might reward an executive for conduct in line with the compliance and risk-management programs.[144] In addition, some

how companies have established a compliance or legal affairs committee to ease the burden of the audit committee).

139. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.10 (Compliance and Ethics Committee); *id.* § 3.11 (Risk Committee).

140. For example, federal bank regulators have provided a detailed model for a risk committee since they mandate that large banking institutions have it. Section 165(h) of the Dodd-Frank Act directed the Board of Governors of the Federal Reserve to require that publicly traded nonbank financial companies supervised by it and publicly traded bank holding companies 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. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111–203, § 165(h), 124 Stat. 1376, 1429 (2010) (codified as amended at 12 U.S.C. § 5365(h)); *see also* 12 C.F.R. § 252.22 (2017) (risk-committee requirement for publicly traded bank-holding company having total consolidated assets of not less than $10 billion); *id.* § 252.33 (risk-committee requirement for a large bank-holding company having total consolidated assets of not less than $50 billion).

141. *See supra* notes 29–35; *see also* NAT'L CTR. FOR PREVENTIVE LAW, *supra* note 13, at 70.

142. *See, e.g.*, NAT'L CTR. FOR PREVENTIVE LAW, *supra* note 13, at 70, 83 (discussing how a company can create an independent board committee to oversee the CCO).

143. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.10(d)(8)–(9) (describing the Compliance and Ethics Committee's involvement in these tasks); *id.* § 3.11(d)(8)–(9) (describing the Risk Committee). In regulated firms, including banks, broker-dealers, and investment advisers, regulators may examine the firms, and part of this examination covers matters like compliance and risk management. *See, e.g.*, BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 99, at 2 (stating its expectations for compliance-risk-management programs at large banking organizations, to be overseen by its examination staff). Even public companies must disclose aspects of their compliance programs and risk management. 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. NYSE, *supra* note 88, § 303A.10.

144. Thus, the ALI Compliance Project recommends that the Compensation Committee meet with the Compliance and Ethics Committee and the Risk Committee for this purpose. *See* ALI

organizations have management-level compliance and risk committees, on which the internal control officers sit, to help ensure that the compliance and risk-management programs are followed throughout the organization.[145] A specialized committee of the governing authority could regularly meet with these management-level committees and thus have a deeper understanding of the implementation of the programs.

One question that the specialized committees raise is the value of enhanced oversight of compliance and risk management—do its benefits justify its increased costs? In certain domains, such as the regulation of large financial institutions, Congress and regulators have concluded that this kind of sustained oversight of risk management is worth the cost.[146] Given the existential threat to an organization posed by material breakdowns in its compliance, we suspect that the governing authority's involvement in compliance oversight will continue to increase, even if compliance committees are not yet the norm.[147] Some have expressed a concern that this specialized approach is costly, has not been proved to be effective, and removes flexibility from organizations that might take a different approach in their oversight of compliance.[148] We on the ALI Compliance Project sidestep the cost-benefit issue by, as noted above, providing organizations with models of committees that they are free to use or to reject, depending upon their own circumstances and the demands of their regulators.

Finally, an important governance issue is the role of the governing authority in the selection and promotion of organizational ethical values and culture with respect to compliance and risk management. Another way of stating this is defining the "tone at the top," a phrase often used to describe the governing authority's role in these issues.[149] This phrase appears to mean that, by their

COMPLIANCE PROJECT, *supra* note 2, § 3.13. As one source of support for this approach, in large bank holding companies 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).

145. COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 10 (noting that some organizations "have a cross-functional compliance committee to coordinate compliance across the organization" in paragraph 5.3.2).

146. *See supra* notes 93–99 and accompanying text.

147. *See* PwC, PWC STATE OF COMPLIANCE STUDY 2016: LAYING A STRATEGIC FOUNDATION FOR STRONG COMPLIANCE RISK MANAGEMENT 3, 13 (2016) (describing a global survey of 800 executives revealing that 20% of firms have "separate, stand-alone compliance/ethics committee," while 65% report that the audit committee oversees compliance); SOC'Y OF CORP. COMPLIANCE & ETHICS & NYSE GOVERNANCE SERVS., COMPLIANCE AND ETHICS PROGRAM ENVIRONMENT REPORT 27–28 (2014) (describing a survey of compliance officers in diverse organizations revealing that, where 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).

148. *See* Griffith, *supra* note 14, at 2116–17 (discussing the SEC's imposition of compliance programs without cost/benefit analysis).

149. *See, e.g.*, Richard G. Ketchum, Chairman & Chief Exec. 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."), http://www.finra.org/newsroom/speeches/052316-remarks-2016-finra-annual-conference [perma: http://perma.cc/3UP5-GDTS].

words and actions, members of the governing authority espouse and exhibit the values of the compliance and risk-management programs.[150] They conform to them and urge other organizational actors to do the same.[151] But what exactly does this mean in concrete terms, other than for them to exercise dutifully their oversight responsibilities, as discussed above? This issue is an important one for organizations, for organizational scholars and social psychologists have long established what practitioners often echo: an organization with a culture of compliance and risk management will be more likely than another to avoid the kind of systemic problems that bring down firms.[152] The ALI Compliance Project discusses these issues in the commentary and the relevant literature is referenced in the Reporter's notes.[153] It may be that the governing authority particularly demonstrates its commitment to organizational values by its actions with respect to the senior executives, such as when it dismisses them upon any evidence of conduct contrary to the organization's values, and by not taking outsized compensation and benefits for its members.[154]

III. REPORTING BY INTERNAL CONTROL OFFICERS

Another important governance issue for the ALI Compliance Project, which is related to the above discussion of the responsibilities of the governing authority, involves the reporting lines of the CCO and the CRO. As noted above, for example, this reporting to the governing authority could promote the independence of these officers and enhance the authority's knowledge of the organization's compliance and risk-management programs.[155] The concept of reporting generally has two meanings in organizations. In its strongest sense, reporting means that an internal control officer works under the direction of a

150. *See* NAT'L CTR. FOR PREVENTIVE LAW, *supra* note 13, at 125 (discussing how senior management sets the appropriate "tone" for an organization's compliance).

151. *Id.*

152. *See* Linda Klebe Treviño et al., *Legitimating the Legitimate: A Grounded Theory Study of Legitimacy Work Among Ethics and Compliance Officers*, 123 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 186, 195 (2014) (discussing the importance of support for compliance by boards and senior executives); *see also* 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); Donald C. Langevoort, *Cultures of Compliance*, 54 AM. CRIM. L. REV. 933, 966–67 (2017) (underlining the importance of board members and officers promoting ethical conduct, but emphasizing the individual and institutional pressures that run counter to this promotion).

153. The Project has a provision requiring that the governing authority and executive management "promote an organizational culture of compliance and sound risk management." ALI COMPLIANCE PROJECT, *supra* note 2, § 3.07(a). It then suggests a number of ways for them to do this: (i) approving the values, ethical standards, and risk culture; (ii) satisfying themselves that organizational practices support these values, standards, and culture; (iii) assuring themselves that employees and agents will live up to them; and (iv) communicating, and demonstrating by their actions, and their adherence to them. *Id.* § 3.07(b)(1)–(4).

154. *See, e.g.*, BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 99, at 7 (stating that the board should make sure that incentive structures promote compliance).

155. *See supra* text accompanying notes 117–22.

particular executive, who has the authority to determine the conditions of the officer's employment and to hire and fire him or her; the officer is a "direct report" of the executive.[156] Under the other meaning, which is actually subsumed in the first, the internal control officer provides information to and advises an executive, the governing authority or one of the latter's committees.[157]

Organizations have numerous possibilities with respect to the reporting, in both senses of the term, by the internal control officers.[158] Take first the question of to whom the CCO or CRO should report, that is, who has direct control or authority over the officer. One possibility is that they report to a senior executive, even to the CEO.[159] As officers in an organizational hierarchy, it would make sense that they should be subject to the authority of another executive who decides to hire them, sets their compensation and other terms of employment and, if they do not fit in or perform satisfactorily, to fire them.[160] On the one hand, if the governing authority, or a committee of the same, were to have complete control over internal control officers, this control might detract from the managerial power of senior executives, particularly the CEO, who generally have authority over lesser officers in an organization.[161] On the other hand, as noted above, giving the governing authority a veto or check on the hiring and firing of CCO and the CRO might make sense in terms of enhancing the authority's oversight of the compliance and risk management functions.[162]

Assuming that these internal control officers report to another executive, which executive should have direct authority over them? The CCO could report to the CEO, the chief operating officer, the chief financial officer, the CRO or the general counsel, to name a few possible reporting structures.[163] General counsels and their intellectual supporters have made a case for having the CCO in their reporting line because they are the central legal authority in an organization (compliance after all mainly deals with compliance with the law) and because they have oversight of all legal proceedings affecting the organization, such as investigations.[164] It thus might make sense to have CCOs

156. *See* LRN, THE 2014 ETHICS AND COMPLIANCE PROGRAM EFFECTIVENESS REPORT 9 (2014) (distinguishing "reporting" to another officer or the board from "updating" the board).

157. *See id.*

158. *See id.* (identifying four such possibilities); LRN, THE 2015 ETHICS AND COMPLIANCE EFFECTIVENESS REPORT 7 (2015) [hereinafter LRN, THE 2015 REPORT] (identifying eight such possibilities).

159. *See* LRN, THE 2015 REPORT, *supra* note 158, at 7 (identifying this as a common reporting structure).

160. *See* NAT'L CTR. FOR PREVENTIVE LAW, *supra* note 13, at 79–84 (discussing generally how the organization's compliance officer fits within the structure of the organization).

161. *See* ABA Section of Bus. Law, Comm. on Corp. Laws, *supra* note 87, at 985 (pointing out that the board typically delegates management of the firm to professional managers).

162. *See supra* text accompanying notes 117–22.

163. *See supra* notes 155–57.

164. *See* Bird & Park, *supra* note 106 (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); DeStefano, *supra* note 69 (comprehensively covering the relationship of compliance

report to the general counsel because, if the CCOs' monitoring uncovered legal violations, they could hand the matter over to the general counsel's office. In addition, from a historical perspective, legal departments initially performed compliance tasks, and only gradually did compliance departments (and compliance officers) separate organizationally from them.[165]

As noted above, the compliance function manages legal risk and thus nominally fits within the ERM framework.[166] Accordingly, the CCO could be placed in the reporting line to the CRO, which occurs in some organizations.[167] Yet, as also observed earlier,[168] although compliance today takes a risk-based approach, in that compliance officers are expected to do an analysis of legal risks before formulating their compliance programs, ERM does not completely harmonize with compliance. While CCOs may privately acknowledge that they cannot prevent every legal violation and will devote their resources to the most serious legal risks, they cannot publicly acknowledge that the organization will accept a certain amount of legal violations in the same way that CROs design a risk-management program where the organization bears certain risks.[169]

The reporting line (again in the strong sense) of the CRO is not without its issues as well. Given that the management of risk is an essential part of all business, an organization may decide to have multiple CROs, or risk officers, embedded in different business divisions, or even no risk officers at all (with business executives performing that function instead), rather than having only one CRO who oversees risk management for the organization.[170] CRO or risk officer reporting could thus be diffused and firm specific, and it might even be to a management-level risk committee, rather than to a senior executive.[171] The issue of what kind of reporting the CRO should make to the governing authority remains (that is, should it be only informational?), but it does not make much sense for the authority to be heavily involved in directing risk management practices (as opposed to overseeing them) in a typical organization because many organizational actors, directed by senior executives, are typically engaged

and legal departments, regulators' pressures to separate the two, and the intellectual debates on the merits of the separation). 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* LRN, THE 2015 REPORT, *supra* note 158, at 7 (showing that, collectively, chief compliance officers report more to others, such as the audit committee and the chief executive officer, than to the general counsel, although the latter remains the largest single reporting line); SOC'Y OF CORP. COMPLIANCE & ETHICS & NYSE GOVERNANCE SERVS., *supra* note 147, at 11.

165. *See* Griffith, *supra* note 14, at 2101–02 (discussing this movement of the compliance function 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).

166. *See supra* text accompanying note 112.

167. *See* LRN, THE 2015 REPORT, *supra* note 158, at 7.

168. *See supra* text accompanying note 85.

169. *See supra* notes 79–81 and accompanying text.

170. *See generally* MILLER, *supra* note 39, at 151–53 (discussing the CRO position generally and providing data on how common the position has become).

171. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.09.

in risk management at all levels of an organization.[172]

In addition, internal control officers, like the CCO and CRO, and their supporters may prefer that their "strong" reporting runs only to the CEO, not to other senior executives.[173] This reporting line would give them a seat at the CEO's conference table, would reflect the institutional importance of their internal control functions, would ensure that they have access to the CEO on internal control matters, as opposed to having their concerns passed along through another executive, and would also likely mean that the internal control officers are themselves senior executives.[174] This reporting would also reflect the professional project of compliance officers, who want their position to be recognized as an independent internal control activity that is governed by established principles of practice and that has the same authority as do lawyers and general counsels of an organization.[175] If the CCO is a lesser officer or executive, this professional project is undermined, or at least not promoted, because the compliance officer position would have less organizational status and recognition. A similar professional story could be made about the position of the CRO and risk officers.[176]

The ALI Compliance Project does not take a firm position on this reporting issue, because we want to acknowledge the different reporting solutions that organizations adopt and to provide them with the flexibility to structure this reporting as they see fit. Certainly, it recommends, particularly for large organizations, that the CCO and CRO report directly to senior executives like the CEO, not through another reporting line.[177] As noted above, this enhances the organizational importance of the internal control functions and encourages the CEO to deal with compliance and risk-management issues as part of decisionmaking and strategy. And it reflects the trend in organizations.[178]

The second reporting issue, which was already discussed in connection with the governing authority's responsibilities, is to whom, other than senior executives, internal control officers provide reports about their internal control

172. *See* INTERNAL CONTROL—INTEGRATED FRAMEWORK, *supra* note 68, at 149 ("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.").

173. *See, e.g.*, NAT'L CTR FOR PREVENTIVE LAW, *supra* note 13, at 81–82 (discussing how to enhance top compliance official's authority by having that officer be a senior executive who reports to the CEO).

174. *See id.* at 82–84 (referencing these issues).

175. *See* Christine Parker, *Lawyer Deregulation via Business Deregulation: Compliance Professionalism and Legal Professionalism*, 6 INT'L J. LEGAL PROF. 175, 188–89 (1999) (discussing the creation of a new compliance profession); John H. Walsh, *Institution-Based Financial Regulation: A Third Paradigm*, 49 HARV. INT'L L.J. 381, 411–12 (2008) (discussing the internal control project).

176. *See generally* Mikes, *supra* note 16 (discussing the growth in importance of CROs).

177. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.16(a) & cmt. a (CCO); *id.* § 3.17(a) & cmt. a (CRO).

178. *See, e.g.*, LRN, THE 2015 REPORT, *supra* note 158, at 7–8 (giving CCO reporting structures).

function and other information. The Project recommends that the CCO and the CRO have an informational reporting line to the governing authority or to a committee of that authority.[179] The CCO could report to a compliance committee, and the CRO could report to the risk committee; in the absence of these committees, both could report to the audit committee or to the full governing authority. This governance structure would reinforce the independence of the control officers from senior executives and would further the governing authority's oversight of compliance and risk management, as was discussed above.[180]

The governing authority, or its committee, would have to work out the details of the reporting relationship of the internal control officers with it. The ALI Compliance Project recommends that the CCO and the CRO could provide regular reports and updates about their control function's activities to the governing authority (or a committee) and meet with it outside the presence of the CEO and other senior executives.[181] Having regular meetings not only ensures that the governing authority stays up-to-date on developments in compliance and risk management and the activities of the programs, but also deflects any implication to others in the organization that there is a serious issue involving the compliance and risk-management programs every time there is such a meeting.[182] Allowing the governing authority (or a committee) to approve the hiring, firing and conditions of employment of the CCO and the CRO is not intended to infringe the senior executives' authority over these officers, but only to enhance the oversight of the governing authority.[183] An important question is whether it should be a standard approach for all large organizations.

CONCLUSION

This Essay, based on remarks given at *Temple Law Review*'s 2017 symposium, has introduced the reader to several governance issues facing the drafters of the ALI Compliance Project, where I have the responsibility for its part on governance of compliance and risk management. After setting forth the background of compliance and risk management, I discussed two general, but related, governance issues that the Project has addressed: (i) the governing

179. *See* ALI COMPLIANCE PROJECT, *supra* note 2, § 3.16(b)(8), (11) (describing the CCO's reporting); *id.* § 3.17(b)(7), (10) (describing the CRO's reporting).

180. *See supra* notes 129–33 and accompanying text.

181. *See supra* notes 134–36.

182. Compliance authorities speak about the need for direct access of the CCO (or someone in this position) to the governing authority. *See, e.g.*, COMPLIANCE MANAGEMENT SYSTEMS—GUIDELINES, *supra* note 13, at 11. The reporting deals with regular activities of the internal control functions, but it may also deal with specific issues, such as compliance violations and "hot" issues in compliance. *See, e.g.*, PWC, *supra* note 147, at 7 (discussing the various kinds of reporting that CCOs make to boards). The regular meetings discussed above would be in addition to those dealing with a common oversight function, which is to assess annually the effectiveness of the compliance and risk management programs. *See id.* at 16 (identifying this as one task of a compliance committee, albeit a managerial committee).

183. *See supra* notes 117–24.

authority's oversight of compliance and risk management and (ii) the reporting of internal control officers, chiefly the CCO and the CRO. In the first, the governing authority's role was presented as understandably reactive insofar as senior executives propose for its approval compliance and risk-management programs that are designed primarily by the CCO and CRO, respectively. I then explored how the governing authority, or one of its committees, engages in its oversight of compliance and risk management by approving the hiring, firing and conditions of employment of the internal control officers and conducting investigations and resolutions of material failures or violations of the compliance program or material failures of or deviations from the risk-management program. Another particularly interesting issue discussed here is the governing authority's contribution to the culture or values of the firm, the well-known "tone at the top."[184]

The second issue raised above involved reporting by the CCO and the CRO, which, as was explained, could be of two kinds, and the Project's treatment of them. As explained, the first kind of reporting, where an executive directs the internal officer's work and determines the officer's conditions of employment, generally deals with the appropriate place and role of compliance and risk management in an organization's hierarchy. Having the CCO and the CRO under the direct authority of the CEO or other senior executives could elevate their importance, and that of their internal control functions, in the organization. This Essay then explained that the second kind of reporting, where internal control officers provide information and reports about the activities of their internal control functions to the governing authority helps the governing authority fulfill its oversight obligation. It observed that, in its treatment of both kinds of reporting, the Project provides flexibility to organizations, which reflects the diversity of organizational practice, while recommending reporting that would enhance the oversight of the governing authority and the status and function of the CCO and the CRO.

The Essay is not intended to be a comprehensive review of the Project's treatment of the governance of compliance and risk management, particularly since the Project is still in its drafting stage. Moreover, as the above discussion demonstrates, the Project takes a non-prescriptive approach that offers organizations different governance possibilities and structures. This approach reflects that the governance of compliance and risk management is evolving in organizations, as the compliance and risk-management functions assume more importance in them.[185] As the Project suggests, there is no "one size fits all" governance solution for all organizations, including as to the oversight duties of the governing authority and the related reporting lines of the CCO and the CRO.[186] Yet the ALI Compliance Project also recognizes that certain

184. *See supra* notes 149–50 and accompanying text.

185. *See* CONTROL RISKS, INTERNATIONAL BUSINESS ATTITUDES TO COMPLIANCE: REPORT 2017, at 6 (2017) (observing that compliance is now fully integrated into most successful international companies).

186. ALI COMPLIANCE PROJECT, *supra* note 2, § 2.01 reporter's note ("Organizations need

governance outcomes are emerging, at least for large organizations, which are those that regulators and other government authorities have mandated, or encouraged, for organizations in the domains under their authority.[187] Accordingly, the ALI Compliance Project might be especially timely because of this coalescence of governance outcomes, which it will also reflect and to which it will lend its support.

flexibility in their governance of internal-control functions to reflect their specific circumstances.").

187. See *supra* notes 11–12 and accompanying text for examples.