THE AMERICAN LAW INSTITUTE

Principles of the Law, Compliance and Enforcement

Black Letter

PART ONE: GENERAL PROVISIONS

Chapter 1, Definitions

§ 1.01. Definitions

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

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

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

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

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

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

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

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

(h) Compliance. Adherence to applicable laws, regulations, rules, an organization's code of ethics, its ethical standards, or legally applicable or otherwise binding industry codes of conduct, and appropriate cooperation with regulators.

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

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

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

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

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

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

(o) Compliance Risk Management. The processes, practices, and activities by which an organization manages its compliance risk.

(p) Deterrence. All the ways in which the threat of liability for misconduct, or the sanctions imposed, can reduce the likelihood that an individual or organization will engage in future misconduct.

(q) Duty of Care. The duty to act with the care, competence, and diligence normally exercised in similar circumstances with respect to the affairs of an organization.

(r) Duty of Loyalty. The duty set forth in Restatement of the Law Third, Agency §§ 8.02-8.06 not to act in one's own interest, or in the interest of another, to the detriment of the best interests of an organization.

(s) Employee. An individual providing goods or services to an organization is an employee if there is mutual consent that the individual should act, at least in part, on behalf of the organization, and that the organization has the right to control either the manner and means by which the individual renders services or otherwise effectively prevents the individual from rendering those services as an independent businessperson.

(t) Enforcement Official. A criminal, civil, or administrative enforcement official empowered to bring actions for criminal or civil misconduct, or for regulatory violations, by an organizational actor or organization.

(u) Enterprise Risk Management. The management of risk on an enterprise-wide basis.

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

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

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

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

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

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

(bb) Independent. Not part of or subject to the control of any other organization or office and not subject to any influence or conflict that would, for any substantial reason, prevent an organizational actor from making a decision on behalf of the organization with only the best interests of the organization in mind.

(cc) Inherent Risk. The risks to an organization if no efforts are undertaken to identify, assess, avoid, prevent, mitigate, reduce, share, or transfer risk.

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

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

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

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

(hh) Knowledge. Substantial certainty about a particular fact or state of affairs. Knowledge can be inferred from the circumstances. Knowledge also can be proven by establishing willful blindness or a conscious avoidance of knowledge.

(ii) Material. Significant, qualitatively or quantitatively, or both, to an organization's reputation, effective functioning, compliance with applicable laws and norms, or financial position.

(jj) Misconduct. Except as otherwise defined in Chapter 6, any violation by an organization or an employee or agent of a criminal statute, civil statute, regulation, or a mandatory internal rule or standard.

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

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

(mm) Principles. These Principles of the Law, Compliance and Enforcement for Organizations.

(nn) Prosecutor. A government official responsible for investigating, charging, prosecuting, and resolving violations of criminal law.

(oo) Regulator. A government officer possessing civil enforcement authority over an organization.

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

(qq) Residual Compliance Risk. The compliance risk that remains after an organization has avoided, prevented, mitigated, reduced, shared, or transferred inherent risk, by means of its compliance risk-management function, including risk from unknown or unforeseeable sources.

(rr) Residual Risk. The risk that remains after an organization has avoided, prevented, mitigated, reduced, shared, or transferred, inherent risk, by means of its risk-management function, including risk from unknown or unforeseeable sources.

(ss) Risk Appetite. The aggregate level and types of risk an organization is willing to assume to achieve its strategy and business objectives, and, if applicable, with respect to a particular activity, the level and type of risk an organization is willing to assume with respect to that activity.

(tt) Risk Assessment. An assessment, including as to potential impact and likelihood, of some or all of the risks an organization faces.

(uu) Risk Capacity. The maximum amount of risk the organization is able to assume in the pursuit of its strategy and business objectives.

(vv) Risk Culture. The organization's norms, assumptions, beliefs, understandings, attitudes, and values that shape its behaviors, decisions, discussions, and assessments relating to risk.

(ww) Risk Limit. A limit with respect to a particular business line or activity, entity within an organization, specific risk category, or other aspect of the organization that, when reached, triggers attention and a response.

(xx) Risk Management. The processes, practices and activities by which risk is identified, assessed, prioritized, avoided, prevented, monitored, mitigated, reduced, shared, transferred, or accepted, and the monitoring of those processes, practices and activities.

(yy) Risk-Management Framework. The principles, policies, procedures, and controls employed by an organization to carry out the task of risk management.

(zz) Risk-Management Function. The operations, offices, personnel, and activities within an organization that carry out the task of risk management.

(aaa) Risk-Management Program. A set of specific rules, procedures, authorities, standards, requirements, and practices that implements the risk-management framework.

(bbb) Risk Tolerance. The maximum level of residual risk an organization is willing to bear.

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

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

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

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

(ggg) Whistleblower. A person who reports to criminal, civil, or administrative enforcement officials about possible wrongful activities by an organization or its employees or agents.

Chapter 2, Subject Matter, Objectives, and Interpretation

§ 2.01. Subject Matter

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

§ 2.02. Objectives

These Principles are intended to promote the following objectives:

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

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

§ 2.03. Characteristics of the Organization

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

(a) size;

(b) legal form;

(c) complexity;

(d) geographic scope;

(e) the nature of its business or affairs;

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

(g) history of its compliance violations;

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

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

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

§ 2.04. Interpretation

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

§ 2.05. Nonliability

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

PART TWO COMPLIANCE

Chapter 3, Governance

§ 3.01. Governance in Compliance and Risk Management

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

§ 3.02. Governance Actors

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

§ 3.03. Governance Map for Compliance and Risk Management

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

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

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

§ 3.05. Governance Accommodations for Organizational Circumstances

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

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

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

(1) be independent; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(6) to be reasonably informed of the staffing and resources allocated by executive management to the internal-control departments of compliance, risk management, and internal audit, and to satisfy itself that the staffing and resources

are adequate and that the departments are sufficiently independent and have the appropriate authority to perform their respective internal-control responsibilities;

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

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

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

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

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

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

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

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

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

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

(c) Subject to subsection (a) and if authorized under the law governing the organization, the board of directors, in its discretion, may delegate to a group or committee

of its members, to a joint committee of directors and executives, or to executive management the power to perform one or more of the responsibilities set forth in subsection (b).

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

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

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

(1) be independent; and

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

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

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

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

§ 3.10. Compliance and Ethics Committee

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

(1) be independent; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) the adequacy of such disclosure or reporting;

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

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

(11) with the assistance of the chief legal officer, the chief compliance officer, outside legal counsel, or outside consultants, to direct its own investigation of any material violation or failure of the compliance program and the code of ethics, including any violation or failure communicated under the organization's procedures for confidential internal reporting; and

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

§ 3.11. Risk Committee

(a) The board of directors, in its discretion, may elect to (or, if required by law, must) delegate to a risk committee, or to another committee or committees, part or all of its

oversight of risk management in the organization. This committee should have full power with respect to the delegated responsibilities, subject to the board's ultimate authority for them and to any reservation made by the board in its delegation. The committee should have at least three members, who should:

(1) be independent; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) the adequacy of such disclosure or reporting;

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

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

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

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

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

(1) independent; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 3.14. Executive Management of Compliance and Risk Management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) to report on their implementation,

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

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

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

§ 3.15. Chief Compliance Officer

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

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

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

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

(B) together with compliance officers and as directed by executive management, to conduct a compliance-risk assessment, and to formulate and

implement the compliance program and the code of ethics, and any revisions thereto, in response to that assessment, and

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

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

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

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

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

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

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

(C) in consultation with the chief legal officer, to direct the investigation of any actual or potential violation of the program and the code detected by

the monitoring or by the procedures for confidential internal reporting and to report the results of the investigation to the appropriate organizational actor;

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

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

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

(9) to confer with executive management:

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

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

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

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

(B) to report on their implementation,

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

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

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

§ 3.16. Chief Risk Officer

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(9) to confer with executive management:

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

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

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

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

(B) to report on their implementation,

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

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

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

§ 3.17. Chief Audit Officer

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

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

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

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

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

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

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

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

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

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

(6) to confer with executive management:

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

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

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

(A) to report on the results of the internal audit of compliance and risk management, particularly on the effectiveness of and inadequacies in the

compliance function and the risk-management function, and to recommend any necessary changes,

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

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

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

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

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

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

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

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

internal-control environment of the organization for compliance and risk management, and

(E) to notify it of any material violation or failure of the compliance program and the code of ethics and of any material deviation from or failure of the risk-management framework and program that the internal audit revealed, to identify the cause or causes of such violation, failure, or deviation, including weaknesses in the internal-control environment of the organization for compliance and risk management, and to recommend remedial measures to address such cause or causes.

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

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

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

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

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

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

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

(3) unless otherwise directed by the board:

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

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

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

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

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

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

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

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

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

(3) to administer the organization's policies and procedures for nonretaliation against employees who use the organization's procedures for confidential internal

reporting and to report any evidence of retaliation to the appropriate organizational actor; and

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

§ 3.20. Multiple Responsibilities of Internal-Control Officers

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

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

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

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

(3) There are in place organizational procedures to deal with any conflicts of interest (other than those disabling ones that would be excluded under subparagraph (2) above) that would arise from the assignment of multiple responsibilities to the internal-control officer.

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

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

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

(c) When subsection (b) applies:

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

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

PART TWO: COMPLIANCE

Chapter 4, Compliance Risk Management

§ 4.01. Nature of Compliance Risk and Compliance Risk Management

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

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

§ 4.02. Goals of Compliance Risk Management

The goals of compliance risk management include:

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

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

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

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

§ 4.03. Characteristics of Organizations Affecting Compliance Risk Management

The compliance risk management appropriate for an organization will vary depending on its characteristics, including:

(a) its size;

(b) the nature of its business;

(c) the heterogeneity of its business;

(d) the complexity of its business;

(e) the geographical reach of its operations;

(f) the location(s) of its operations;

(g) its dealings with third parties who might cause it to face increased exposure to risks;

(h) its exposure to cyber risk;

(i) the laws and regulations applicable to it and its businesses;

(j) its status as a publicly held or privately held company;

(k) its status as a for profit, not-for-profit, or benefit corporation;

(l) the nature of its compensation structure and other terms of employment;

(m) the existence of an effective risk-management program, including as to compliance risk, and any history of risk-management failures or deviations, including as to compliance risk management;

(n) the existence of an effective risk culture, including as to compliance risk; and

(o) the consistency of its organizational culture with its risk culture.

§ 4.04. General Compliance Risk-Management Activities of Organizations

An organization should, as appropriate given its attributes and circumstances, do the following:

(a) develop and employ an effective framework, function, and program to manage compliance risk;

(b) review its management of compliance risk, and make such changes as are appropriate or desirable, on a regular as well as an ongoing basis and when changes to business context, business conditions, regulation, or other relevant matters occur;

(c) regularly assess whether the requirements and rationale of its program to manage compliance risk are properly communicated throughout the organization;

(d) monitor on a regular as well as an ongoing basis whether the program is being followed, investigating deviations and failures;

(e) establish appropriate governance structures within the organization to create, effectuate, support, and complement the organization's risk management, including its compliance risk management;

(f) support, facilitate the hiring of, and appropriately compensate, qualified risk managers, particularly as to compliance risk, including, if appropriate or required, a chief compliance officer, a chief legal officer, and a chief risk officer;

(g) commit the appropriate resources, leadership, and support to compliance risk management;

(h) coordinate compliance risk-management activities with those personnel responsible for implementing internal-control functions, including the compliance function;

(i) allocate ownership of particular compliance risks to the appropriate operational managers (the first line of defense), and those monitoring the first line of defense, including managers in the risk management and compliance functions (the second line of defense), to assist in managing the risks and advancing the goal of accountability;

(j) integrate compliance risk management throughout the organization, including it in the processes by which the organization develops and considers alterations to its strategy, business objectives, and business plan, and makes major decisions, as well as embedding it into operational units;

(k) ensure that practices and policies relating to employment, notably hiring, training, compensation, promotions, and discipline, are consistent with and in furtherance of its risk management, including its compliance risk management;

(l) ensure that mechanisms are in place to promote ongoing communication of compliance-risk-relevant information to the appropriate organizational actors; and

(m) establish, promote, and maintain a risk culture that supports and enhances the effectiveness of its risk management, including its compliance risk management, and ensure that its organizational culture is consistent with its risk culture in this regard.

§ 4.05. Structuring the Terms of Employment

(a) An organization should take risk-management concerns, including those pertaining to compliance risk management, into account in:

(1) making decisions as to hiring, retention, promotion, sanctioning, and firing of employees; and

(2) designing employee compensation and other incentives, including awards and recognitions, and designing employee-training programs.

(b) An organization should monitor the effects of compensation and other incentives on risk-taking, including risk-taking that implicates or involves compliance risks.

(c) An organization should have in place processes and procedures by which the appropriate personnel can promptly become informed about employees' conduct that implicates risk-management issues, particularly compliance risk-management issues.

§ 4.06. Risk Culture

(a) An organization should put in place appropriate mechanisms to establish, promulgate, and maintain a sound risk culture throughout the organization, including as it relates to compliance risk.

(b) An organization's risk culture should:

(1) promote compliance-risk-aware behavior and attitudes throughout the organization;

(2) discourage, both at the individual and the group level, behavior, attitudes, and norms that promote compliance risk-taking, as well as excessive or inappropriate risk-taking of any sort;

(3) reinforce its values as to accountability, ethics, and transparency;

(4) make its compliance risk management more effective;

(5) encourage adherence to the organization's policies and procedures concerning internal reporting;

(6) encourage appropriate deference to relevant expertise and established compliance risk-management procedures within the organization;

(c) An organization's board of directors and executive management should regularly demonstrate and communicate the importance of its risk culture, including as it relates to compliance risk, setting an appropriate "tone at the top" and ensuring that it is also a tone *from* the top.

(d) An organization should consider whether significant changes affecting the organization might have unanticipated effects on its risk culture, including as it relates to compliance risk, and, if necessary or appropriate, take steps to identify and address any such effects; and

(e) An organization should ensure that its organizational culture is consistent with the organization's risk culture, including as it pertains to compliance risk.

§ 4.07. Elements of Effective Compliance Risk Management

An organization's compliance risk management should:

(a) identify the compliance risks the organization faces;

(b) assess those risks;

(c) prioritize those risks;

(d) adopt strategies to reduce or respond to those risks

(e) monitor those risks;

(f) execute appropriate risk responses;

(g) assess and, to the extent appropriate, accept the residual compliance risk; and

(h) review, validate, and, if warranted, adjust these elements of its compliance risk management on a regular and ongoing basis.

§ 4.08. Strategies for Identifying Compliance Risks

(a) An organization should seek to employ the most effective available methods to identify its compliance risks.

(b) The methodology an organization uses for identifying compliance risks will necessarily be a function of the size, resources, and sophistication of the organization.

(c) In identifying compliance risks, an organization should seek to be as comprehensive as is feasible.

(d) An organization's identification of compliance risks should, to the extent appropriate for the organization, occur at the entity/enterprise, division, operating-unit, function, and process levels.

(e) An organization should regularly review and validate the methods it uses to identify compliance risks.

§ 4.09. Strategies for Assessing and Prioritizing Compliance Risk

(a) An organization should assess the compliance risks it identifies, determining the likelihood of each risk and the impact on the organization should the risk come to pass.

(b) An organization should prioritize the risks it deems to be the most serious, considering both the likelihood and potential impact on the organization, and devote greater resources to managing such risks.

(c) The methodology an organization uses for assessing and prioritizing compliance risks will be a function of its size, resources, and sophistication.

(d) An organization's assessment and prioritization of its compliance risks should be conducted, to the extent appropriate for the organization, at the entity/enterprise, division, operating-unit, function, and process levels.

(e) An organization should regularly review and validate its methods for making its compliance risk assessments and prioritizations.

(f) An organization's assessment and prioritization of its compliance risks should inform its assessment and prioritization of its risks for purposes of its overall risk management.

§ 4.10. Strategies for Addressing Compliance Risk

(a) An organization should seek to prevent, avoid, reduce, share, or transfer its inherent compliance risk.

(b) When appropriate, an organization should employ the following strategies for carrying out the functions described in subsection (a):

(1) putting in place controls or other mechanisms that may prevent the risk from coming to pass or limit its impact if it does come to pass.

(2) sharing or transferring compliance risk by using insurance or indemnification, if permitted by applicable law,

(3) sharing or transferring some portion of the activity from which the risk arises, or

(c) An organization may find it advisable to put in place a risk-response plan. Such a plan should be as specific as to risks and responses as the organization considers desirable and appropriate.

§ 4.11. Strategies for Monitoring Compliance Risk

(a) An organization should monitor for compliance risks, using such techniques as it determines are appropriate.

(b) The monitoring should encompass matters internal and external to the organization that could present compliance risks. Different monitoring strategies may be indicated depending on the possible sources of the risk.

(c) An organization should perform monitoring on both a regular and an ongoing basis.

(d) An organization's risk-management program and risk culture should encourage its employees at all levels to report on matters relevant to its monitoring of risk, including

compliance risk, and otherwise participate appropriately, as determined by the organization, in its risk monitoring.

(e) An organization should ensure that its employees are informed as to how to provide information relevant to compliance risk to the appropriate personnel within the organization.

(f) An organization should regularly review and validate the methods it uses to monitor its compliance risks.

§ 4.12. Compliance Risk Responses

(a) An organization should ensure that its responses to compliance risks that have come to pass are effectively executed.

(b) At both the time an organization executes its risk response and afterwards, the organization should monitor for new risks created by or during the process of responding to the risk that has come to pass, and make appropriate adjustments to its risk management to address any such new risks.

§ 4.13. Assessing and Accepting Residual Compliance Risk

(a) An organization should assess the residual compliance risk that remains after controls, risk-sharing, risk-transfers, and other risk-reduction strategies are implemented.

(b) If the organization finds its residual compliance risk to be excessive, it should implement additional strategies for risk reduction.

(c) The organization may accept residual compliance risk that is not excessive. Any acceptance of residual risk should be undertaken with deliberation and with a reasoned analysis of the impact that will likely occur if a risk that is not sufficiently controlled, transferred, shared, or mitigated comes to pass.

(d) The organization should reassess its residual compliance risk on a regular and ongoing basis and if, during a reassessment, it finds the risk to be excessive, the organization should take action to reduce the risk.

Chapter 5, Compliance Policies and Programs

§ 5.01. Nature of the Compliance Function

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

§ 5.02. Goals of the Compliance Function

Goals of the compliance function include the following:

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

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

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

(d) investigating and identifying violations of the law;

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

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

§ 5.03. General Compliance Activities of Organizations

An organization should do the following with respect to compliance:

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

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

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

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

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

§ 5.04. Enterprise Compliance

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

§ 5.05. Elements of an Effective Compliance Function

Elements of an effective compliance function include:

(a) a compliance program;

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

(c) effective management;

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

(e) incentives for compliant behavior; and

(f) procedures for independent validation.

§ 5.06. Compliance Program

The organization's compliance program should be reasonably designed to prevent and detect violations of internal and external laws and norms. It should:

(a) be governed by written rules and procedures approved by the board of directors;

(b) be informed by an assessment of risk to the organization;

(c) be based at least in part on underlying principles rather than standardized procedures;

(d) assign responsibility for compliance within the organization;

(e) be impartially and fairly administered;

(f) provide reliable and timely advice to employees regarding their compliance obligations;

(g) be effectively communicated to affected employees;

(h) include appropriate compliance training for employees, agents, and members of the board of directors;

(i) include procedures for internal reporting of violations;

(j) include procedures for monitoring employee conduct;

(k) include procedures for investigating violations;

(l) include procedures for disciplining violations;

(m) create appropriate incentives for compliant behavior and disincentives for violations;

(n) be regularly assessed for effectiveness and updated as necessary; and

(o) be periodically reviewed and reaffirmed by the organization's senior executives and board of directors.

§ 5.07. Compliance Risk Assessment

(a) When deciding how to allocate resources provided for the compliance function, the chief compliance officer should undertake a compliance risk assessment.

(b) Depending on the facts and circumstances, factors relevant to the compliance risk assessment may include:

(1) the nature of the organization's business;

(2) the industry's history of violations;

(3) the organization's history of violations;

(4) compensation arrangements for executives and employees;

(5) whether the organization has introduced a new product line or entered into a new business activity;

(6) whether there has been a change in applicable laws;

(7) whether internal controls are subject to manual override;

(8) the extent of the organization's foreign activities;

(9) the organization's exposure to compliance violations by agents, vendors, customers, or supply-chain counterparties;

(10) regulatory enforcement priorities; and

(11) the probable impact of compliance violations on the organization's reputation.

(c) Any risk assessment performed pursuant to subsection (a) should, if feasible and appropriate, be:

(1) in writing;

(2) evaluated both in terms of the absolute level and the trend of compliance risk; and

(3) reviewed and, if advisable, revised on a periodic basis and be subject to revision as new risks become apparent or old ones subside.

(d) In performing the risk assessment pursuant to subsection (a), the chief compliance officer should make an independent judgment about the compliance risks facing the organization but should also take account of the views of others within the organization, particularly the chief legal officer.

§ 5.08. Compliance Advice

(a) The compliance function should stand ready to provide advice to employees and agents on how to behave in a compliant and ethical way.

(b) The advice described in subsection (a) may be provided by a compliance officer, a legal officer, or some other appropriate person. The identity of the person providing such advice and the mechanism through which it is provided depend on the facts and circumstances.

(c) Employees or agents who rely on such advice in good faith should be protected against retaliation or punishment by the organization if the advice given proves to be mistaken.

§ 5.09. Oversight of Employees and Others

(a) The compliance function should engage in oversight of executives, employees, agents, and others whose actions may be attributed to the organization in order to promote compliance with internal and external norms.

(b) The nature and scope of appropriate oversight by the compliance function depends on the facts and circumstances. Consistently with rights of privacy, limitations on permissible data gathering, and internal organizational norms, the organization may:

(1) review internal and external communications of employees;

(2) require reports from business-line activities or employees, when appropriate;

(3) conduct interviews with business-line employees;

(4) perform on-site inspections of offices or functions;

(5) perform drug and alcohol tests as permitted by law;

(6) review documents prepared by business-line employees;

(7) review customer and other third-party complaints;

(8) conduct audits of, or otherwise monitor, vendors for compliance risk and violations;

(9) retain third parties to perform monitoring tasks; and

(10) engage in other appropriate monitoring activities.

(c) Coordination with other internal-control functions is sometimes warranted.

(1) Oversight activities by the compliance function may be coordinated with the activities of other internal-control functions such as risk management or internal audit, as well as with business-line activities that overlap with the compliance function, provided that appropriate separation is maintained between these functions;

(2) The compliance function should avoid unnecessary duplication of effort with other internal-control functions; and

(3) If appropriate, the compliance function may rely on information provided by other internal-control functions.

(d) Oversight activities by the compliance function must be carried out in accordance with the applicable law governing the privacy rights of employees, agents, or others.

§ 5.10. Training and Education

(a) The compliance function should include training and other educational activities regarding the compliance obligations of the organization and its employees and agents.

(b) The compliance function should make appropriate compliance training available to all employees. Compliance training should include advising the board of directors and senior managers on applicable laws, rules, and standards.

(c) The appropriate form of training depends on the facts and circumstances surrounding each organization, including its size, its complexity, the nature of the business line's activity, the compliance risk posed, the level of sophistication and experience of the employees involved, and the legal requirements for training of personnel.

§ 5.11. Red Flags

(a) The compliance function should be alert to red flags of potential violations. Depending on the facts and circumstances, red flags can include but are not limited to:

(1) transactions with no apparent business purpose;

(2) sudden material changes in performance that cannot be explained by known causes;

(3) excessively complex structures;

(4) frequent failures to complete required paperwork;

(5) efforts to disguise the identity of customers or other counterparties;

(6) gifts or favors to customers or business partners, or family members of customers or business partners, that appear excessive in light of the customs of the industry;

(7) gifts or favors to government officials or to family members of government officials;

(8) unusual and persistent failures to take allowed vacations or time off; and

(9) unauthorized self-dealing or other conflicted activities by employees and agents.

(b) The presence of a red flag does not indicate that a violation has occurred.

(c) A compliance officer who knows of a red flag of a violation should undertake appropriate responsive actions.

§ 5.12. Escalation Within the Organization

(a) If a compliance officer knows that an employee or agent has engaged, or intends to engage, in illegal conduct or other impermissible activity that poses a significant risk to the organization or a third party if not corrected or remediated, he or she should act as reasonably necessary in the best interests of the organization.

(b) If the matter cannot be addressed in a timely manner within the scope of his or her authority, the chief compliance officer should refer the issue to an official who has the power to address the matter, including, when appropriate, the board of directors. Reporting up is not required if the effort would clearly be futile due to potential involvement in misconduct by higher level officials.

(c) If after undertaking the actions described in subsection (b), the chief compliance officer in good faith believes that the matter will not be satisfactorily addressed in an appropriate time within the organization and that the failure to address the matter poses a material threat to the organization's financial position or strategic objectives or to third parties, he or she may disclose the concerns to an appropriate government regulator.

§ 5.13. Compliance Under Legal Uncertainty

(a) Unless the organization's rules of governance otherwise provide, the chief compliance officer is not responsible for resolving uncertainty in applicable rules or regulations.

(b) If the chief compliance officer deems it important to resolve a legal uncertainty in order to perform his or her responsibilities, he or she should ordinarily seek guidance from the chief legal officer or another qualified attorney. If such guidance is not available, the chief compliance officer should apply the most reasonable interpretation.

§ 5.14. Hiring of Employees, Retention of Agents, and Selection of Counterparties

(a) Unless otherwise indicated by the circumstances, the official charged with hiring employees or retaining agents should consider a candidate's background and history of compliance with applicable laws, regulations, and ethical norms. Candidates deemed to present an unacceptable risk of violations should not be hired or retained.

(b) The official tasked with selecting a vendor or supplier, or engaging in a transaction with a customer, should take into consideration the risk that misconduct by that vendor, supplier, or customer will be attributed to or otherwise result in harm to the organization. Prospective vendors, suppliers, or customers should not be dealt with if they present an unacceptable risk of misconduct that will result in harm to the organization.

§ 5.15. Background Checks

In carrying out the activities contemplated in § 5.14, an organization may engage in background checks of potential employees, agents, or counterparties. Such background checks must comport with applicable legal restrictions, must not result in invidious discrimination, should be appropriate for the position in question, and should avoid intruding unnecessarily on reasonable expectations of privacy.

§ 5.16. Compensation

(a) An employee's record of compliant or noncompliant behavior should be considered as a factor in setting his or her compensation.

(b) Bonuses and other nonsalary compensation for employees in a compliance function should be independent of the performance of any business line overseen by the employee and should be based in substantial part on the achievement of compliance-based objectives.

§ 5.17. Discipline

(a) In addition to setting compensation practices to incentivize compliant behavior, organizations should consider imposing nonmonetary discipline for violations.

(b) As in the case of monetary sanctions, the form of nonmonetary discipline should be commensurate with the gravity of the offense and consistent with the organization's stated policies and procedures.

(c) Nonmonetary sanctions should be based on clearly expressed and widely disseminated norms of conduct and should be administered within the organization on an evenhanded basis.

(d) The organization's decision whether to report misconduct should depend on the facts and circumstances, including the gravity of the offense, whether third parties have been harmed by the misconduct, the likelihood of recidivism, the probable response of regulators, and fairness to parties involved.

§ 5.18. Procedures for Internal Reporting

(a) An organization should encourage its employees to communicate legitimate concerns about compliance violations to appropriate persons within the organization.

(b) The organization should publicize and make available reasonable means by which concerns about compliance violations can be communicated. These include:

(1) telephone tip lines;

(2) an "open door" policy on the part of senior executives and other supervisors;

(3) a drop box for anonymous written communications;

(4) an e-mail address or other means for online communication; and

(5) any other mechanisms or media that encourage full, frank, and anonymous communication of potential violations.

(c) The organization should publicly announce the person or persons to whom communications should be directed.

(d) The organization should adopt and publicly announce a policy of nonretaliation against employees and agents who make reports described in this Section.

(e) The organization should provide such employees with reasonable protections against retaliation by employees or other parties who are subject to the organization's control.

(f) When deciding upon the appropriate discipline for employees' misconduct, the organization should take into account whether they self-reported their violations in a timely fashion.

§ 5.19. The Role of Third-Party Service Providers

Third-party service providers can play a role in an organization's compliance function. A professional service provider's compliance responsibilities depend on the nature of its services and the terms of the retention.

§ 5.20. Attorneys

(a) Attorneys owe duties of care and loyalty to their clients when providing legal services in connection with the compliance function.

(b) The compliance attorney's loyalty is to the organization and not to the chief executive officer or any other employee or agent of the client.

(c) When performing compliance-related services, an attorney may not assist a client in carrying out an illegal action.

(d) If, in the course of compliance-related representation, an attorney comes to know of illegal conduct that may be attributed to the client, the attorney should be guided by applicable rules of professional conduct.

§ 5.21. External Auditors

(a) External auditors are responsible for providing an independent review of matters specified in the audit engagement letter.

(b) If, during the course of an audit, an external auditor uncovers evidence of significant compliance violations, he or she should promptly inform an appropriate officer of the organization.

(c) The external auditor should not issue an unqualified audit opinion if the compliance violations have:

(1) materially affected the integrity of the organization's financial reporting;

(2) made it impossible for the auditor to support management's assessment of the organization's internal controls over financial reporting; or

(3) otherwise made it impossible for the auditor to carry out its assigned responsibilities.

§ 5.22. The Decision to Investigate

An organization's decision to investigate an allegation or other evidence of misconduct depends on the facts and circumstances. Relevant factors include but are not limited to:

(a) the plausibility of any allegation of misconduct and the credibility of the party making the allegation;

(b) the gravity of the alleged misconduct;

(c) the likely cost of an investigation if one is performed;

(d) the risk of reputational harm if an investigation is not conducted;

(e) the likely response of the regulator to the organization's actions;

(f) the likely response of the involved employee to questions about his or her conduct;

(g) the possibility that the misconduct might reflect broader or more systemic problems; and

(h) any guidance provided by the organization's compliance policy, code of ethics, or other governing compliance-related documents.

§ 5.23. Scope of Internal Investigations

(a) The scope of an internal investigation should be defined in advance but should also be flexible enough to allow the investigator to pursue related lines of inquiry as facts are developed.

(b) Internal investigations into compliance violations should have the following features:

(1) The investigator should be allowed sufficient independence to perform the inquiry free from interference by any party;

(2) The investigator should be provided with sufficient resources to carry out his or her responsibilities, including, if necessary, the ability to hire outside attorneys and consultants;

(3) The investigator should be provided access to relevant information within the organization, including documents, computer files, and physical objects, and should be allowed to conduct interviews with relevant persons; and

(4) The investigator should set aside the time needed to complete the inquiry in as prompt a fashion as possible.

(c) The organization is entitled to exercise reasonable oversight over the investigation, provided that doing so does not interfere with the investigation's effectiveness and that the officer engaging in such oversight is not personally involved in the matter under review. Reasonable oversight can involve the following:

(1) reviewing the investigator's budget and expenditures;

(2) receiving reports of the investigator's progress;

(3) granting rights of approval for expansions of the investigation beyond its original scope; and

(4) granting rights to review and comment on, but not to alter, the investigator's draft and final reports.

§ 5.24. The Investigator

(a) The person tasked with leading the internal investigation should:

(1) have the skill, ability, and integrity to perform the responsibility capably;

(2) have no personal involvement in the alleged wrongdoing;

(3) have no personal or business relationships or bias that could interfere with his or her impartiality; and

(4) have sufficient time available to complete the investigation expeditiously.

(b) An attorney should lead or participate in investigations of misconduct that pose a material threat to the financial condition or strategic plans of the organization.

§ 5.25. Privilege in Investigations

The following privileges and protections apply in connection with internal investigations into possible compliance violations:

(a) Communications between employees and their attorneys are protected by the attorney–client privilege if a significant purpose of the communication is to obtain or provide legal advice;

(b) Notes, mental impressions, and other work product of attorneys are covered by the work-product protection if prepared in contemplation of litigation or other adversarial proceedings;

(c) Internal-investigation reports prepared in contemplation of adversarial proceedings may have qualified protection against compelled disclosure.

§ 5.26. Responding to Government Investigations

(a) An organization should not hinder or impede a government investigation.

(b) An organization may elect to cooperate with a government investigation. Such cooperation may include:

(1) sharing information obtained during the course of the organization's internal investigation;

(2) directing employees to cooperate with reasonable demands for information;

(3) obtaining, reviewing, and analyzing information and providing such information to the government; and

(4) informing the investigator of relevant private information not then in the possession of the government.

(c) Organizations that voluntarily cooperate with government investigations may be entitled to credit in connection with charging decisions and decisions that relate to settling enforcement actions.

(d) As long as the organization's conduct is for the purpose of presenting a bona fide legal defense, the organization is entitled to use all legally appropriate strategies for defending itself, even if the result is to delay a government investigation or to make it more difficult for the government to obtain information it needs to complete its investigation.

§ 5.27. Fairness to Employees During Investigations

(a) In general, employers may examine any on-the-job conduct when conducting an internal investigation.

(b) The scope of internal investigations should be limited by the following considerations:

(1) Employers should comply with legal requirements designed to protect employee rights during internal investigations;

(2) Employers should refrain from intruding on an employee's reasonable expectations of privacy; and

(3) When interviewing an employee during an internal investigation, an attorney for the organization should clarify whom he or she is representing and who holds the attorney–client privilege.

§ 5.28. Responding to the Internal Investigator's Report

An organization should respond promptly and effectively to the findings in a report by an internal investigator. Depending on the facts and circumstances, the organization may respond by:

(a) undertaking no action, if the investigator finds that charges or misconduct allegations are not substantiated, are of minor importance, or are mitigated or excused;

(b) instituting disciplinary proceedings against employees or agents found to have engaged in misconduct;

(c) reporting the findings of the investigation to the government or other entities; and

(d) undertaking remedial actions to rectify the harms caused by the violations.

§ 5.29. Lessons Learned

An organization should evaluate the results of an internal investigation and, as appropriate, should implement reforms to reduce the probability that the violations or misconduct uncovered during the investigation will recur.

§ 5.30. Responsibility of Parent Companies for Compliance in Subsidiaries

(a) Parent companies are subject to the compliance obligations of their subsidiaries:

(1) if so provided by law;

(2) if the parent company has undertaken such an obligation; or

(3) if the parent exercises control over the subsidiary's management and benefits in a material respect from the subsidiary's compliance violations.

(b) If the parent provides internal-control services for the subsidiary, the parent should perform those services competently and for the benefit of the subsidiary.

§ 5.31. Supply-Chain Due Diligence

(a) Depending on the circumstances, an organization should compile an inventory of significant contractors and subcontractors and the services they perform or goods they supply.

(b) The organization should assess the compliance risk posed by violations committed by significant contractors or subcontractors.

(c) The organization should seek to verify that critical contractors and subcontractors understand and agree to adhere to the organization's policies, procedures, and code of ethics.

§ 5.32. Vendor and Business-Partner Due Diligence

In cases in which an organization determines that its relationship with a vendor presents a material compliance risk, the organization should consider the following measures:

(a) assessing the vendor's or business partner's capacity to perform the assigned task in a compliant fashion;

(b) seeking representations and warranties from the vendor or business partner regarding compliance with applicable laws and regulations;

(c) seeking the right to audit the vendor's or business partner's compliance with applicable laws and regulations; and

(d) as appropriate, engaging in training or other activities designed to inform vendors and business partners about compliance issues pertinent to the organization.

§ 5.33. Customer Due Diligence

(a) An organization should maintain awareness of the compliance risks posed by its customers.

(b) The rigor with which an organization should conduct customer due diligence depends on the facts and circumstances. Relevant considerations include but are not limited to:

(1) the type of industry involved;

(2) the significance to the organization of the customer relationship;

(3) whether the customer is also an affiliate of the organization;

(4) the country where the customer is located;

(5) the products or services utilized by the customer;

(6) the legal-entity structure of the customer;

(7) the procedures through which transactions with customers are arranged; and

(8) the customer's record of compliant or noncompliant behavior.

§ 5.34. Commitment to Ethical Behavior

An organization should aspire to conduct its affairs not only legally, but also in accordance with broader standards of ethics.

§ 5.35. Codes of Ethics

(a) An organization may embody its commitment to ethical behavior in a code of ethics.

(b) The code of ethics may make it clear that employees are expected to conduct themselves in ways that go beyond compliance with laws, regulations, professional standards, and the organization's compliance policies and procedures.

(c) The code of ethics may prohibit conduct that displays disrespect or unfairness to others.

§ 5.36. Special Considerations for International Firms

An organization conducting substantial business in other countries should:

(a) be familiar with and seek to comply with the laws, regulations, and other governing norms of each country where the organization does business;

(b) ensure that its compliance policy, compliance program, and other compliance-related information are translated into local languages and made available to the organization's employees and agents in each country where the organization does business;

(c) take account of the compliance risk factors created by the culture, norms, and history of each country where the organization does business;

(d) review and, if necessary, revise its compliance policy and compliance program whenever the organization enters into business in a new country or merges with another organization that does business in the new country;

(e) establish policies for determining whether potential business partners in foreign countries pose material compliance risks; and

(f) establish systems for sharing information about suspicious activities between relevant branches or offices of the organization located in different countries.

PART THREE: ENFORCEMENT

Chapter 6, Criminal and Civil Enforcement Against Individuals and Companies for Corporate Misconduct

§ 6.01. Definitions

The following definitions apply throughout this Chapter:

(a) Administrative order: An order that resolves an administrative enforcement proceeding filed with administrative law judge or administrative agency governing body (e.g., commission).

(b) Cease and desist order: An administrative enforcement order that enjoins an organization from future violations of the law.

(c) Civil enforcement official: An enforcement official empowered to bring civil or administrative enforcement actions against individuals or organizations for organizational civil misconduct.

(d) Civil misconduct: Any violation of a civil statute or regulation. These Principles focus on intentional or knowing civil misconduct.

(e) Criminal misconduct: Any violation of a criminal statute or a regulation that is enforceable through criminal sanctions.

(f) Collateral consequences: Limitations on an organization's business activities and other disadvantages to an organization that are authorized or required by state, federal, or foreign law, as a direct result of the organization being convicted of a crime, other than those sanctions imposed by a court in sentencing the organization. The term includes consequences that can result from either a civil or administrative finding that the organization engaged in certain forms of misconduct or was subject to certain sanctions or other forms of relief, such as an injunction. The term also includes disadvantages to an organization, such as exclusion, imposed by a self-regulatory or non-government organization with jurisdiction over the organization as a result of it being subject to a criminal, civil, or administrative enforcement action or to particular forms of sanctions, such as an injunction.

(g) Consent decree: A negotiated civil or administrative resolution that resolves a civil or administrative enforcement action, generally without the organization admitting that it engaged in misconduct.

(h) Condoned: An employee who is part of an organization's substantial authority personnel (see 6.01(y) below) condones material criminal or civil misconduct if he or she knows that some form of misconduct is occurring (or consciously avoids knowledge of its occurrence) and does not intervene to terminate it or report it to appropriate authorities within the organization.

(i) Disgorgement order: An order that requires the defendant to forfeit the benefit it obtained from criminal or civil misconduct.

(j) Declination: An explicit statement by a prosecutor, or a civil or administrative enforcement official, not to file either criminal charges or a civil or administrative action or to seek to sanction an organization otherwise.

(k) Deferred prosecution agreement (DPA): A nontrial resolution under which a prosecutor files criminal charges, or civil or administrative enforcement official files a civil or administrative complaint, against an organization, but suspends criminal prosecution or

the civil or administrative action provided that the organization complies with the DPA's provisions.

(l) Employee: An individual providing goods or services to an organization is an employee if there is mutual consent that the individual should act, at least in part, on behalf of the organization, and that the organization has the right to control either the manner and means by which the individual renders services or otherwise effectively prevents the individual from rendering those services as an independent businessperson.

(m) Enforcement official: A criminal, civil or administrative enforcement official empowered to bring actions for criminal or civil misconduct, or for regulatory violations, by an organizational actor or organization.

(n) Full corrective action: The steps taken by an organization that self-reports criminal or civil misconduct (in accordance with § 6.04), fully cooperates with prosecutors or civil enforcement authorities (in accordance with § 6.05), and engages in timely and full disgorgement, restitution, and remediation (in accordance with § 6.06).

(o) Guilty plea: A negotiated criminal resolution pursuant to which a prosecutor files charges against the organization and the organization agrees to plead guilty to the charges in court.

(p) High-level personnel: Individuals who have substantial control over an organization or who have a substantial role in making policy within an organization.

(q) Knowledge. Substantial certainty about a particular fact or state of affairs. Knowledge can be inferred from the circumstances. Knowledge also can be proven by establishing willful blindness or a conscious avoidance of knowledge.

(r) Misconduct: A violation of a criminal statute, civil statute, regulation, or mandatory internal rule or standard. These Principles focus on knowing or intentional misconduct.

(s) Material criminal or civil misconduct. Misconduct is material if a reasonably prudent enforcement official seeking to pursue the public interest would consider the misconduct itself an appropriate subject for an enforcement action, independent of other considerations such as organizational self-reporting or full cooperation.

(t) Neither-admit-nor-deny resolution: A civil or administrative resolution under which an organization resolves an action without admitting to the misconduct but subject to

a prohibition on denying that it engaged in misconduct, except as provided in the nontrial resolution.

(u) Non-prosecution agreement (NPA): An agreement under which a prosecutor agrees not file criminal charges, or a civil enforcement authority agrees not to bring a civil action, against an organization if it complies with agreement's provisions.

(v) Nontrial resolution: A resolution of a criminal, civil, or administrative action that imposes, or is predicated on, sanctions against or undertakings by an organization. The term includes a guilty plea, DPA, NPA, declination with disgorgement, neither-admit-nor-deny resolution, cease and desist order, and a consent decree. It does not include a traditional declination predicated on a finding that the organization did not engage in provable misconduct.

(w) Organizational actor: A person who is either an employee or nonemployee agent of an organization.

(x) Restitution order: An order requiring the defendant to compensate identifiable victims of an offense.

(y) Remedial order: An order to remedy the harm that has already occurred or to reduce or eliminate the threat of future harm.

(z) Substantial authority personnel: Individuals who, within the scope of their authority, exercise a substantial measure of discretion in acting on behalf of an organization.

(aa) Willful misconduct: A person engages in willful misconduct for purposes of these Principles if they engage in unlawful conduct voluntarily and intentionally and with the specific intent to do something the law forbids. A person must know that their actions are unlawful but need not know the specific law that they are violating.

§ 6.02. Enforcement Policies for Nontrial Criminal, Civil, or Administrative Resolutions of Organizational Misconduct

(a) When seeking nontrial resolutions of criminal, civil, and administrative enforcement actions against organizations, enforcement authorities should act in accordance with a written enforcement policy that is publicly available so that organizations may predict, with reasonable accuracy, what actions of theirs will affect the offered nontrial resolution.

(b) To achieve the public interest in cases involving material criminal or civil misconduct, the enforcement policy should be structured to:

(1) promote proactive pursuit of enforcement actions against the individuals responsible for the misconduct;

(2) provide predictable and substantive incentives to organizations to:

(A) detect and self-report material misconduct to enforcement authorities, in accordance with § 6.04;

(B) fully cooperate with enforcement authorities' investigations, including by providing evidence on the identity and culpability of the individual wrongdoers substantially responsible for material misconduct, in accordance with § 6.05;

(C) promptly terminate the misconduct; and

(D) reduce the risk of future material misconduct by remediating its underlying causes, in accordance with § 6.07;

(3) ensure that individual and organizational wrongdoers disgorge any net benefits from their misconduct, remediate the harm caused, and pay restitution to victims where appropriate, in accordance with § 6.07;

(4) impose sanctions on organizations that are appropriate and consistent with § 6.02(b) (2); and

(5) provide public disclosure of the relevant facts about material misconduct and the basis for and contents of the resulting nontrial criminal, civil, or administrative resolution.

(c) Enforcement policy should promote cooperation and coordination between the different enforcement authorities that are investigating and considering enforcement actions for the same instances or patterns of misconduct.

(d) Nontrial resolutions with organizations are inappropriate unless enforcement officials have a good-faith belief, based on the evidence, that there is sufficient evidence to support bringing criminal charges or a civil action against the organization.

(e) Organizations should be provided a transparent procedure for presenting to senior enforcement personnel a good-faith argument that they did not violate the law or an existing nontrial resolution, without risk of adversely impacting the nontrial resolution.

(f) A nontrial resolution with an organization of a criminal case should not name an individual as a perpetrator unless the individual is a party to the agreement, was previously adjudicated to be legally responsible for the misconduct, or otherwise had an opportunity to be heard.

§ 6.03. Accountability of Individual Wrongdoers for Organizational Misconduct

(a) Enforcement officials investigating material organizational misconduct should:

(1) seek to identify, as early as reasonably possible in the investigation, the individuals who are substantially responsible for any material misconduct, including any high-level personnel or substantial authority personnel;

(2) focus on obtaining evidence against them as early as reasonably possible in the investigation; and

(3) communicate and coordinate with other enforcement authorities in the investigation of individuals responsible for material misconduct to the extent reasonably practical;

(b) In seeking to resolve cases involving material misconduct by an organization, enforcement officials should:

(1) pursue appropriate enforcement actions against culpable individuals who committed and are substantially responsible for material misconduct;

(2) ensure that they are subject to appropriate sanctions and do not retain any benefit resulting from their misconduct;

(3) communicate and coordinate with other enforcement officials about the proposed resolution of an action against an individual to help ensure that appropriate sanctions are imposed; and

(4) predicate their assessment of an organization's remedial undertaking on whether the organization has taken appropriate actions to hold accountable those organizational actors who committed, condoned, or knowingly failed to terminate the misconduct, or who were substantially responsible for material deficiencies in the organization's efforts to detect it, investigate it, or appropriately remediate it in accordance with § 6.07.

§ 6.04. Voluntary Self-Reporting by Organizations

(a) To be deemed to have self-reported material organizational misconduct for purposes of these Principles (e.g., §§ 6.17–6.20, 6.22, 6.25), an organization generally should have:

(1) voluntarily disclosed criminal or civil misconduct to criminal and civil enforcement officials, respectively, prior to either:

(A) detection of the misconduct (or a known imminent threat that it will be detected) by enforcement officials; or

(B) commencement of an investigation by prosecutors, civil enforcement officials, or regulators into whether the organization engaged in the misconduct;

(2) disclosed such misconduct within a reasonably prompt time after becoming aware of it;

(3) disclosed all of the relevant facts reasonably known to the organization at the time of its self-report about the nature and scope of the misconduct, and the identity and role of any organizational actors involved in, or responsible for, the misconduct, and any material deficiencies related to the organization's response to it; and

(4) disclosed all information obtained subsequently during the organization's investigation about the nature and extent of any material misconduct and the identity of those involved in or responsible for it that can be disclosed without waiver of any attorney–client privilege or work-product protections (see § 6.05).

(b) An organization that receives information about material organizational misconduct through an internal report may obtain credit for self-reporting pursuant to subsection (a), even if the organization has reason to believe that the source of the internal report may have reported, or is about to report, the misconduct to government authorities, as long as the organization:

(1) reports the misconduct within a reasonable time after receiving the information from the employee and prior to being informed that the government has commenced an investigation of the misconduct; and

(2) otherwise satisfies the conditions in subsection (a), including investigating and reporting any suspected misconduct beyond the subject of the internal report.

§ 6.05. Full Cooperation by Organizations

(a) To be deemed to have fully cooperated for purposes of these Principles, an organization must:

(1) conduct a thorough investigation into any suspected material misconduct; and

(2) provide the following information to the relevant enforcement officials to the extent it can do so consistent with § 6.06:

(A) the material facts known to the organization that relate to the misconduct or additional misconduct detected during the investigation;

(B) the identity, and nature of the involvement, of all individuals who the organization knows or has reason to know:

(i) were substantially involved in, or responsible for, the misconduct, including all high-level or substantial authority personnel who knowingly participated in in the misconduct;

(ii) possess information likely to be material to the government's investigation; or

(iii) are high-level or substantial authority personnel who bear material responsibility for any deficiencies in the organization's detection, investigation, and remediation of the misconduct, and any deficiencies in the organization's cooperation with enforcement authorities.

(3) all material documentary and digital evidence relevant to the misconduct and any other material information known to the organization that is:

(A) not subject to attorney–client privilege or work-product protection; and (B) not precluded from production by other applicable laws.

(b) To be deemed to have fully cooperated, during the course of and following its investigation, an organization also should:

(1) disclose proactively to enforcement officials, and undertake continuing disclosure of:

(A) relevant information or evidence about which it becomes aware relating to the scope and nature of any material misconduct;

(B) the identity and culpability of those who committed the material misconduct; and

(C) the existence and location of material evidence relating to the material misconduct, even if it is not in the organization's possession;

(2) act in good faith to ensure the timely preservation of relevant documents and evidence by organizational actors and third parties acting on the organization's behalf who could have material information pertaining to any material misconduct;

(3) make employees who possess relevant information available to enforcement officials, subject to any limitations imposed by law;

(4) comply with enforcement officials' reasonable and justified requests that the organization not interview particular organizational actors or other witnesses absent a legal obligation to do so or the need to obtain information that is material to identifying and terminating ongoing misconduct likely to cause material harm to the persons or property of others.

(c) A determination as to whether an organization fully cooperated in a government investigation should not be adversely affected by the organization's:

(1) efforts to assist its employees to safeguard their rights, such as by indemnifying them for their defense costs and advising them of their right to obtain their own legal counsel;

(2) unwillingness to enter into a criminal or regulatory settlement on a specific set of charges; or

(3) reasonable, good-faith assertion of a right or obligation not to disclose pursuant to its attorney–client privilege or work-product protection (see § 6.06) or other laws.

(d) Failure to fully cooperate is not itself evidence of misconduct and thus does not provide an independent basis for enforcement officials to file criminal charges or a civil or

administrative enforcement action against an organization, absent a statute or regulation requiring cooperation.

§ 6.06. Cooperation: Waiver of the Attorney–Client Privilege and Work-Product Protection

(a) Enforcement authorities should not seek waiver of the attorney–client privilege or work-product protection as a condition of giving the organization credit for cooperation.

(b) Communications falling within the attorney–client privilege, and thus subject to subsection (a) absent an exception to the attorney–client privilege or an assertion by the organization of an advice-of-counsel defense, include communications:

(1) between:

(A) an organization and its inside or outside legal counsel; or

(B) an organization through its inside or outside legal counsel and the organization's employees during an internal investigation conducted for the purposes of determining whether and to what extent a legal violation has occurred, or for determining the organization's appropriate legal response to it; and

(2) made for the purposes of seeking or dispensing legal advice on behalf of the organization about the organization's activities.

(c) Enforcement officials can require an organization to disclose information known to it about the facts of its misconduct and its organizational actors' involvement in it because the organization can disclose this information without waiving the attorney–client privilege or work-product protection, even if it obtained that information through privileged interviews of organizational actors.

(d) An organization risks waiver or partial waiver of its attorney–client privilege if it reveals:

(1) the transcript of a privileged interview between an organizational actor and the organization's legal counsel; or

(2) specific statements made by an organizational actor to the organization's legal counsel during a privileged interview.

(e) When an organization has asserted an advice-of-counsel defense or otherwise placed attorney–client communication at issue in its response to a government investigation, enforcement authorities may ask for disclosure of the organization's communications with the lawyer that allegedly support this defense, as well as any associated attorney work product.

(f) Enforcement authorities should adopt preapproval and oversight procedures to guide individual enforcement officials' requests that an organization waive attorney–client privilege and work-product protections, where such requests are not based upon a legal exception.

§ 6.07. Disgorgement, Restitution, and Remediation by Organizations

(a) To be deemed to have undertaken full disgorgement, restitution, and remediation, an organization must do the following prior to, or as part of, any resolution for organizational misconduct:

(1) terminate the misconduct;

(2) make restitution for harm caused to victims;

(3) remediate material harm caused by the misconduct to persons or property;

(4) disgorge or agree to disgorge any benefit derived from the misconduct that has not been, or will not be, paid as restitution or by way of other remedial measures, either before or shortly after the date of the resolution;

(5) conduct an assessment of the underlying material causes of the misconduct and make or initiate any needed reforms to remedy any deficiencies; and

(6) take appropriate actions with respect to persons who are employees, non-employee agents, or suppliers of the organization, and who committed the misconduct; knowingly induced, condoned, failed to terminate, or failed to internally report it; or knowingly impeded compliance officers or the investigation.

(b) An organization may make restitution for the harm caused by the misconduct through payments made to persons harmed by the misconduct or to enforcement authorities with jurisdiction over the matter.

(c) Organizations considering disciplinary actions against organizational actors should give them appropriate opportunity to respond to any claims against them.

(d) When an organization is subject to enforcement actions by multiple enforcement authorities, the enforcement authorities should coordinate to ensure that the total amount of the restitution, disgorgement, and remediation required across all of the actions is appropriate.

§ 6.08. Assessing the Effectiveness of an Organization's Compliance Function

(a) In assessing the effectiveness of an organization's compliance program, enforcement officials should reference the Principles set forth in Chapters 3 and 5 to assess whether the compliance program was:

(1) well-designed;

(2) adequately resourced and empowered to function effectively; and

(3) effectively implemented.

(b) Enforcement officials also should consider facts relating to the nature of an organization's misconduct and the organization's response that are relevant to the effectiveness of its compliance program, including:

(1) the underlying material causes of the misconduct;

(2) the appropriateness of the organization's response to any detected misconduct and the underlying causes of any deficiencies in the organization's efforts to detect, terminate, investigate, and remediate it;

(3) the pervasiveness and duration of any detected misconduct;

(4) complicity, if any, of high-level or substantial authority personnel of the organization or a unit thereof in committing, inducing, or condoning the misconduct; and

(5) awareness of any misconduct on the part of any employees, and, if so, whether they reported it to their supervisor, the organization's compliance or ethics department, or the organization's internal-reporting system.

§ 6.09. Required Internal Reforms to an Organization's Compliance Function

(a) Unless contrary to applicable law or regulation, criminal, civil, and administrative resolutions may include provisions that require an organization to undertake or to continue

specific reforms, including changes to the organization's compliance program, or the hiring of a compliance monitor.

(b) A nontrial resolution with an organization may require the organization to maintain any reforms it implemented prior to the resolution for the duration of the agreement.

(c) A nontrial resolution with an organization may require the organization to adopt and implement an effective compliance program that meets standards defined under applicable law or regulation, or official guidance or guidelines issued by an enforcement authority or regulator.

(d) An enforcement official who is part of a regulator with substantial authority over the organization that extends to ensuring that its compliance program is effective may require the organization to undertake specific reforms beyond those associated with subsections (b), (c), and (e) if consistent with the regulator's authority.

(e) Except as provided in subsection (d), enforcement officials presumptively should not require organizations to undertake specific reforms beyond those specified in subsections (b) and (c) unless one of the following circumstances exist:

(1) the mandated reform is directly designed to address a cause of material misconduct that has not been fully remediated by the organization's voluntary reforms; or

(2) the enforcement official has substantial reasons for concluding that the organization's current executive management or its board of directors cannot be relied upon to adopt and implement an effective compliance program, and the compliance deficiency requiring remediation will not likely be addressed by a regulator with substantial authority over the organization.

(f) Enforcement officials who require an organization to undertake specific reforms pursuant to subsection (e)(2) should:

(1) target the required reforms at remediating a material cause of the misconduct;

(2) disclose in the nontrial resolution the justifications for imposing the required reforms; and

(3) include provisions in the nontrial resolution to ensure effective oversight of the organization's compliance with the required reforms by a party independent of executive management and the board of directors.

(g) Prosecutors' offices, civil enforcement offices, and regulatory authorities whose enforcement officials have authority to incorporate required reforms in nontrial resolutions should:

(1) provide clear guidance to their enforcement officials on when they should and should not use settlement agreements to impose remedial measures on organizations and what those measures should be;

(2) provide a way for their enforcement officials to obtain additional guidance or to consult with experts in compliance, in the industry, or in the regulatory requirements applicable to the organization so as to be better able to evaluate whether an organization's compliance program is effective; and

(3) periodically undertake a systematic evaluation of both the effectiveness and cost of their recommended remedial measures and the effectiveness of their oversight of the implementation of those measures and modify the measures as appropriate.

§ 6.10. Factors Relevant to the Appropriateness of a Monitor or Other External Oversight of an Organization

(a) An organization is presumed not to need a monitor if it:

(1) self-reported, fully cooperated, and undertook full disgorgement, restitution, and remediation consistent with §§ 6.03–6.07; or

(2) had an effective compliance program at the time of the misconduct, promptly terminated this misconduct and fully remediated the root causes of both the misconduct and any deficiencies in the organization's compliance program in accordance with § 6.07, and fully cooperated with the government's investigation in accordance with § 6.05.

(b) Enforcement officials should only require external oversight over an organization through a monitor if:

(1) an organization's compliance program was not effective at the time of the misconduct and has not been fully remediated in accordance with § 6.07 prior to the nontrial resolution; and

(2) organizational actors with authority to ensure the future effectiveness of the compliance program have not demonstrated that they can be relied on to adopt and implement an effective compliance program consistent with § 6.08 and to implement other measures needed for full remediation without oversight.

(c) Enforcement officials may appropriately impose a monitor to oversee the organization's operations in a specific country if that country's laws prevent enforcement officials from fully investigating the misconduct or ascertaining whether an organization has fully remediated the underlying causes of the misconduct.

§ 6.11. Duties and Authority of Compliance Monitors

(a) A monitor's primary responsibility is to assess and monitor an organization's compliance with the terms of the settlement agreement that are specifically designed to address and reduce the risk of future material misconduct, including evaluation of and overseeing the implementation of the organization's compliance program.

(b) A compliance monitor should:

(1) be independent;

(2) not be an employee or agent of the organization or the government; and

(3) at all times exercise independent judgment with respect to the performance of his or her tasks.

(c) The agreement governing the monitorship should specify:

(1) the nature of the monitor's responsibilities; the extent and duration of the monitor's authority; arrangements for the monitor's compensation; the form, frequency, and confidentiality of the monitor's reports; and the people who should receive the monitor's reports;

(2) that a monitor who detects potential material misconduct may undertake a preliminary investigation to determine whether misconduct has occurred and, if so,

whether it warrants a report either to the organization or to both the organization and enforcement officials;

(3) that the monitor should:

(A) determine findings and conclusions fairly, objectively, and impartially, based on the relevant evidence;

(B) state the factual basis for findings and maintain records sufficient to show it; and

(C) disclose any material facts that are inconsistent with the monitor's conclusions and explain why the monitor nevertheless reached his or her ultimate decision;

(4) that the organization is obligated to provide accurate information to the monitor and correct any material errors or deficiencies if the organization learns that inaccurate information has been provided;

(5) that the monitor should promptly correct any detected material errors or inaccuracies in previously issued reports and formally notify all recipients of the reports;

(6) that the monitor has appropriate discretion to modify, adjust, or discontinue a remedial or compliance measure if the monitor finds that it is impractical or inadvisable to continue the measure and the applicable regulator or prosecutor approves;

(7) that the monitor should promptly report to enforcement authorities if the organization does not adopt a material recommendation of the monitor within a reasonable time, along with the organization's reasons for not complying;

(8) the basis for the monitor's compensation and require a regular report of that compensation to both the organization and enforcement authorities;

(9) the procedures to be used to resolve any dispute that may arise between the monitor and the organization; and

(10) that the monitor cannot have or obtain a financial interest in the organization and that the organization cannot hire the monitor to perform other services, directly or through any affiliated entity, for a material period after the end of the monitorship.

§ 6.12. Selection and Oversight of Compliance Monitors by Enforcement Officials

(a) Enforcement officials should adopt a process for selecting monitors that is designed to ensure that the monitor selected has the expertise, experience, integrity, resources, and independence needed to be an effective monitor for the type of organization that is the subject of the nontrial resolution.

(b) The integrity and quality of the selection process can be enhanced through the creation of a supervisory body, such as a standing committee, that is responsible for overseeing the selection of monitors.

(c) Prior to selecting a monitor, enforcement officials should consult with the organization and other regulatory authorities with expertise in the relevant areas to identify:

(1) the necessary qualifications for a monitor based on the facts and circumstances of the case; and

(2) a diverse pool of candidates with the expertise and other traits need to be a good monitor, including a detailed justification for the inclusion of each candidate.

(d) An individual should not be selected as a monitor if:

(1) there is a reasonable basis for concluding that the person is, for any substantial reason, incapable of making a decision in the best interests of the organization's legal compliance. Such reasons include that the person:

(A) has a financial stake in the organization or in any businesses owned or controlled by employees of the organization, directly or through an immediate family member;

(B) is currently receiving or reasonably expects to receive any benefit from the organization or any of its employees, other than the remuneration expressly agreed upon for monitor services;

(C) is loyal to, beholden to, or otherwise influenced by an organization-affiliated party, including members of executive management, so as to undermine the monitor's ability to perform his or her duties impartially, or

(2) the individual previously engaged in material misconduct.

(e) To enable oversight of the monitorship and the organization, the monitoring agreement should:

(1) require the monitor to make periodic, confidential written reports to both enforcement officials and the organization;

(2) require the monitor, in appropriate circumstances, to send his or her periodic written reports to a regulatory agency with substantial authority over the organization that was not a party to the monitor agreement and/or to the court that approved the agreement; and

(3) in appropriate circumstances, provide a mechanism for the organization to meet periodically with the relevant enforcement official to discuss its remediation activities and any material issues that have arisen during the monitorship.

§ 6.13. Compliance Consultants

(a) Compliance consultants are responsible for providing input and advice to an organization in the implementation of its compliance program.

(b) A compliance consultant should not counsel an organization to engage in, or assist an organization in engaging in, conduct that misleads or unlawfully impedes a government official in the performance of an official function.

(c) Enforcement officials who determine that a compliance consultant has not been acting in good faith to promote an organization's genuine compliance with the law can appropriately condition the decision to give the organization credit for remediation on the organization's agreement to cease using that compliance consultant and may treat use of that consultant as a factor weighing against the conclusion that the organization has an effective compliance program.

§ 6.14. Mandated Limitations on an Organization's Business Activities

(a) Enforcement officials should have a presumption against including any provision in a nontrial resolution that restricts an organization from engaging in specific lawful business activities unless statutes or regulations expressly authorize the enforcement authority to place limitations on the organization's ability to conduct its business.

(b) In rare circumstances, an enforcement official who is not expressly authorized by law to impose collateral consequences may appropriately include a provision in a nontrial

resolution of a matter involving material misconduct that restricts the organization from engaging in a specific business activity for a specified period of time if:

(1) a substantial portion of the organization's engagement in such business activity was found to violate the law;

(2) the organization's continued engagement in this business activity presents an exceptionally high risk of future material misconduct that has not been adequately remediated; and

(3) the risk of future material misconduct cannot be adequately addressed through other measures, such as enhanced oversight by a regulator or a monitor or collateral consequences imposed by an agency with express authority to restrict the organization's business activities.

(c) A decision to restrict the scope of an organization's business activities under subsection (b) should be made by, or in consultation with, the appropriate regulator or in consultation with senior officials in the relevant enforcement authority.

§ 6.15. Forms of Criminal Nontrial Resolutions for Organizations

(a) Criminal prosecutors may use a variety of forms of nontrial criminal resolutions to resolve a criminal case with an organization that prosecutors have concluded engaged in criminal misconduct as a result of criminal actions by its employees committed in the scope of their employment to benefit the organization, including a:

(1) guilty plea;

(2) deferred prosecution agreement (DPA);

(3) non-prosecution agreement (NPA);

(4) declination with disgorgement; or

(5) declination.

(b) A guilty plea and a DPA may share the following features:

(1) filing in court;

(2) a statement of the charges filed by indictment or information;

(3) a statement of facts in which the organization admits responsibility for criminal misconduct;

(4) a statement of the reasons why the organization was offered or refused a DPA;

(5) financial penalties including disgorgement of the profits attributable to the misconduct, payment of restitution, remediation for harms to others, and a criminal fine;

(6) a provision requiring the organization to fully cooperate in accordance with § 6.05;

(7) a provision requiring that the organization fully remediate in accordance with § 6.07, including through specified internal reforms when in accordance with § 6.09;

(8) a requirement that the organization pay for and cooperate with a monitor, in accordance with §§ 6.10–6.12; and

(9) a requirement that the organization periodically report to prosecutors concerning its internal investigation, its remediation activities, and any newly detected criminal misconduct.

(c) An NPA may contain all the provisions in § 6.15(b) except that they are not filed in court and no charges are filed.

(d) Guilty pleas can produce consequences that do not result from resolution through a DPA or NPA:

(1) for certain offenses, a guilty plea can result in the organization being subject to presumptive or mandatory collateral consequences such as debarment, exclusion, or delicensing by federal, state, local, or other authorities.

(2) a guilty plea can establish the organization's liability in a civil or administrative enforcement action or private civil litigation through offensive collateral estoppel.

(e) A guilty plea, DPA, or NPA with an organization should be publicly disclosed and made available and should explain the facts of the misconduct, the crime the organization committed, the justification for using the form of nontrial resolution imposed, the sanctions and other consequences resulting from the resolution, any provisions for providing restitution or remediation to victims, any voluntary remediation by the organization, and the duration of the resolution.

§ 6.16. Declinations (traditional)

(a) An organization should be offered a declination (without a precondition of disgorgement, restitution or remediation) if the prosecutor determines that:

(1) the evidence does not establish beyond a reasonable doubt that the organization committed a crime; or

(2) the offense is not material, as defined in § 6.01(s), or otherwise does not warrant prosecution.

§ 6.17. Guilty Pleas

(a) Except as provided in subsection (c), prosecutors should presumptively resolve a case involving material criminal misconduct through a guilty plea unless the organization:

(1) self-reported misconduct in accordance with § 6.04; or

(2) fully cooperate in accordance with § 6.05, including by identifying and providing all evidence reasonably available against all employees substantially involved in the misconduct, and engaged in full disgorgement, restitution, and remediation in accordance with § 6.07.

(b) Prosecutors should presumptively not seek to impose a guilty plea on an organization that self-reported or fully cooperated, in accordance with §§ 6.04 and 6.05, and also fully remediated, in accordance with § 6.07.

(c) When a guilty plea is the presumptively appropriate form of criminal resolution under subsection (a), a prosecutor may instead offer to resolve a case involving material misconduct through a deferred prosecution agreement if:

(1) conviction would subject the organization:

(A) to presumptive or mandatory material collateral consequences in the United States or abroad that would impose material harm on consumers, employees in organizational units not involved in the misconduct, or the public, that cannot be addressed through a prior agreement with the authorities positioned to impose the collateral consequences; or

(B) additional civil or administrative sanctions to government agencies or private parties in the United States or abroad whose combined magnitude exceeds the sanctions appropriately imposed for the misconduct and it is impracticable for enforcement officials to enter into a coordinated resolution with all the parties who could impose liability on the organization, and

(C) one of the following conditions is met:

(i) the organization had an effective compliance program at the time of the misconduct; provided sufficient cooperation to identify and provide actionable evidence against all individuals who were knowingly or intentionally involved in committing, attempting to commit, conspiring to commit, aiding and abetting the commission of, the misconduct or who knowingly failed to internally report or terminate the misconduct; and the organization has engaged in full disgorgement, restitution, and remediation in accordance with § 6.07; or

(ii) the organization currently is acting in good faith to satisfy § 6.24(b)(2); or

(iii) all high-level or substantial authority personnel responsible for the organization's earlier refusal to fully cooperate are no longer with the organization in a position of authority; the organization has provided sufficient cooperation to identify and provide actionable evidence against all individuals who were knowingly or intentionally involved in committing, attempting to commit, conspiring to commit, aiding and abetting the commission of the misconduct, or who knowingly failed to internally report or terminate the misconduct; and the organization has engaged in full disgorgement, restitution, and remediation in accordance with § 6.07.

(d) Guilty pleas should ensure full disgorgement, restitution, and remediation in accordance with § 6.07, should impose criminal fines, and may include provisions that require internal reforms or a monitor in accordance with §§ 6.09–6.12.

§ 6.18. Declinations Following Disgorgement, Restitution, and Remediation

(a) An organization that committed material criminal misconduct should not be offered a declination following disgorgement, restitution, and remediation unless it self-reported the criminal misconduct (in accordance with § 6.04), fully cooperated with prosecutors (in accordance with § 6.05), and engaged in timely and full disgorgement, restitution, and remediation (in accordance with § 6.06) [hereinafter "full corrective action"].

(b) An organization that undertook full corrective action should presumptively receive a declination with full disgorgement pursuant to this Section unless an aggravating circumstance is present, as defined in subsection (c).

(c) For purposes of determining the form of civil or criminal nontrial resolution with an organization, the following constitute aggravating circumstances:

(1) high-level or substantial authority personnel of the organization or a unit thereof:

(A) knowingly participated in committing material misconduct;

(B) knowingly participated in efforts to impede the detection or investigation of material misconduct;

(C) knowingly failed to intervene to terminate material misconduct or report it to appropriate authorities within the organization after becoming aware of it; or

(D) were willfully blind to material misconduct;

(2) the material misconduct caused substantial harm to persons, property, or the public interest;

(3) the material misconduct occurred over many years or was widespread within the organization; or

(4) the organization is a recidivist in that it entered into a criminal or civil enforcement resolution for similar material misconduct within the last five years, and its remediation of the past misconduct was, in light of all surrounding circumstances, inadequate.

(d) An organization that engaged in full corrective action may appropriately be offered a declination following full disgorgement, restitution, and remediation even if

aggravating circumstances in subsection (d)(1) or (2) are present, provided that subsections (d)(3) or (4) do not apply and the following conditions are met:

(1) all high-level or substantial authority personnel who:

(A) knowingly participated in committing the offense;

(B) knowingly participated in undermining detection or investigation of the offense;

(C) knowingly failed to intervene to terminate the offense or report it to appropriate authorities within the organization after becoming aware of it; or

(D) were willfully blind to the misconduct;

are no longer with the organization in positions of authority;

(2) the organization has identified and provided the evidence reasonably available against all of its employees—including all high-level or substantial authority personnel—who participated in committing the offense with the requisite mens rea for the offense;

(3) the organization terminated and self-reported all detected misconduct promptly; and

(4) the organization undertook prompt and full disgorgement, restitution, and remediation sufficient to disgorge all profits from the offense, remedy the harm caused thereby, and establish and implement an effective compliance program.

(e) An organization that engaged in full corrective action should presumptively not be subject to a monitor, even if aggravating circumstances are present, consistent with §§ 6.10 and 6.12.

§ 6.19. Deferred and Non-Prosecution Agreements

(a) An organization that did not self-report or fully cooperate (in accordance with § 6.05) should presumptively not be offered a deferred prosecution agreement (DPA) or and non-prosecution agreement (NPA) in a case involving material criminal misconduct except as provided in § 6.17(c).

(b) An organization that undertook full corrective action in accordance with §6.01(n), but is not eligible for a declination pursuant to § 6.18(c) & (d), should presumptively be offered an NPA if the following conditions are satisfied:

(1) all high-level or substantial authority personnel who:

(A) knowingly participated in committing the offense or knowingly participated in undermining detection or investigation of the offense; or

(B) knew about material misconduct and failed to intervene to terminate it or report it to appropriate authorities within the organization after becoming aware of it;

are no longer with the organization in positions of authority;

(2) the organization has identified and provided all evidence reasonably available against all of its employees—including all high-level or substantial authority personnel—who participated in committing the offense with the requisite mens rea for the offense;

(3) the organization has undertaken a good-faith and reasonable effort to undertake full disgorgement, restitution, and remediation, including acting proactively in good faith to adopt and implement an effective compliance program; and

(4) the aggravating circumstances of § 6.18(c)(3) & (4) do not apply.

(c) An organization that fully cooperated (in accordance with § 6.05), and undertook full disgorgement, restitution, and remediation (in accordance with § 6.07), should presumptively be offered a DPA, and not an NPA or declination, if:

(1) it did not self-report detected material misconduct in accordance with § 6.04; or

(2) it self-reported detected misconduct but the aggravating circumstances set forth in § 6.18(c)(3) or (4) are present.

§ 6.20. Monetary Penalties in Nontrial Criminal Resolutions with Organizations that Committed Material Criminal Misconduct

(a) An organization that committed detected material misconduct should be required to undertake full disgorgement, restitution, and remediation in accordance with § 6.07.

(b) Criminal enforcement officials should structure their policy governing monetary penalties to recommend substantially lower fines for those organizations with material criminal misconduct that self-reported and fully cooperated (in accordance §§ 6.04 & 6.05) than for organizations that either:

(1) fully cooperated; or

(2) had an effective compliance program at the time of the misconduct, but did not self-report.

(c) An organization that undertakes full corrective action should presumptively not be subject to a criminal fine if the organization is presumptively eligible for a non-prosecution agreement under § 6.19(b).

(d) Criminal and civil enforcement officials should coordinate the penalties imposed on an organization sanctioned for misconduct.

(e) Prosecutors considering a request to adjust sanctions based on an organization's inability to pay should:

(1) determine the veracity of the claim, including by assessing recent and projected disbursements to shareholders and owner-managers;

(2) predicate a downward adjustment on the organization undertaking all appropriate remedial actions available to it, including appropriate disciplinary actions;

(3) place a priority on ensuring victim restitution and remediation of harm, and evaluate mechanisms for providing restitution and remediation through the organization's future earnings; and

(4) the nontrial resolution prohibits the organization from making any distributions to shareholders and from providing incentive compensation or bonuses to high-level personnel until the organization has satisfied its obligations to make payments to criminal, civil and administrative authorities.

§ 6.21. Forms of Civil Nontrial Resolutions and Sanctions for Organizations

(a) Civil and regulatory enforcement officials may resolve a matter with an organization that they have determined engaged in knowing or intentional material misconduct through the following forms of nontrial resolutions:

(1) a resolution in which the organization is formally adjudicated without a trial to have committed the misconduct;

(2) a full-admission resolution under which the organization is required to admit to all of the facts needed to establish that the organization engaged in the misconduct but is not formally adjudicated to have committed the misconduct (e.g., many regulatory deferred prosecution agreements);

(3) a partial-admission resolution under which the organization admits to some of the material facts of the misconduct, but not to all the facts needed to establish that it engaged in the misconduct, and is not formally adjudicated to have committed the misconduct;

(4) a neither-admit-nor-deny resolution under which the organization is found to have engaged in the misconduct and is prohibited from publicly denying that it engaged in the misconduct (except in certain limited circumstances, such as in litigation against the organization by a party other than the enforcement authority that entered into the resolution), but is not required to admit that it engaged in misconduct; or

(5) a no-admission/denial-permitted resolution under which the organization is found to have engaged in the misconduct, but is not required to admit to any facts of the misconduct and may publicly deny that it engaged in the misconduct.

(b) Civil and regulatory authorities may seek a variety of forms of relief including:

(1) civil or administrative monetary sanctions;

(2) an injunction against future misconduct;

(3) disgorgement or forfeiture of the benefit of misconduct;

(4) remediation;

(5) restitution;

(6) debarment, exclusion, or delicensing; and

(7) remedial measures, such as requiring compliance-program reforms and appointing a compliance monitor.

§ 6.22. Enforcement Policy for Civil and Administrative Nontrial Resolutions

(a) A civil or administrative enforcement authority should issue and make publicly available a written enforcement policy setting forth the factors that its enforcement officials will use when determining whether to employ a form of nontrial resolution that would:

(1) trigger, or avoid triggering, mandatory, presumptive, or permissive collateral consequences;

(2) adjudicate that the organization engaged in material misconduct;

(3) require the organization to admit to all or some of the facts of the misconduct; or

(4) preclude the organization from denying—or permit the organization to deny—that it engaged in misconduct.

(b) The written enforcement policy should provide that an organization should not be granted a downward adjustment in monetary penalty based on the organization's inability to pay unless:

(1) enforcement officials have determined that the organization truly cannot pay;

(2) the organization did not make substantial disbursements to shareholders or high-level personnel during the period between when the organization became aware of the misconduct and the nontrial resolution;

(3) the organization has undertaken all appropriate remedial actions available to it, including appropriate disciplinary actions against employees and agents who committed, conspired to commit, aided and abetted the commission of the misconduct or failed to take appropriate action upon becoming aware of the misconduct, in accordance with § 6.07;

(4) the nontrial resolution is structured to place a priority on ensuring that victims receive restitution and that harm is remediated, including through measures designed to require that restitution payments be made from the organization's future earnings; and

(5) the nontrial resolution prohibits the organization from providing distributions to shareholders, or incentive compensation or bonuses to high-level personnel, until the organization has satisfied its obligations under the agreement.

§ 6.23. Traditional Declinations and Decisions Not to Pursue an Enforcement Action

(a) Enforcement officials should decline to pursue an enforcement action if they determine that:

(1) they do not have, and would be unlikely to obtain through a full and thorough investigation, sufficient evidence to establish that the organization violated the law; or

(2) the misconduct is not material, as defined in § 6.01(s), or otherwise does not warrant an enforcement action.

§ 6.24. Choice of Nontrial Resolution When an Adjudicated Resolution Could Trigger Collateral Consequences in the United States or Abroad

(a) An organization that engaged in knowing or intentional material misconduct should presumptively be offered a nontrial resolution that finds the organization culpable for the misconduct and is not structured to avoid triggering mandatory, presumptive, or permissive collateral consequences for the organization, except as provided in subsections (b) and (c).

(b) An organization that engaged in knowing or intentional material misconduct should presumptively be offered a nontrial resolution that is structured to avoid triggering mandatory, presumptive, or permissive collateral consequences for the organization in the United States or abroad if the organization:

(1) engaged in full corrective action in accordance with §§ 6.01(n), 6.04, 6.05, and 6.07;

(2) fully cooperated in accordance with § 6.05 and undertook full disgorgement, restitution, and remediation in accordance with § 6.07, or

(3) undertook full disgorgement, restitution, and remediation in accordance with § 6.07 and engaged in substantial material cooperation which, while not fully in accordance with § 6.05, provided enforcement officials with material evidence that they otherwise did not have, and could not readily obtain, about:

(A) the full extent of the organization's knowing or intentional material misconduct or

(B) about the identity and culpability of all employees—including all high-level or substantial authority personnel—who:

(i) knowingly participated in committing, conspiring to commit, attempting to commit, or aiding and abetting the commission of the misconduct;

(ii) knowingly participated in undermining efforts to detect or investigate the misconduct, or failed to intervene to terminate it or report it to appropriate authorities within the organization after becoming aware of it; or

(iii) were willfully blind to the misconduct.

(c) An organization that engaged in knowing or intentional material misconduct should presumptively be offered a nontrial resolution that is structured to avoid triggering mandatory, presumptive, or permissive collateral consequences for the organization in the United States or abroad, even if it has not satisfied the requirements of subsection (b), if, but only if:

(1) imposing collateral consequences on the organization would likely cause material harm to consumers, employees in units of the organization that were not involved in the misconduct, or the public, and the magnitude of that harm would exceed the likely benefits of imposing collateral consequences given the availability of other means for reducing the organization's future risk of misconduct, such as appointing a compliance monitor;

(2) the organization has fully remediated in accordance with § 6.07 or will be required to fully remediate in accordance with § 6.09; and

(3) one of the following conditions is satisfied:

(A) the organization did not fully cooperate based on a good-faith belief, predicated on a reasonable interpretation of the law, that it did not engage in misconduct;

(B) the nontrial resolution requires an organization that did not have an effective compliance program at the time it knowingly or intentionally engaged in material misconduct to accept and pay for oversight by a compliance monitor (in accordance with §§ 6.10–6.12); or

(C) the organization had an effective compliance program at the time of the misconduct, in accordance with Chapter 5.

(d) A nontrial resolution structured to avoid collateral consequences because the organization engaged in full corrective action in accordance with § 6.01(n) should presumptively not impose a monitor on the organization, even if aggravating circumstance were present, consistent with §§ 6.10–6.12.

§ 6.25. Policies Governing Admissions of Facts and Denials of Culpability

(a) An organization that engaged in knowing or intentional material misconduct should presumptively be offered a nontrial resolution that formally adjudicates the organization's culpability or require the organization to fully admit to the facts underlying the misconduct unless:

(1) the organization meets the requirements for a nontrial resolution that avoids triggering collateral consequences under § 6.24(b);

(2) such a determination or admission would trigger mandatory, presumptive, or permissive collateral consequences and § 6.24(c) is satisfied; or

(3) the following conditions are met:

(A) the organization fully remediated in accordance with § 6.07;

(B) the organization provided substantial material cooperation to enforcement officials that either enabled them to either detect and terminate misconduct more rapidly than they could have on their own or provided them with evidence material to their case(s) against the individuals responsible for the misconduct that they could not reasonably have obtained on their own in a timely way, and

(C) a finding of culpability or a full admission could subject the organization to substantial penalties or liability imposed by other parties that cannot be addressed through a coordinated resolution with those parties.

(b) Except as provided in subsection (c), nontrial resolutions that do not adjudicate the organization's culpability or require a full admission of the facts of the misconduct should:

(1) require the organization to admit to most of the material facts of the misconduct; and

(2) state that the organization cannot deny its culpability for the misconduct except in litigation brought against it by others who are not parties to the nontrial resolution.

(c) Civil and administrative enforcement officials entering into a nontrial resolution that does not involve a finding of culpability or a full admission of the facts needed to establish the alleged misconduct should not preclude the organization from denying its culpability for the misconduct if, at the time of the resolution:

(1) the organization provided full cooperation in accordance with § 6.05;

(2) enforcement officials lack sufficient evidence to establish the organization's culpability for the alleged misconduct and do not expect to be able to obtain the evidence needed to prove the misconduct without incurring costs that are excessive relative to the benefit to the public that an admission would provide;

(3) enforcement officials have good-faith and reasonable belief that they could obtain the necessary evidence if they incurred the necessary cost; and

(4) the nontrial resolution sets forth the reasons why the enforcement authority is agreeing to a denial-permitted resolution with the organization.

§ 6.26. Collateral Consequences: Debarment, Exclusion, and Delicensing

To the extent permitted by applicable laws, the following Principles set forth the most effective use of a government agency's authority to impose collateral consequences on an organization under the agency's jurisdiction.

(a) Collateral consequences, such as debarment, exclusion, and delicensing, for knowing or intentional material misconduct should be reserved for situations in which the agency has established that an organization engaged in the misconduct and concluded that:

(1) the organization continues to present a significant risk of committing future material violations that pose harm to the interests that the agency is charged with protecting; and

(2) the risk of future violations cannot be adequately addressed through other means, such as mandated internal reforms, enhanced oversight, or the appointment of a compliance monitor in accordance with §§ 6.09–6.12.

(b) Government officials with authority to impose collateral consequences on an organization that engaged in misconduct presumptively should not impose them on organizations that satisfied § 6.24(b).

(c) Evidence that an organization committed a violation generally does not, in and of itself, establish that the organization presents a significant risk of committing future misconduct when the organization's liability is predicated on either respondeat superior or on absolute liability imposed by a public welfare statute.

(d) In determining whether an organization continues to present a significant risk of committing future material violations sufficient to justify imposing collateral consequences on it, officials should consider the following factors:

(1) whether the misconduct was committed or condoned by high-level personnel in the organization or a unit thereof who remain in positions of authority;

(2) whether the misconduct was widespread within a unit of the organization or across multiple units of the organization and was committed or knowingly condoned by high-level or substantial authority personnel who remain in positions of authority;

(3) whether the misconduct conferred benefits on the organization that were sufficiently large to potentially motivate the organization to engage in similar misconduct in the future, and the risk of this misconduct cannot be adequately reduced through measures such as appointing a compliance monitor;

(4) whether the organization's compensation, promotion, retention, or disciplinary policies were a substantial cause of the misconduct and whether the organization has fully remediated them;

(5) whether the organization has fully remediated all of the deficiencies in its compliance function that existed at the time of the misconduct; and

(6) whether the organization has fully demonstrated its commitment to preventing and deterring misconduct by providing all information reasonably available to it regarding the scope of the misconduct and the identity of, and evidence against, those individuals responsible for it.

(e) Collateral consequences should be restricted to the specific business unit or units within the organization that committed the misconduct and continue to present an ongoing risk, whenever applicable laws allow the authorities to do so. The collateral consequences should remain in place for the period of time necessary for the organization to remediate the internal root causes of the misconduct.

(f) When an organization does not present a substantial risk of committing the same offense in the future, it may be appropriate for those officials with authority over whether to impose collateral consequences to inform both the organization and any other enforcement officials with the authority to sanction the organization that the organization will not be subject to collateral consequences should it be sanctioned for the detected misconduct, if such a waiver is allowed under applicable law.

§ 6.27. Protecting Employees and Agents Who Uphold the Law or Report Misconduct from Retaliation

(a) To the extent permitted by applicable law, civil and administrative enforcement authorities should adopt provisions that provide credible assurances that individuals who provide information about material misconduct to government authorities will not have their identity disclosed, directly or indirectly, until any whistleblower award has been paid, except when enforcement officials:

(1) need to identify the individual in the course of producing documents or calling witnesses during the course of a legal proceeding;

(2) receive authorization from the whistleblower to reveal the person's identity; or

(3) are ordered to reveal the person's identity by a court of law or a statute.

(b) To the extent allowed by law, civil and administrative authorities should protect whistleblowers from retaliation and pretaliation that is, or would be, based on their good-faith decision to report material misconduct internally or to the government.

(1) "Retaliation" includes termination, demotion, reduction of salary, and reduction of responsibilities and authority.

(2) "Pretaliation" is a preemptive effort by an employer to deter whistleblowing. An employer presumptively engages in pretaliation if it adopts any policy likely to be interpreted by a reasonable employee as restricting the employee's ability to disclose nonpublic information about misconduct within the organization to government authorities or self-regulatory bodies. Policies that potentially operate as pretaliation, absent a clause specifically stating that an employee retains the right to report suspected misconduct to the government or self-regulatory bodies and to obtain any recovery that might result from reporting, include:

(A) confidentiality and nondisclosure agreements;

(B) separation and severance agreements;

(C) nondisparagement agreements; and

(D) clauses establishing trade secret or other intellectual property rights in the organization's nonpublic information.

(c) To the extent allowed by law, civil and administrative authorities should adopt and enforce provisions that protect employees from retaliation or pretaliation if they object to conduct that they reasonably believe violates or would violate the law.

(d) An employer that acts adversely against an employee who reported misconduct or objected to engaging in misconduct should not be treated as having acted in retaliation if the employer:

(1) had taken material steps to take the adverse action against the employee prior to when:

(A) the employee decided to report the misconduct internally to the employee's superior or externally to the government;

(B) the organization anticipated that the employee was likely to report misconduct; and

(C) the employee objected to or the employer anticipated that the employee would object to conduct that the employee reasonably and in good faith believed violated the law; and

(2) the employee's decision or anticipated decision to report the misconduct internally or externally or to object to engaging in the misconduct was not a contributing cause of the employer's decision to act adversely against the employee.