2

Implementation of Effective Compliance and Ethics Programs and the Federal Sentencing Guidelines

*Steven D. Gordon**

How should a company go about designing and implementing a compliance program? While other chapters address the specifics of compliance programs in particular industries, this chapter considers issues relating to designing and implementing compliance and ethics programs generally. The biggest influence on the design and implementation of a compliance program is guidance from the U.S. Sentencing Commission contained in the Federal Sentencing Guidelines that apply to companies convicted of federal criminal offenses. The Sentencing Guidelines set standards that have become the norm for

* The author wishes to acknowledge Michael Manthei, Christopher A. Myers, and Jonathan Strouse for their contributions to this chapter.

virtually all companies, even though relatively few will ever be prosecuted or convicted. In fact, the most useful benefit from using the Guidelines to design and implement a compliance and ethics program is that it can help companies avoid investigations and convictions in the first place.

In addition to complying with the Sentencing Guidelines, if the company is publicly held, it must comply with the Sarbanes-Oxley Act of 2002. And if the company is a federal government contractor or subcontractor, the Federal Acquisition Regulation (FAR) comes into play. Other compliance requirements apply to other industries. Fortunately, these various guidelines and requirements do not conflict and, instead, tend to complement each other.

Sentencing Guidelines Basics

Q 2.1 What are the Federal Sentencing Guidelines?

Since 1991, the sentencing of corporations and other business entities convicted of federal criminal offenses has been governed by the Federal Sentencing Guidelines ("Sentencing Guidelines"), established by the U.S. Sentencing Commission. These Sentencing Guidelines originally were mandatory, but in 2005, the Supreme Court ruled that it is unconstitutional to apply them in mandatory form. The Court left them intact as voluntary guideposts that federal courts should consult but are not bound to follow.[1]

In addition to providing guidance on how convicted companies should be sentenced, the Sentencing Guidelines also contain detailed guidance from the Sentencing Commission on what it means to have an "effective" compliance and ethics program. This guidance, contained in chapter 8 of the *Guidelines Manual*,[2] is used by hundreds of companies to design and implement their compliance programs and is also the standard used by many government agencies to evaluate company compliance and ethics programs.

Q 2.2 How do the Sentencing Guidelines relate to an effective compliance program?

A company convicted of a federal offense is eligible for a reduced sentence under the Sentencing Guidelines if it has an effective compliance and ethics program and the offense occurred despite the program.[3] The Sentencing Guidelines spell out the basic elements of an effective compliance program.[4] Additionally, a prosecutor might exercise his or her discretion not to bring criminal charges if the company has a compliance program that meets the Sentencing Guidelines' requirements.

The Department of Justice (DOJ), in the *U.S. Attorney's Manual*, describes factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. These factors include "the existence and effectiveness of the corporation's pre-existing compliance program" and the corporation's remedial efforts "to implement an effective corporate compliance program or to improve an existing one."

Q 2.2.1 Why should my company care about the Sentencing Guidelines if it conducts business honestly and is unlikely ever to face criminal prosecution?

If the business is a corporation, its management probably has a duty to ensure that the business has an adequate compliance program. The Delaware courts have held that corporate management has such a duty under Delaware law in light of the Sentencing Guidelines.[5] Also, having an effective compliance program can show that the corporation was not at fault if an employee does engage in criminal or unethical conduct.

Even ethical companies get investigated. In the event of an investigation, enforcement authorities will look at a variety of factors to determine whether there has been wrongdoing, who is at fault, and whether to bring criminal, civil, administrative, or no claims against the company. Among the most significant factors influencing these decisions is whether the company has a compliance program that meets the Sentencing Guidelines' requirements.

The Fraud Section of the DOJ has published a list of topics it explores and the questions it asks when it assesses the effectiveness of a corporate compliance program.[6] In essence, the topics it explores are the elements of an effective compliance and ethics program described in the Sentencing Guidelines. The questions the DOJ asks probe the company's actual commitment to the compliance program and how well it works in practice.

Components of an Effective Compliance Program

Q 2.3 What policies and procedures should my company implement to meet the Sentencing Guidelines' requirements?

You are required to have written standards and procedures. After performing a thorough assessment of your company's legal, compliance, and reputational risks, you should create policies addressing those risk areas. The number and types of standards and procedures a

company requires depend on a number of factors, including the industry in which the company operates.

Q 2.3.1 What are the elements of an effective compliance program that will satisfy the Sentencing Guidelines?

The Sentencing Guidelines state that the two fundamental elements of an effective compliance and ethics program are:

(1) exercising due diligence to prevent and detect criminal conduct; and
(2) otherwise promoting an organizational culture that encourages ethical conduct and a commitment to compliance with the law.[7]

Q 2.3.2 What specific steps must our company take to create an effective compliance program?

The Sentencing Guidelines provide that, at a minimum, a company must do the following in order to have an effective compliance and ethics program:

(1) Establish standards and procedures to prevent and detect criminal conduct.
(2) Ensure that the company's governing authority (board of directors, etc.) understands the content and operation of the program and exercises reasonable oversight with respect to its implementation and effectiveness. Specific senior manager(s) shall have overall responsibility to ensure the implementation and effectiveness of the program. Specific individuals shall be delegated day-to-day operational responsibility for the program and shall be given adequate resources and authority. They shall report periodically to senior management and shall have direct access to the board of directors or a subgroup thereof.
(3) Keep bad actors out of managerial ranks (or other key positions). Reasonable steps should be taken to screen out persons whom the company knows, or should know through the exercise of due diligence, to have a history of engaging in illegal activity or other misconduct.

(4) Take reasonable steps to communicate periodically and in a practical manner its standards and procedures to its officers, employees, and, as appropriate, its agents, by conducting effective training programs and otherwise disseminating information.
(5) Take reasonable steps to:
  (a) ensure that the program is followed, including using monitoring and auditing to detect criminal conduct;
  (b) evaluate periodically the program's effectiveness; and
  (c) have a system whereby employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation (although a mechanism for anonymous reporting is not required).
(6) Promote and enforce the program through appropriate incentives and disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.
(7) Take reasonable steps to:
  (a) respond appropriately to criminal conduct, which may include providing restitution or remediation and self-reporting and cooperation with authorities; and
  (b) prevent similar criminal conduct, including making any necessary modification to the compliance and ethics program.[8]

Q 2.3.3 Is there a standard compliance program that most companies can use?

No. There is no "one-size-fits-all" solution. The Sentencing Guidelines recognize that an effective program must be tailored to the particular company.

The Sentencing Guidelines require a company to engage in periodic risk assessments in designing, implementing, and modifying its compliance and ethics program.[9] Each company must examine the nature of its business and its own prior history to determine what sorts of criminal conduct pose the greatest risk, and then take steps designed to prevent and detect such misconduct.

For example, if your company employs sales personnel who have flexibility in setting prices, you must have established standards and procedures designed to prevent and detect price-fixing. If you employ sales personnel who have flexibility to represent the material characteristics of a product, you must have established standards and procedures designed to prevent fraud. Your company should prioritize the risks that you face in terms of the severity of the criminal conduct and its likelihood of occurring, and tailor your compliance and ethics program accordingly.[10]

When the DOJ evaluates a compliance program, it asks what methodology the company has used to identify, analyze, and address the particular risks it faces, what information the company collected, and how the company utilized that information in shaping its compliance program.[11]

Designing and Implementing a Compliance Program

Relevant Factors and Considerations

Q 2.4 Are industry practice and standards considered in assessing the effectiveness of a compliance program?

Yes. The Sentencing Guidelines recognize that the particulars of an effective compliance and ethics program are likely to be affected by applicable industry practice or the standards called for by any applicable governmental regulation. For publicly traded corporations, applicable governmental regulations would include the requirements of the Sarbanes-Oxley Act of 2002. A company's failure to incorporate and follow applicable industry practice or to comply with applicable government regulations will weigh against a finding that its compliance program is an effective one.[12] For healthcare companies, the Department of Health and Human Services, through its Office of Inspector General, has issued a number of very specific compliance program guidances targeting specific business sectors such as hospitals and pharmaceutical manufacturers.

Q 2.4.1 Does the company size matter?

Size is a relevant factor in structuring a compliance and ethics program. A large company generally should have more formal operations and devote greater resources to its program than a small company.

Q 2.4.2 What are the differences between compliance programs for large companies and small companies?

- The governing authority in a small company may directly manage the compliance and ethics efforts.
- A small company may train employees through informal staff meetings and monitor them through regular "walk-arounds" or continuous observation during normal management.
- A small company may use available personnel, rather than separate staff, to carry out the compliance and ethics program.[13]

Requirements; Risk Areas

Q 2.5 When it comes to putting a compliance program together, where do we start?

A first step is to determine whether the compliance program must satisfy the mandates of the Sarbanes-Oxley Act[14] in addition to the Sentencing Guidelines. Sarbanes-Oxley, if applicable, imposes fairly detailed requirements that focus on the company's internal control over financial reporting and its disclosure controls and procedures. A good compliance program should also address the prevention of other employee misconduct that may impose civil liability on the company or that may victimize the company itself.

The foundation for designing a good compliance program is to identify the principal risks of misconduct that must be safeguarded against. This is a task that requires input from counsel and senior management. The effectiveness of the compliance program likely will be directly proportional to the time and effort invested in designing it.

Q 2.5.1 What are the most common risk areas that we may need to address in our compliance program?

Consider the following sixteen areas:

1. Accounting practices. Sarbanes-Oxley has made internal control over financial reporting and disclosure controls and procedures the foremost risk area for every public company. It also spells out in detail the procedures that must be used to address this risk area.[15]

Private companies must also protect against the risk that an officer or employee may "cook" or alter the books in order to boost performance or hide problems. Common examples include improper revenue recognition, intentional overstatement of assets, or understatement of liabilities, as well as false entries to cover up employee embezzlement and theft, or expenditures for improper or illegal purposes such as bribes.

2. USA PATRIOT Act. The PATRIOT Act aims to cut off sources of financing for terrorists by strengthening anti-money laundering laws. The PATRIOT Act greatly expanded the definition of "financial institutions" covered by anti-money laundering laws to include not only banks, savings associations, and credit unions, but also securities broker-dealers; investment companies; hedge funds; commodities brokers; mutual funds; issuers or redeemers of travelers checks; operators of credit card systems; insurance companies; telegraph companies; loan or finance companies; automobile, airplane, and boat dealers; real estate brokers; persons or companies involved in real estate closings and settlements; currency exchanges; money transmitters; pawn brokers; travel agencies; dealers in precious metals, stones, or jewels; and casinos.[16]

The PATRIOT Act requires that "*each* financial institution *shall* establish anti-money laundering programs" unless the Treasury Department issues a specific exemption. These programs must include written policies and procedures; a designated compliance officer; employee training; and periodic auditing and monitoring.[17] Further, financial institutions must implement special account opening procedures and "Know Your Customer" due diligence.[18]

In addition, banks, securities broker-dealers, money services businesses, and casinos are required to file reports of suspicious transactions with the Treasury Department's Financial Crimes Enforcement Network.[19] Finally, all persons (not only financial institutions) who receive in excess of $10,000 in cash in one transaction, or two or more related transactions, in the course of their trade or business are required to file a currency transaction report.[20]

3. Conducting business with suspected terrorists. Following the September 11 attacks, Executive Order 13224 mandated creation of a list of persons, entities, and groups believed to be connected with terrorism. This order bans *anyone* in the United States from conducting *any* business with *any* person, entity, or group on the list, which is maintained by the Treasury Department's Office of Foreign Assets Control (OFAC).[21] The OFAC list is constantly updated and now is quite lengthy, consisting of thousands of names, aliases, and "doing business as" designations. Businesses, particularly those with some international component, must ensure that they are complying with the provisions of the Executive Order. Specifically, before entering into or continuing any financial relationship, businesses should check the identities of existing and potential clients and customers against the latest OFAC List.

4. Conflicts of interest; corporate opportunities. Conflicts of interest are an issue for every company. The code of ethics mandated by Sarbanes-Oxley specifically requires a company to promote the ethical handling of actual or apparent conflicts of interest between personal and professional relationships.[22] Common breeding grounds for conflicts of interest include employee relationships with the company's suppliers and outside employment.

The corporate opportunity doctrine forbids employees, officers, and directors of a company from:

(i) taking for themselves personally opportunities that are discovered through the use of corporate property, information, or position;
(ii) using corporate property, information, or position for personal gain; and
(iii) competing with the company.

The New York Stock Exchange (NYSE) has adopted rules requiring each issuer listed on the Exchange to adopt a code of conduct that addresses, separately, both conflicts of interest and corporate opportunities.[23]

Further, Sarbanes-Oxley, in order to strengthen protections against conflicts of interest, prohibits public companies from making personal loans to any director or executive officer.[24]

5. Bribes, kickbacks, improper payments, inappropriate gifts. Improper payments to government officials are a potential issue for many companies, especially if the government is a customer or if the business is subject to significant government regulation. Giving bribes or gratuities to U.S. government officials is prohibited by federal law,[25] and bribery of foreign government officials is prohibited by the Foreign Corrupt Practices Act.[26] Kickbacks are explicitly prohibited, both at the prime contractor and subcontractor levels, in connection with any federal government contract.[27] Kickbacks also are prohibited in exchange for the referral of business for which payment is made under federal healthcare programs, such as Medicare and Medicaid.[28] In addition, a number of states have criminal commercial bribery statutes that prohibit payments to influence the conduct of an agent or employee with respect to the affairs of the agent's employer.[29]

6. Antitrust issues. Antitrust issues such as price-fixing, collusive bidding, and market allocation are a concern in many industries.

7. Confidential information and trade secrets. For many companies, protection of confidential information and trade secrets is a significant issue. In the healthcare industry, protection of individual health information is critical. Often such information may be a key company asset and, under Sarbanes-Oxley, the safeguarding of company assets is one of the elements of internal control over financial reporting.[30] In order to protect its proprietary data and trade secrets, a company must take the requisite steps to preserve confidentiality. At a minimum, this includes reminding employees, during the course of their employment and upon their departure, of their continuing duty to safeguard such information. In addition, written confidentiality agreements may be desirable.

Further, companies must ensure that they do not become liable for misappropriating trade secrets belonging to their competitors or third parties. Employees should be warned against acquiring a competitor's confidential or trade secret information—and against bringing such information with them from a prior employer when they join the company.

8. Product safety. If the company manufactures or processes tangible products, especially consumer goods, then product safety may well be a key risk area. Indeed, in highly regulated industries that implicate public health and safety, such as food and drugs, product safety is likely to be the single most important risk issue. Where public health and safety are implicated, defective products may trigger strict criminal liability for the company as well as its senior managers.[31]

9. Workplace safety. In industries such as manufacturing, construction, or extraction of natural resources, workplace safety may be a significant issue.

10. Environmental issues. For many businesses, compliance with environmental laws is a significant concern. Some environmental statutes are drafted in such sweeping terms as to create something approaching strict criminal liability in the event of a violation.[32]

11. Government contracts issues. As detailed in chapter 14 on government contractors, mandatory compliance and ethics program requirements went into effect in 2008 for many government contractors and subcontractors. These requirements amend the Federal Acquisition Regulation (FAR) and are modeled to a large extent on the Federal Sentencing Guidelines criteria for effective compliance and ethics programs.[33] In addition to the specific elements of a compliance and ethics program that must be implemented, the FAR provisions also require mandatory reporting of violations of federal criminal law, violations of the civil False Claims Act, and "significant" overpayments.

Companies engaged in contracting with the federal government are especially vulnerable to liability for business misconduct. A number of statutes impose civil liability upon government contractors for engaging in fraudulent conduct or failing to comply with applicable

procurement and contracting rules.[34] Further, an array of criminal statutes may be applied to contractors who engage in fraud or other misconduct.[35]

The most common types of fraud encountered in government contracting include defective pricing, cost mischarging, product substitution, progress payment fraud, antitrust violations, kickbacks, bribery, gratuities, and conflicts of interest.[36]

12. Insider trading. Another risk for publicly held companies is that directors, officers, or employees may engage in insider trading in the company's shares. The NYSE considers this risk so significant that it identifies insider trading as one of the issues to be addressed by the code of conduct it requires for listed companies.[37]

13. International business practices. U.S. laws that may create significant risks for companies engaged in international business include export control laws and the Foreign Corrupt Practices Act (FCPA). Export control laws and regulations prohibit the export of certain commercial products, strategic goods, defense articles and their related technologies, and the furnishing of defense services, unless licensed by the appropriate federal agency—either the Department of Commerce or the Department of State.

Note that an "export" can occur anywhere when equipment or technical data is released or made available to a foreign person, whether within the United States or abroad.

The FCPA prohibits bribery in the conduct of business abroad. In general, the FCPA prohibits corrupt payments to foreign officials or political parties (whether made directly or through intermediaries) for the purpose of obtaining or keeping business.[38]

14. Employee relations. Discrimination and harassment issues are a concern for virtually all employers. Federal statutes and regulations forbid discrimination in the workplace based on race, color, sex, religion, national origin, marital status, age, or disability.[39] Discrimination or harassment can subject a company to civil liability for compensatory damages and, in cases involving malice or reckless indifference, to punitive damages as well.[40]

15. Other issues. There are a number of additional issues that are less common but very significant to particular businesses or industries. Certain highly regulated industries, such as banking and healthcare, face numerous compliance risks that derive from the specialized laws and regulations that govern their conduct. Other businesses, though not highly regulated, may have particular attributes that create significant compliance risks. For example, marketing organizations are vulnerable to charges of fraudulent sales techniques. Compliance programs must be designed to combat these risks.

16. Mergers and acquisitions. One distinct area of risk that companies may face is acquiring a problem through a merger or acquisition. This scenario happens often enough that the DOJ lists mergers and acquisitions (M&A) as a distinct topic in its discussion of how prosecutors should evaluate corporate compliance programs.[41] Addressing this M&A risk requires care both during the due diligence process and in integrating the acquired business into the company's existing compliance function. If the acquired business is a new line of business for the company, it may require the company to engage in a new risk assessment to ensure that it is guarding against any novel risks that it now faces.

Code of Conduct

Q 2.6 Is a code of conduct a required part of a compliance program?

A code of ethical conduct is a centerpiece of a compliance program. The Sentencing Guidelines and Sarbanes-Oxley now make a code of ethics virtually mandatory for all companies. Furthermore, both the NYSE and NASDAQ have rules that mandate that listed companies adopt codes of business conduct and ethics.[42]

Sarbanes-Oxley effectively requires every publicly traded corporation to adopt a code of ethics that applies to its principal executive officer, principal financial officer, principal accounting officer or controller, or persons performing similar functions.[43]

Q 2.6.1 What are the legal requirements for a code of conduct?

Sarbanes-Oxley mandates that the code consist of written standards that are reasonably designed to deter wrongdoing and to promote:

(1) honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
(2) full, fair, accurate, timely, and understandable disclosure in reports and documents that a registrant files with, or submits to, the SEC and in other public communications made by the registrant;
(3) compliance with applicable governmental laws, rules, and regulations;
(4) the prompt internal reporting of violations of the code to an appropriate person or persons identified in the code; and
(5) accountability for adherence to the code.[44]

The Sentencing Guidelines impose more general requirements for a code of conduct. They require that the company establish standards and procedures to prevent and detect criminal conduct, and take reasonable steps to communicate periodically and in a practical manner its standards and procedures to all employees and agents by conducting training programs and otherwise disseminating information.

Q 2.6.2 What are the elements of a good code of conduct?

A corporate code of ethical conduct should accomplish several distinct, but related, objectives:

1. *Address, in a direct, practical manner, the compliance risk issues that are relevant to the particular company.* The code should alert employees to the principal risks and spell out their duty to avoid them. Some of the most effective codes follow up their discussion of the relevant standards with sample questions and answers applying the standard(s) to common situations that employees are likely to encounter.

2. *Identify the personnel who administer the company's compliance program, from the senior executive(s) in charge of the program down through any lower-level contact personnel.* In addition, the code should

outline the system for reporting suspected misconduct. Employees and agents must be able to report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

Furthermore, it is desirable (and sometimes required) that the system permit confidential, anonymous reporting.[45] The code should state unequivocally that any employee may contact compliance personnel to discuss potential violations of the code without fear of retribution and, if applicable, that anonymous reporting is an option. The code should encourage employees to contact compliance personnel whenever an ethical issue arises and they are uncertain about whether or how the code applies.

3. *Announce that employees who violate code provisions will be sanctioned for their misconduct, indicating the range of sanctions that may be applied.* The sanctions may range from a reprimand for minor or unintentional violations up to termination for cause for serious violations. The Sentencing Guidelines note that disciplinary actions sometimes may need to be taken not only against the actual offender but also against individuals who fail to take reasonable steps to prevent or detect the misconduct.[46] Thus, the code should also state that an employee who witnesses a violation and fails to report it may be subject to discipline, as may a supervisor or manager to the extent that the violation reflects inadequate supervision or lack of diligence.

4. *Be distributed to all company employees and agents in writing and/or by making it available on the company's website.* Many companies require that employees certify that they have received and read the code of conduct. Some companies make this an annual ritual. Such certifications can provide useful evidence of the company's good faith and diligence if an issue ever arises. However, the certifications can end up undercutting the company's position if they are incomplete or out of date. Thus, if a company decides to utilize employee certifications, it must diligently monitor them to ensure that they are complete and up to date.

Q 2.6.3 How many codes of conduct should a company have?

Sarbanes-Oxley mandates a code of ethics only for a select group of senior corporate officials: a company's principal executive officer,

principal financial officer, principal accounting officer or controller, or persons performing similar functions. In contrast, the Sentencing Guidelines and the NYSE and NASDAQ rules require a code that is broadly applicable to a company's officers, employees, and (as appropriate) agents.

For most companies, it would seem simplest to have only one code of conduct that applies to all officers, employees, and agents, and that either applies the Sarbanes-Oxley standards to all such persons, or else "adds on" the specific Sarbanes-Oxley requirements for the specified senior officers who are subject to them. Multiple codes of conduct applicable to different groups of officers and/or employees are likely to breed problems for the company.

Compliance Program Administration

Q 2.7 How do we administer and enforce a compliance program?

1. Establish comprehensive written policies and procedures that implement the Code of Conduct and that address the specific risk areas you have identified.

2. Conduct effective training programs and otherwise disseminate information about the compliance program to officers and employees.

3. Establish and publicize a system for reporting violations.

4. Promptly and carefully investigate any reports of suspected misconduct and take corrective action if appropriate.

5. Provide feedback to employees who have reported suspected misconduct so that they know that you took their allegations seriously and that an appropriate resolution was reached. Employees who believe that you have ignored their complaints are far more likely to become "whistleblowers" initiating litigation against the company than are employees who believe that their complaints have been considered and addressed.

6. Document the complaints you receive and the steps that you take to resolve them. Although there is a risk that such documentation may later be discoverable by adverse parties, it is simply not an

option for the company to keep no records regarding the workings of its compliance program. Among other things, a failure to keep records would make it difficult or impossible to audit the workings of the program, which is a process required by Sarbanes-Oxley and the Sentencing Guidelines.

7. Actively check for misconduct and periodically evaluate the effectiveness of its compliance program.

> **TIP:** Be mindful that the results of an internal investigation can end up providing a roadmap of corporate misconduct to adverse parties such as the government, civil litigants, or disaffected shareholders. It may be wise to place an attorney in charge of investigating matters that appear to involve serious misconduct in order to secure the protections of the attorney-client privilege and attorney work-product doctrines insofar as possible. To the extent that the compliance program, or any aspect(s) thereof, is administered by non-legal personnel, such as the audit department or H.R., it is likely that the results of their work will be discoverable in subsequent proceedings.

In addition to investigating reports of suspected misconduct, the Sentencing Guidelines require a company to engage in proactive enforcement efforts by monitoring and auditing to detect criminal conduct.[47] Sarbanes-Oxley requires management to evaluate and disclose the effectiveness of the company's internal control over financial reporting by utilizing a recognized control framework such as the COSO Internal Control—Integrated Framework. The assessment of a company's internal control must be based on procedures sufficient both to evaluate its design and test its operating effectiveness.[48]

Q 2.7.1 Who should administer the compliance program?

The Sentencing Guidelines provide that the company must appoint senior managers who must have overall responsibility for the compliance program. Additionally, several different departments within

the company may have significant roles to play in administering the compliance program. These include the inside audit or accounting department, the security department, human resources, and the legal department. They probably already perform compliance functions in their respective areas. Their various compliance efforts must be coordinated as part of a single program and specific senior manager(s) must be responsible—and accountable—for overseeing compliance efforts.[49]

Q 2.7.2 Which senior executive(s) should be placed in charge of the compliance program?

For public companies, Sarbanes-Oxley makes the audit committee (and, by extension, the entire board of directors) directly responsible for ensuring that a company's internal control over financial reporting functions properly and that all requisite disclosures are made. Otherwise, there is no single, required approach for assigning responsibility for management of the compliance program. Many companies, especially smaller ones, will designate one compliance officer. Larger organizations often designate individual compliance officers by substantive areas and may utilize a compliance committee in lieu of a single compliance officer, or a combination of an individual compliance officer who is supported by a committee from different areas. Increasing the number of compliance officers presents problems of communication, possible inconsistency, and lack of accountability.[50]

Q 2.7.3 What role does top management have in administering a compliance program?

The Sentencing Guidelines require that the company's governing authority (board of directors, etc.) understand the content and operation of the compliance program and exercise reasonable oversight with respect to its implementation and effectiveness. At least annually, but more often if practicable, the board should receive an update as to the status and operation of the compliance program, including usage of reporting mechanisms, reports of wrongdoing, reports of disciplinary action, reports of new risk areas, and other pertinent information.

Specific senior manager(s) must be assigned overall responsibility to ensure the implementation and effectiveness of the program. The individuals delegated day-to-day operational responsibility shall be

given adequate resources and authority. Moreover, they shall report periodically to senior management and shall have direct access to the board of directors.[51]

Sarbanes-Oxley places responsibility for the creation and operation of a company's compliance program on both senior management and the audit committee of the board of directors, which it requires to be comprised of outside, independent directors.[52] The audit committee must establish procedures for (1) the receipt, retention, and treatment of complaints about accounting, internal accounting controls, or auditing matters, and (2) the confidential, anonymous submission by employee of concerns regarding questionable accounting or auditing matters.[53]

Sarbanes-Oxley imposes compliance responsibilities on senior corporate officials by requiring the principal executive officer and the principal financial officer, or persons performing similar functions, to make a series of certifications in each annual and quarterly report filed with the SEC. Each of these officers must certify that:

(1) he/she has reviewed the report;
(2) based on his/her knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact;
(3) based on his/her knowledge, the financial information in the report fairly presents in all material respects the financial condition, results of operations, and cash flows of the company;
(4) he/she and the company's other certifying officials are responsible for establishing and maintaining the company's disclosure controls and internal control over financial reporting;
(5) the disclosure controls and procedures have been designed to ensure that material information relating to the company and its consolidated subsidiaries is made known to the certifying officials by others in the company;
(6) the internal control over financial reporting has been designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
(7) he/she and the company's other certifying officials have evaluated the effectiveness of the disclosure controls and procedures and presented in this report their conclusions about

their effectiveness as of the end of the period covered by the report;

(8) he/she and the company's other certifying officials have disclosed in the report any change in the company's internal control over financial reporting that occurred during the most recent fiscal quarter that has materially affected or is reasonably likely to materially affect the company's internal control over financial reporting; and

(9) he/she and the company's other certifying officials have disclosed to the company's outside auditors and the audit committee of the board of directors

  (a) all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting that are reasonably likely to adversely affect the company's ability to record, process, summarize, and report financial information; and

  (b) any fraud, whether or not material, that involves management or other employees who have a significant role in the company's internal control over financial reporting.[54]

The overriding need to protect the investing public drives the Sarbanes-Oxley requirement for disclosure of any material weaknesses in the company's internal control over financial reporting or in its disclosure controls and procedures.

Q 2.7.4 What is meant by a "culture" of compliance?

Government enforcement authorities look to determine if there is executive "buy-in" regarding compliance programs and expect company officers to set the tone. As one SEC official stated,

> We're trying to get the fundamentally honest, decent CEO or CFO or General Counsel—the one who wouldn't break the law—to say to herself when she wakes up in the morning: "I'm going to spend part of my day today worrying about, and doing something about, the culture of my company."[55]

This is what is meant by a "culture" of ethics and compliance, and of the top setting the tone. Chapter 3 also offers an in-depth discussion of assessing and managing an ethical culture.

Q 2.7.5 How can we demonstrate a culture of ethics and compliance?

When the DOJ evaluates a compliance program, it asks whether and how senior leaders, through their words and actions, have discouraged misconduct, and what concrete actions they have taken to lead compliance efforts. It asks whether the board of directors (or external auditors if there is no board) has held private sessions with the individuals in charge of the company's compliance and control functions. It asks how the compliance function compares with other functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision makers. It asks whether compliance and control personnel have the appropriate experience and qualifications. And it asks whether compliance personnel have independence to conduct their investigations and report their findings.[56]

Thus, in order to demonstrate a culture of compliance and ethics, a company should:

- ensure that top management is invested in compliance and demonstrates this on a regular basis;
- ensure that the head of compliance reports (on either a straight line or dotted line basis) to the board of directors and/or its audit committee, and meets with them regularly;
- ensure that the board of directors receives periodic compliance program reports;
- ensure that compliance and control personnel have the appropriate qualifications and experience, and receive the necessary resources;
- ensure that compliance personnel have appropriate stature within the company; and
- ensure, if possible, that the chief compliance officer does not have managerial responsibilities apart from the compliance function (this may not be feasible in small companies).

Q 2.7.6 What are reasonable efforts to exclude bad actors?

There is no sure-fire way to root out each and every employee who possibly could act improperly. Companies are, however, expected to make *reasonable* efforts not to hire or retain as managers or other

higher-level employees any individuals who have engaged in illegal or unethical conduct.

TIP: Background Checks and Other Due Diligence

Potential employers should check lists of "excluded persons" within their particular industry.

For example, healthcare companies should check their employees against the Department of Health and Human Services Office of Inspector General List of Excluded Individuals/Entities, https://exclusions.oig.hhs.gov. Government contractors should utilize the General Services Administration's Excluded Parties List System (EPLS), accessible via www.sam.gov.

Training

Q 2.8 What is required in the way of training and communication?

Training should be provided upon hiring or transfer of an existing employee to a new position. Training should be provided at least annually thereafter, but more often if the circumstances dictate. Training can be provided using any number of means. It can be in-person, computer-/Internet-based, lecture-style, or by any other method that is appropriate to the content and reasonably calculated to provide a meaningful training experience.

It should never be forgotten that Enron seemed on the surface to have a compliance program, including a code of conduct. As it turned out, however, all Enron had was a "paper" program, and nothing of substance. In the words of Enron whistleblower Sharon Watkins, "It's not just a snappy little code of conduct or code of ethics that makes sure things are done right."[57] Instead, a company must ensure that *all* employees receive training on the code and policies that are relevant and applicable to their particular jobs within the company.

Good training is the cornerstone of an effective compliance and ethics program. A company can have the best-drafted code of conduct and the most thorough ethics policies money can buy, but if the company's employees are not trained on them, they are worthless paper.

Q 2.8.1 Who within our organization needs to be trained?

The Sentencing Guidelines state that, for an effective compliance and ethics program, the following individuals must receive training:

- members of the company's governing authority (for example, board of directors);
- high-level personnel;
- substantial authority personnel;
- employees; and
- agents, as appropriate.

Q 2.8.2 Do we need to educate every employee about every policy?

No; that would be a waste of the company's resources. A front-line cashier of a nationwide retailer does not need to be trained on the company's import/export controls policy. Instead, the company should determine which categories of employees (for example, sales, human resources, management) need training on the company's various policies. In particular, the company should identify high-risk and control employees and provide tailored training to them. Key gatekeepers (for example, the persons who issue payments or review approvals) in the control processes should receive training relevant to their roles.

Q 2.8.3 We hold a training session for new employees. Is a thorough, one-time training session on our code and policies enough?

No. The Sentencing Guidelines require *periodic* communication of the company's written standards and procedures. A company that trains its employees only during an orientation program does not have an effective compliance program. As time goes by, laws and regulations affecting a company will change, sometimes dramatically, and the company's written standards and policies must change accordingly.

Even if the applicable law or the company's policies have not changed, periodic retraining is valuable. And it is required.

Audits

Q 2.9 How can my company maintain the compliance program's effectiveness?

Conducting regular, periodic audits and monitoring of its program are effective means for a company to determine whether its compliance program is actually being followed. The audit can be done internally under the direction and supervision of the compliance officer, or it can be done externally. If an external audit is performed, it should be performed by outside counsel, due to the protections of the attorney-client privilege. The audit should be performed by evaluators with expertise in the relevant federal and state laws and regulations that affect the company's business.

In addition, a company's monitoring procedures should include a reporting system, discussed in greater detail below. Additionally, the company should conduct an investigation any time potential wrongdoing is revealed through the company policy.

Q 2.9.1 What should an audit of the program be examining?

The audit should be the company's method of determining whether the company does indeed have all of the elements of an effective compliance and ethics program in place. The following is just a sampling of the questions that auditors should be asking in an evaluation of the program:

- ❒ Does the company have in place all of the standards and procedures that are necessary, given the applicable legal and regulatory framework?
- ❒ Has the company appropriately distributed those written standards and procedures, including its code of conduct?
- ❒ Has the company provided ongoing training programs to educate its employees, officers, and (where appropriate) agents and contractors?

- ❒ Has the company devoted adequate resources to the operations of its compliance program, and does the compliance officer have sufficient authority within the organization?
- ❒ Are employees actually following the company program?
- ❒ Have there been any internal investigations of alleged noncompliance with the program? If so, what were the results?
- ❒ If internal investigations have taken place, were the proper procedures for investigations followed?
- ❒ Were remedial actions taken upon discovery of wrongdoing?

Q 2.9.2 What is internal auditing?[58]

The Institute of Internal Auditors has developed the globally accepted definition of internal auditing:

> Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objective by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance process.

Independence is established by the organizational and reporting structure while objectivity is achieved by an appropriate mind-set. The internal audit activity evaluates risk exposures relating to the organization's governance, operations, and information systems for: effectiveness and efficiency of operations; reliability and integrity of financial and operational information; safeguarding of assets; and compliance with laws, regulations, and other legal documents.

Q 2.9.3 Why should an organization have internal auditing?[59]

A cornerstone of strong governance, internal auditing bridges the gap between management and the board, assesses the ethical climate and the effectiveness and efficiency of operations, and serves as an organization's safety net for compliance with rules, regulations, and overall best business practices.

Management is responsible for establishing and maintaining a system of internal controls within an organization. Internal controls are

those structures, activities, processes, and systems which help management effectively mitigate the risks to an organization's achievement of objectives. Management is charged with this responsibility on behalf of the organization's stakeholders and is held accountable for this responsibility by an oversight body (for example, board of directors, audit committee, elected representatives).

Q 2.9.4 What is internal auditing's role in preventing, detecting, and investigating fraud?[60]

Internal auditors support management's efforts to establish a culture that embraces ethics, honesty, and integrity. They assist management with the evaluation of internal controls used to detect or mitigate fraud, devalue the organization's assessment of fraud risk, and are involved in any fraud investigations.

Although it is management's responsibility to design internal controls to prevent, detect, and mitigate fraud, the internal auditors are an appropriate resource for assessing the effectiveness of the internal control structure that management has implemented.

Q 2.9.5 What is the appropriate relationship between the internal audit activity and the audit committee of the board of directors?[61]

The audit committee of the board of directors and the internal auditors are interdependent and should be mutually accessible, with the internal auditors providing objective opinions, information, support, and education to the audit committee; and the audit committee providing validation and oversight to the internal auditors.

Reporting Systems/Whistleblowing/Non-Retaliation

Q 2.10 What type of reporting system does my company need to have?

The Sentencing Guidelines require a reporting system that allows employees (1) to report ethical or legal concerns or (2) to seek guidance on particular ethical or legal matters. To achieve these goals, companies typically use a hotline. However, the reporting system a company chooses should be tailored to the size and geographical range of the

company. A smaller company may decide to set up an internal telephone extension as its hotline, or—better yet—may use a toll-free number that allows callers to leave a voicemail message. A larger, geographically diverse company should at the very least have a toll-free number. Companies may also choose to set up an email account for the reporting of potential violations or seeking guidance.

Some external vendors can manage the reporting system, setting up internal and external websites that allow for anonymous reporting but also allow employees to check back in with the system to determine whether their reports are being investigated by the company. This type of two-way communication can provide employees with confidence that their concerns are being taken seriously by the company, and thus tends to cultivate company loyalty.

Although reporting systems may vary depending on the company, there are some across-the-board requirements. The system must:

- allow for anonymous and/or confidential reporting;
- be accompanied by a non-retaliation policy.

In order for a hotline to be effective, employees must have confidence that confidentiality and anonymity will be respected.

Q 2.10.1 What is a non-retaliation policy?

A non-retaliation policy should explain that a company will not retaliate against any employee who, in good faith, reports a potential violation. All employees should be made aware that any attempt at retaliation against an employee who uses the reporting system or engages in any kind of whistleblowing in good faith will result in immediate disciplinary action. A company should also instruct employees to contact the compliance officer immediately if they feel they are being retaliated against.

A non-retaliation policy is critical if your reporting system is to be more than "just for show." Without such a policy, employees and others will not feel secure reporting potential problems internally. In addition, they will not feel comfortable seeking guidance on some of the complex laws and regulations that govern many businesses and will, therefore, be less likely to prevent problems.

Rewards/Discipline

Q 2.11 How can my company effectively enforce the compliance program?

With both discipline and positive reinforcement. Companies should make compliance and ethics an integral part of employee evaluations. The promotions process should also take into account an employee's commitment to compliance. For example, has the employee been cooperative when asked to answer questions as part of an internal investigation? Has the employee brought ethical concerns to the attention of his or her supervisor, in an effort to ensure that the company's operations were aboveboard?

Conversely, companies need to dispense punishment as necessary and appropriate where employees have broken the law, have violated the company's written standards and procedures, or have otherwise acted counter to the goals of the compliance and ethics program. Companies will need to administer disciplinary actions that are suitable for given violations (for example, suspensions without pay or termination).

When the DOJ evaluates a compliance program, it pays particular attention to the issue of accountability. It asks whether and how the wrongdoer was dealt with. It also asks whether managers were held accountable for misconduct that occurred under their supervision. It asks about the company's overall record on employee discipline (or discipline relating to the type of conduct at issue), including the number and types of disciplinary actions. It asks whether the company has ever terminated or otherwise disciplined anyone for the same or similar misconduct. And it asks whether disciplinary actions have been fairly and consistently applied across the organization.[62]

Q 2.11.1 Despite our best efforts to promote a culture of honesty and integrity, some criminal or unethical conduct has occurred. How should the company respond?

Promptly discipline individuals who engage in criminal or unethical conduct.

Second, consider whether the company should take steps to remedy any harm that was done, such as making restitution.

Third, take steps to prevent further similar conduct—for example, by reviewing your compliance and ethics program to determine where the weak links are (Was there enough training conducted on certain policies? Were there gaps in your company's compliance auditing process?), and by modifying the program accordingly.

Fourth, depending on the industry involved and the nature and severity of the misconduct, self-disclosure to regulatory or law enforcement authorities may be prudent or required. For example, government contractors and subcontractors must make written disclosure to the government whenever they have credible evidence of a violation of federal criminal law or a violation of the civil False Claims Act.[63]

Notes to Chapter 2

1. United States v. Booker, 543 U.S. 220 (2005).
2. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1.
3. *Id.* § 8C2.5(f)(1).
4. *Id.* § 8B2.1.
5. *In re* Caremark Int'l, Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996); Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 368–70 (Del. 2006).
6. U.S. DEP'T OF JUSTICE, CRIMINAL DIVISION, FRAUD SECTION, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, www.justice.gov/criminal-fraud/page/file/937501/download (last visited July 6, 2017).
7. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(a).
8. *Id.* § 8B2.1(b).
9. *Id.* § 8B2.1 cmt. (n.7).
10. *Id.* § 8B2.1 cmt. (n.2).
11. EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 6, at 4–5.
12. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. (n.2(B)).
13. *Id.* § 8B2.1 cmt. (n.2(C)(iii)).
14. Pub. L. No. 107-204 (Sarbanes-Oxley), 116 Stat. 745 (codified in scattered sections of titles 11, 15, 18, 28, and 29 U.S.C.).
15. Certification of Disclosure in Companies' Quarterly and Annual Reports, Securities Act Release No. 8124 (Aug. 30, 2002), www.sec.gov/rules/final/33-8124.htm.
16. *See* 31 U.S.C. § 5312(a)(2) and (c)(1).
17. 31 U.S.C. § 5318(h)(1).
18. *Id.* § 5318(*l*).
19. 12 C.F.R. § 21.11; 31 C.F.R. §§ 103.18, 103.19, 103.20, 103.21.
20. 31 C.F.R. §§ 103.22, 103.30.
21. *See Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. DEP'T OF TREASURY (June 29, 2017) (providing links to downloadable lists), www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.
22. Sarbanes-Oxley § 406, 15 U.S.C. § 7264.
23. NYSE MANUAL § 303A.10 (Code of Business Conduct and Ethics), http://nysemanual.nyse.com/lcm/Help/mapContent.asp?sec=lcm-sections&title=sx-ruling-nyse-policymanual_303A.10&id=chp_1_4_3_11.
24. Sarbanes-Oxley § 402, 15 U.S.C. § 78m(k).
25. *See* 18 U.S.C. § 201.
26. 15 U.S.C. §§ 78a, 78m, 78dd-1, 78dd-2, 78ff.

27. 41 U.S.C. § 51 *et seq.*

28. 42 U.S.C. § 1320a-7b(b).

29. *See* United States v. Parise, 159 F.3d 790, 804 & n.1 (3d Cir. 1998) (Garth, J., dissenting) (collecting state commercial bribery statutes).

30. *See* 68 Fed. Reg. 36,636, 36,640 (2003).

31. *See* United States v. Park, 421 U.S. 658 (1975); United States v. Dotterweich, 320 U.S. 277 (1943); United States v. Cattle King Packing Co., 793 F.2d 232, 240 (10th Cir.), *cert. denied*, 479 U.S. 985 (1986).

32. *See, e.g.*, United States v. Weitzenhoff, 1 F.3d 1523, 1529 (9th Cir.), *reh'g denied and amended*, 35 F.3d 1275 (9th Cir. 1993) (construing criminal provision of the Clean Water Act).

33. *See* FAR subpt. 3.10, [48 C.F.R.] §§ 9.406-2, 9.407-2, 52.203-13, 52.203-14; 73 Fed. Reg. 67,064, FAR Case 2007-006, Contractor Business Ethics Compliance Program and Disclosure Requirements (Nov. 12, 2008).

34. *E.g.*, False Claims Act, 31 U.S.C. § 3729; claim forfeiture statute, 28 U.S.C. § 2514; Anti-Kickback Statute, 41 U.S.C. § 51 *et seq.*; Procurement Integrity Act, 41 U.S.C. § 423; Contract Disputes Act, 41 U.S.C. § 601 *et seq.*; Truth in Negotiations Act, 10 U.S.C. § 2306a.

35. *E.g.*, 18 U.S.C. § 1001 (false statements); 18 U.S.C. § 287 (false claims); 18 U.S.C. § 371 (conspiracy to defraud the United States); 18 U.S.C. § 1031 (major fraud against the United States).

36. *See* DEP'T OF DEFENSE, HANDBOOK ON FRAUD INDICATORS FOR CONTRACT AUDITORS, IGDH 7600.3 (Mar. 31, 1993), www.dodig.mil/resources/policyreferences/Audit/igdh7600.pdf; Inspector General, Dep't of Defense Pub. No. IG/DOD 4075.1-H (1987).

37. NYSE MANUAL § 303A.10 (Code of Business Conduct and Ethics), *supra* note 23.

38. 15 U.S.C. § 78dd-1.

39. *See* Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e; Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12101–213.

40. Civil Rights Act of 1991, 42 U.S.C. § 1981.

41. EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 6, at 7.

42. NYSE MANUAL § 303A.10 (Code of Business Conduct and Ethics), *supra* note 23; NASDAQ Rule 5610.

43. Sarbanes-Oxley § 406, 15 U.S.C. § 7264; 17 C.F.R. §§ 228.406, 229.406. If the company does not adopt a code of ethics, it must explain why not. *Id.*

44. 17 C.F.R. §§ 228.406, 229.406.

45. *See* Sarbanes-Oxley § 301, 15 U.S.C. § 78f(m)(4).

46. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(6).

47. *Id.* § 8B2.1(b)(5).

48. 68 Fed. Reg. 36,636, 36,642–43 (2003).

49. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2).

50. *See* JEFFREY M. KAPLAN, JOSEPH E. MURPHY & WINTHROP M. SWENSON, COMPLIANCE PROGRAMS AND THE CORPORATE SENTENCING GUIDELINES § 8.11 (1995).

51. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(2).
52. Sarbanes-Oxley § 301, 15 U.S.C. § 78f(m)(3)(A).
53. Sarbanes-Oxley § 301, 15 U.S.C. § 78f(m)(4).
54. Sarbanes-Oxley § 302, 15 U.S.C. § 7241; 17 C.F.R. § 229.601(a)(31).
55. Stephen M. Cutler, Dir., SEC Enf't Div., Speech at Second Annual General Counsel Roundtable, Tone at the Top: Getting It Right (Dec. 3, 2004), www.sec.gov/news/speech/spch120304smc.htm.
56. EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 6, at 2–3.
57. Andrew Countryman, *Enron Whistleblower Spreads Around Blame*, CHI. TRIB., Jan. 15, 2003.
58. This question-and-answer is based on information from the Institute of Internal Auditors, Altamonte Springs, Florida, and has been reprinted with permission from their website FAQs. *See* www.theiia.org.
59. *Id.*
60. *Id.*
61. *Id.*
62. EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 6, at 6.
63. *See* FAR [48 C.F.R.] §§ 9.406-2, 9.407-2, 52.203-13(b)(3)(i).