Case Study 2
Auditing the Compliance and Ethics Program

LEARNING OBJECTIVES

- Understand the concept of compliance and its relationship to a healthy ethical culture.
- Describe the legal and regulatory reasons for maintaining an effective compliance and ethics program.
- Identify the board’s and management’s responsibilities for the organization’s compliance and ethics program.
- Determine the benefits of taking an integrated systems approach to establishing and maintaining a compliance and ethics program.
- Describe the essential elements of an effective compliance and ethics program.
- Understand how to develop and communicate compliance standards and procedures.
- Understand the roles of monitoring and auditing a compliance and ethics program and how to develop appropriate monitoring and internal audit plans.
- Describe the different roles and responsibilities the compliance, internal audit, legal, and human resources functions have in the compliance and ethics program.
- Understand how compliance and ethics programs evolve and mature and how the internal audit function can add value by assessing the compliance and ethics program’s stage of maturity.

Chapter 3, “Governance,” and chapter 6, “Internal Control,” present the broad types of objectives that are critical to the overall governance, risk management, and control of every organization within the operations, reporting, and compliance COSO objective categories. While internal auditors have long been auditing compliance, it has not traditionally been considered one of the more glamorous aspects of internal auditing.

The significant consequences of the many recent failures of organizations to abide by laws and regulations and to exhibit ethical behavior have raised societal awareness of the cost of organizational corruption and increased expectations that organizations be held accountable. Because organizations have become so
large, far reaching, and interconnected, the damage that can be caused by organizational misconduct is massive and addressing compliance issues through traditional, after-the-fact law enforcement is no longer feasible. Regulators, boards, and senior executives are increasingly taking proactive measures to decrease the likelihood of misconduct and reduce the magnitude of its consequences. They also are demanding stronger assurance regarding organizational compliance and are increasingly asking internal auditors to provide such assurance. In response, the internal audit profession is rapidly developing new compliance audit approaches. Compliance auditing is quickly evolving into a much more interesting part of internal audit practice than it has been in the past.

WHAT IS COMPLIANCE?

The term “compliance” is defined in the Glossary to The IIA’s International Standards for the Professional Practice of Internal Auditing as “Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.” However, this definition captures only the narrow sense of what compliance means today. In its broadest sense, “compliance” refers to the organization’s compliance and ethics program. Such a program can be characterized as follows:

It is a system of individuals, processes, and policies and procedures developed to ensure compliance with all applicable federal and state laws, industry regulations, and private contracts governing the actions of the organization. A compliance program is not merely a piece of paper or binder on a shelf; it is not a quick fix to the latest hot problem; it is not a collection of hollow words. A compliance program—an effective compliance program—must be a living, ongoing process that is part of the fabric of the organization. A compliance program must be a commitment to an ethical way of conducting business and a system for helping individuals to do the right thing.¹

This broader concept of compliance involves a number of processes such as risk management, policy and procedure development, training, implementation of prevention and detection controls, monitoring, enforcement, and assurance. The above description also reflects a widening view that compliance is intermingled inherently with ethics—that compliance means more than simply meeting the minimal legal requirements—it also means enabling people in the organization to do the “right thing.” While not all organizations agree with this perspective, the trend in recent years has been to blend the two, especially as it becomes increasingly apparent that compliance programs cannot be effective unless they operate in a healthy ethical culture. In recognition of this trend, we use the term “compliance and ethics program” throughout the remainder of this case study.

TAKING AN INTEGRATED SYSTEMS APPROACH TO ESTABLISHING AND MAINTAINING A COMPLIANCE AND ETHICS PROGRAM

Today’s organizations face an increasingly complex legal and regulatory environment. A number of factors contribute to this complexity, the most significant being:

- Technological advancements that increase the speed of communications and expand the number of individuals an organization touches.
- Globalization that allows even small organizations to operate in multiple countries and jurisdictions.
- Increased interdependency of organizations through outsourcing, alliances, and extended supply chains.
Increased demand for accountability because of numerous high-profile scandals and failures.

Organizations must now address an array of compliance requirements, including antitrust, environmental, health and safety, anti-bribery, privacy, and money laundering.

Due to the nature of their operations, the history of significant, widespread compliance failures, and legal and regulatory environments, some industries have had to focus much more on compliance than others. Government contracting and health care are two industries in which organizations have had to develop increasingly sophisticated and pervasive programs to manage compliance risk. Exhibit CS 2-1 presents typical compliance risks for defense contractors that span the organization, including sales and marketing, billing and accounting, human resources, quality control, and environmental, health, and safety risks. The chemical and oil industries are two other industries facing significant, although more focused, compliance requirements pertaining to environmental, health, and safety risks.

### EXHIBIT CS 2-1
**TYPICAL COMPLIANCE RISKS FOR DEFENSE CONTRACTORS**

<table>
<thead>
<tr>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providing business courtesies which may be perceived as excessive.</td>
</tr>
<tr>
<td>Personal and organizational conflicts of interest.</td>
</tr>
<tr>
<td>Time charging and expense reporting.</td>
</tr>
<tr>
<td>Use of company property, equipment, and facilities.</td>
</tr>
<tr>
<td>Use of copyrighted or licensed materials.</td>
</tr>
<tr>
<td>Accurate representation in proposals of data or credentials and employee qualifications.</td>
</tr>
<tr>
<td>Proper recording and disbursement of funds and other assets.</td>
</tr>
<tr>
<td>Prohibitions on customer and competitor proprietary data/source selection information.</td>
</tr>
<tr>
<td>Quality assurance.</td>
</tr>
<tr>
<td>Prohibiting kickbacks from suppliers and subcontractors.</td>
</tr>
<tr>
<td>Relationships with customers and suppliers.</td>
</tr>
<tr>
<td>Engagement and control of agents, including consultants and sales representatives.</td>
</tr>
<tr>
<td>Lobbying and political contributions.</td>
</tr>
<tr>
<td>Reporting adverse personnel information.</td>
</tr>
<tr>
<td>Drug and substance abuse.</td>
</tr>
<tr>
<td>Equal opportunity employment.</td>
</tr>
<tr>
<td>Sexual harassment.</td>
</tr>
<tr>
<td>Inventions/patents policy.</td>
</tr>
<tr>
<td>Government audits and investigations.</td>
</tr>
<tr>
<td>Control of technology transfer to foreign persons.</td>
</tr>
<tr>
<td>Hiring former government employees and other “revolving door” issues.</td>
</tr>
<tr>
<td>Restrictions on duty assignments to former government employees.</td>
</tr>
<tr>
<td>Misconduct in science.</td>
</tr>
<tr>
<td>Computer system usage and internet use.</td>
</tr>
<tr>
<td>Money laundering.</td>
</tr>
<tr>
<td>Protecting government property.</td>
</tr>
<tr>
<td>Insider trading.</td>
</tr>
<tr>
<td>Security and crisis management.</td>
</tr>
</tbody>
</table>


The approach traditionally taken by organizations was to address significant compliance issues individually as they arose, assigning responsibility to the functional areas of the organization in which they originated or to the legal function. Organizations created numerous compliance “silos,” each with its own processes and reporting structures. One might find, for example, the vice president of operations overseeing the environmental compliance process, the general counsel having responsibility for the antitrust process, the
director of human resources managing the equal employment opportunity (EEO) office, the chief information officer (CIO) overseeing computer security and privacy reporting, and the chief audit executive (CAE) having responsibility for the anti-bribery process. As the compliance demands increase, the “silo” approach becomes unwieldy, with duplication of effort and resources and an ineffective reporting structure.

The United States defense industry was among the first to develop a more integrated approach to compliance. Defense spending accelerated rapidly in the early 1980s, and the numerous reports of waste, fraud, and abuse generated a public outcry for reform. In 1986, the industry established the Defense Industry Initiative on Business Ethics and Conduct (DII), a consortium of 32 leading defense contractors. The purpose of the DII was to combine the common dedication of its members to establish a culture and practice of ethics and right conduct in all business with the U.S. Defense Department and others. As part of the initiative, members agreed to adopt a set of fundamental principles that included the establishment of a written code of ethics, training employees on the code, establishing a system for internal reporting of code violations, implementing controls to monitor compliance, sharing best practices, and having an outside board member review compliance. This consortium now has more than 75 member organizations.

Also in 1986, the industry, in conjunction with the U.S. Department of Defense, undertook an initiative to improve contractor self-governance. This initiative sought to help defense contractors improve their compliance and ethics programs by implementing broad and effective systems of internal controls and having internal audit functions monitor compliance with government contracting procedures, corporate standards of conduct, and other requirements. The internal audit function was charged with evaluating actual compliance as well as the effectiveness of compliance systems of internal controls. The initiative also included the strengthening of the internal audit function, with more resources, better training on compliance requirements, and direct access to audit committees.

While the activity in the United States defense industry laid the groundwork for an integrated systems approach to compliance, it was the issuance of the Federal Sentencing Guidelines for Organizations (“Guidelines” or “Guidelines for Organizations”) in 1991 that established the structure for today’s concept of a “compliance system.” These Guidelines for Organizations augmented the 1987 Federal Sentencing Guidelines, which addressed individual offenders. The 1987 guidelines were issued in response to criticism that judges had too much discretion in determining punishment and that the disparity between punishments for “white-collar” crime and other types of crimes was too great. The 1987 guidelines (for individuals) set minimum and maximum punishments (fines and jail time) for every felony offense. The Guidelines for Organizations (chapter 8 of the Federal Sentencing Guidelines) applied the same logic to organizations setting boundaries on fines, probation (which can include a monitor), forfeiture of assets, and, in extreme cases, an “organizational death penalty” under which an organization agrees to divest all its assets. This represented a significant change in the United States’ legal and regulatory environment. Prior to the issuance of the Guidelines for Organizations, fines for corporations and other organizations were minimal. From 1984 to 1988, the average fine for sentenced corporations was less than $156,000, with 50% of all fines being less than $10,000. Court-imposed restitution requirements also were limited with the average amount of restitution paid being less than $50,000 and no restitution requirements imposed in 80% of the cases. Under the new guidelines, fines alone may total in the hundreds of millions of dollars, giving organizations and their governing bodies a stronger incentive to be concerned with compliance. An organization may now incur a significant cost for the misconduct of its employees.

One explicit purpose of the Guidelines for Organizations is to provide incentives for organizations to manage ethical misconduct and illegal behavior. While fines and probation provided negative incentives, the Guidelines also offered positive incentives in the form of reduction of fines and probation if the
organization cooperated with an investigation, self-reported violations, or had an effective compliance and ethics program in place. The benefits of an effective compliance and ethics program depend on several factors, including the level of culpability. Having an effective program can reduce fines from 30% to 91% and remove the requirement that the organization be placed on probation.7

But what is an effective compliance and ethics program? Seven minimal elements of an effective compliance and ethics program were presented in a somewhat obscure footnote in the original 1991 version of the Guidelines (commentary note 3(k) to section 8A 1.2), making this one of history's most significant footnotes. These seven elements, which are discussed below, became the basis for compliance and ethics programs worldwide. In acknowledging its importance, the Sentencing Commission expanded the note and moved its contents to a separate section of the Guidelines, Section 8B 2 – Effective Compliance and Ethics Program, in its 2004 revision.

THE FEDERAL SENTENCING GUIDELINES AND THE CRITERIA FOR AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM

The purpose of the criteria presented in the Guidelines is to guide the court in determining whether an organization's compliance and ethics program merits a reduction in fines or probation when sentencing the organization for offenses covered by section 8. However, the impact of the criteria extends well beyond judicial sentencing. The criteria have become the foundation for many organizational compliance and ethics programs, both in the United States and throughout the world. In effect, the criteria have become a set of "generally accepted compliance principles."

The text of the Guidelines pertaining to compliance and ethics program effectiveness is presented in exhibit CS 2-2. The Guidelines state that an organization should "strive to 1) exercise due diligence to prevent and detect criminal conduct and 2) promote an organizational culture that encourages ethical conduct and commitment to compliance with the law."8 The Guidelines then present seven fundamental elements that a program must have in place to minimally meet these two goals:

1. Standards and procedures.
2. Assignment of oversight and specific responsibilities for compliance and ethics.
3. Efforts to avoid assigning substantial authority to individuals with a history of noncompliance.
4. Education and training on compliance standards and procedures.
5. Monitoring and auditing to detect noncompliance and to evaluate effectiveness of the program.
6. Performance incentives and disciplinary actions.
7. Response to criminal conduct and remediation.
EXHIBIT CS 2-2
ELEMENTS OF AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM
SECTION 8B2.1 OF THE U.S. FEDERAL SENTENCING GUIDELINES

8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of ...[determining fines and recommending conditions of probation], an organization shall—

(i) exercise due diligence to prevent and detect criminal conduct; and

(ii) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) [the paragraph above] minimally require the following:

(i) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(ii) (A) The organization’s governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

(iii) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(iv) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals’ respective roles and responsibilities.

(B) The individuals referred to in subdivision (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization’s employees, and, as appropriate, the organization’s agents.
(5) The organization shall take reasonable steps—

(A) to ensure that the organization’s compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization’s compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization’s employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization’s compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization’s compliance and ethics program.

(c) In implementing subsection (b) [the seven elements], the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) [the seven elements] to reduce the risk of criminal conduct identified through this process.


Organizations also must implement an organizationwide periodic risk assessment and management process designed to reduce the risk of occurrence of criminal conduct to an acceptable level.

**Standards and procedures**. The first essential element of a compliance and ethics program is standards and procedures that establish expectations regarding compliance and ethics. One basic method is the development of a code of ethics (frequently referred to as a code of conduct), which clearly states the organization’s core values and sets expectations regarding appropriate behavior. The code should be understandable to all personnel; it should be written clearly and translated into all appropriate languages. Moreover, the code should be more than just a sheet of paper that employees get the day they join the organization and then stick in a desk drawer never to be thought of again; the values and expectations expressed in the code should be embedded in day-to-day operations. The code should be readily accessible to all who interact with the organization, such as customers and suppliers, potential investors, and other stakeholders.

The content of the code of ethics will depend on the organization’s values and its legal and regulatory environment. Elements of a typical code of ethics are presented in exhibit CS 2-3. Regardless of its other content, a good code of ethics outlines the protocol for seeking assistance in determining the right thing to do and how to report actual or suspected violations of the code.
The organization will also need written policies and procedures specific to the people involved in particular processes. For example, there may need to be specific policies and procedures for sales personnel or for personnel with access to sensitive data. These policies and procedures should be readily accessible to whom they apply, be clear and non-conflicting, and be kept current for changes in the laws and regulations affecting the organization or for other changes in the organization's external or internal environments.

Assignment of oversight and specific responsibilities for compliance and ethics. Ultimately, compliance and ethics are the responsibility of all employees in an organization. However, specific responsibility must be assigned for directing and overseeing the compliance and ethics program. The organization’s governing body (usually the board of directors) must provide a reasonable level of oversight of the compliance and ethics program. This oversight responsibility may be assigned to a particular subcommittee of the board, such as the compliance committee or the audit committee. To exercise its oversight role effectively, the board or its subcommittee must have a sufficient understanding of the organization’s compliance and
ethics program. For example, they must understand the program's scope and structure, its objectives and risk assessment process, the reporting process, and the adequacy of the resources devoted to the program. This oversight responsibility also includes obtaining assurance on the effectiveness of the program.

In the United States, the courts are increasingly holding corporate directors responsible for exercising reasonable oversight. In the 1996 Caremark case (In re Caremark International Inc. Derivative Litigation, 698 A.2d 959, Del. Ch. 1996), the court held that a director has a duty to attempt, in good faith, to determine that:

1. A corporate information and reporting system exists, and
2. This reporting system is adequate to assure the board that appropriate information as to compliance with applicable laws will come to its attention in a timely manner as a matter of ordinary operations.9

In essence, it is the responsibility of the board, together with senior management, to ensure that the corporation has a functionally effective compliance and ethics program in place.

Overall day-to-day responsibility for making sure that the organization has an effective compliance and ethics program should be assigned to a member of senior management. In many cases, this is the general counsel or the CAE, but in an increasing number of organizations it is given to a new executive role—that of the chief compliance officer (CCO). This role includes both a proactive and reactive aspect. It is proactive in the sense that the CCO is responsible for building the compliance and ethics program to deter organizational misconduct. The role is reactive in the sense that the CCO has responsibility for managing the responses to cases of actual or potential misconduct. The CCO should have direct access to both senior management and the governing body and report directly to them the effectiveness of the program and compliance and ethics issues that arise. The CCO must have sufficient authority to enforce standards, policies and procedures, and disciplinary actions. In large organizations there may be a number of compliance officers reporting to the CCO and many additional program staff. The organization should provide adequate human and financial resources to meet the program's mission and objectives.

Efforts to avoid assigning substantial authority to individuals with a history of noncompliance. One proactive step an organization can take to reduce the risks related to compliance and ethics is to make a serious effort to avoid hiring individuals prone to misconduct. Background checks and reference verifications should be performed on all prospective new hires. More rigorous tests should be conducted for senior management candidates and candidates for sensitive positions.

Education and training in compliance standards and procedures. Even an organization of people, each trying to do the right thing, can experience misconduct and ethical lapses if they do not know what behavior is appropriate or fail to recognize that they are facing an ethical issue. Education and training on compliance and ethics standards and procedures are essential. The general compliance and ethical expectations need to be communicated to each employee. This includes a code of ethics that is easy to understand, of reasonable length so that it will be read, and readily available via written documents and websites. The code should be translated into the relevant languages of the organization's personnel and distributed to vendors, customers, joint-venture partners, and other third-party stakeholders. Periodic training should be required of all personnel, including senior management, the board, and contractors.

Specialized education and training programs can be developed for those working in areas where there are complex compliance requirements (such as information privacy, Medicare billing, or safety) or high
risk of noncompliance (such as sexual harassment or conflicts of interest). Education and training should be designed to improve employees’ and managers’ ability to recognize ethical and compliance issues. For example, conflicts of interest training should focus on areas in which people are less apt to recognize such conflicts and training on giving and accepting gifts should encompass any differences in cultural practices that exist.

Monitoring and auditing to detect noncompliance and to evaluate effectiveness of the program. As discussed in chapter 6, monitoring is a critical part of any system of internal controls. Monitoring can help ensure that the compliance and ethics program is operating effectively. As exhibit 6-8 illustrates, monitoring can be an ongoing activity or periodic evaluations conducted by supervisors and managers involved in operations or in the compliance and ethics program. Such monitoring provides assurances to those within the line of operating responsibility and to the CCO. However, the governing board, senior management, and regulators may require higher levels of assurance provided by persons independent of operations and the compliance function. These higher levels of assurance can be obtained through the results of internal audit activities or other independent assurance activities.

The Guidelines call for two types of monitoring and auditing activities. The first is designed to directly detect criminal conduct. This type of activity includes, for example, a supervisor investigating an unusual transaction, a compliance officer conducting a review of gift disclosures, or the internal audit function reviewing expense reports of executives. The IIA’s Standards requires the internal audit function’s involvement in such monitoring by evaluating the risk exposures relating to compliance (Standard 2120.A1) and the effectiveness of compliance-related controls (Standard 2130.A1).

The second type of monitoring and auditing activities required by the Guidelines is periodic evaluation of the effectiveness of the compliance and ethics program. The IIA’s Standards also requires that the internal audit function evaluate the design, implementation, and effectiveness of the organization’s ethics-related objectives, programs, and activities (Standard 2110.A1). While such evaluations are often conducted by the internal audit function, they may be conducted as an independent peer review by compliance professionals from other organizations or a consulting firm. The Practice Guide, Evaluating Ethics-related Programs and Activities, has a number of best practices and specific guidance on how the internal audit function can evaluate the effectiveness of the organization’s compliance program.

An audit evaluating the effectiveness of a compliance and ethics program typically involves two major components:

1. The assessment of the entity-level controls over the compliance program which, at a minimum, includes evaluating the organization’s process for assessing risk of noncompliance and ethical misconduct and the design and implementation of the Guidelines’ seven elements.

2. The assessment of controls specifically designed to reduce the risk of noncompliance in the high risk areas identified by the organization’s risk assessment process.

The case study activities presented later in the chapter illustrate how certain aspects of such audits are conducted.

The Guidelines also recognize the importance of “hotlines” or other mechanisms that allow confidential or anonymous reporting by employees, customers, vendors, or other organizational stakeholders. Tips, particularly from employees, are the most common method of identifying noncompliance and misconduct.
Designing a method for individuals to provide information on actual or potential misconduct and to systematically collect and evaluate this information is one of the most effective monitoring tools an organization can implement. For these mechanisms to work effectively, particularly in the case of employees, the fear of retaliation must be mitigated. There should be a strong policy regarding protection from reprisals and an opportunity for anonymous reporting. This policy should be prominently featured in the code of ethics and in training.

A systematic and defensible process for assessing allegations should be developed. Assessment criteria commonly used include:

- The source of the complaint.
- The amount of tangible evidence.
- The degree of detail and specificity contained in the allegation.
- The seriousness of charges.
- Related complaints.

Best practice is for the assessment to be made by a committee rather than by the CCO or the CAE acting alone. Many organizations use committees composed of a representative from the compliance, human resources, internal audit, and legal functions. It is important to include human resources personnel on the committee because allegations of misconduct often involve issues such as disgruntlement with supervisors, perceived unfair treatment, or other personnel matters. Only about 13 percent ultimately pertain to corruption or fraud, while another 38 percent relate to company or professional code violations, employment law violations, or environment, health, or safety.10

**Performance incentives and disciplinary actions.** Organizations must not only “talk the talk” of compliance and ethics, but “walk the walk” by actually enforcing their policies and procedures through disciplinary actions and by providing incentives to act ethically. The organization should take a “zero tolerance” position by removing personnel who commit fraud and demonstrate serious misconduct from the organization and prosecuting them as appropriate. As is the case with all disciplinary actions, dismissal from the organization should be consistently applied to all personnel regardless of position. While compliance and ethics programs in most organizations tend to focus on negative incentives, positive incentives are also important. Most importantly, the organization’s compensation and incentive structure should be designed to support the compliance and ethics program.

**Response to criminal conduct and remediation.** Appropriate steps should be taken when an organization discovers an incidence of potential misconduct. Best practice suggests that, at least in large organizations, a formal response plan should be developed. The response plan should define the specific actions to be taken when a potential case of serious misconduct is uncovered. The plan should outline the steps to be taken and articulate specific remediation roles and responsibilities. The plan should address, for example, who is responsible for investigating the potential misconduct, when and how the board should be notified, who will inform outside parties, and who will determine and implement remedial action. It is particularly important that organizations develop a process for recording responses to both actual and potential misconduct. This record allows the organization to demonstrate to regulators, prosecutors, and the courts that it is committed to compliance and to maintaining a strong ethical culture.
ROLES AND RESPONSIBILITIES FOR THE COMPLIANCE AND ETHICS PROGRAM

Organizational compliance and ethics programs, along with organizational governance, have developed rapidly over the past two decades as society grapples with the challenge of regulating increasingly complex global organizations. Wide variability in how organizations assign compliance and ethics responsibilities still remains. It is becoming increasingly clear, however, that governing bodies, such as boards or their compliance or audit committees, are expected to be knowledgeable about their organizations’ compliance and ethics programs, obtain assurances regarding the effectiveness of these programs, and exercise reasonable degrees of oversight.

As indicated earlier in this case study, overall responsibility for managing the compliance and ethics program is assigned to an executive level position in the organization. It is becoming more common for larger organizations to assign this responsibility to a full-time CCO. Some organizations assign the responsibility to an executive with other responsibilities, such as general legal counsel, risk management, human resources, or the internal audit function. Although the benefits and drawbacks of the CCO performing other duties is the subject of continued discussion, there is widespread consensus that care must be exercised to avoid potential conflicts of interest. For example, combining the CCO role with legal counsel may result in the loss of attorney-client privilege and combining it with the internal audit function may require the use of an external service provider to independently evaluate the program’s effectiveness.

It also is common to assign responsibility for compliance in areas requiring particular technical specialization to officers responsible only for those areas. Such areas include, for example, health and safety, information privacy, financial trading operations, loss prevention, and quality of medical care. As indicated above, it is preferable for these specialized compliance functions to be integrated through the CCO as opposed to operating as their own “silos.”

Personnel in the organization other than those directly involved in the compliance function also have responsibilities for certain aspects of the program. Senior management is responsible for ensuring that the compliance and ethics program is designed to promote the right type of culture within the organization. They can demonstrate this through their selection and evaluation of the CCO and their support of the program. Both senior and operating managers are responsible for ensuring that all operations under their purview are conducted in accordance with applicable laws, regulations, and policies, including internal policies. The organization’s legal and regulatory department is responsible for identifying new compliance requirements as the legal and regulatory environment changes and to advise the organization on appropriate methods for implementing these new requirements. Human resources is responsible for conducting background checks of job candidates, making sure employees receive compliance and ethics training, and responding to actual or suspected misconduct. The internal audit function plays a significant role in the compliance and ethics program by investigating allegations of misconduct, evaluating how well specific risks have been mitigated, and providing assurance on the overall effectiveness of the program controls.

COMPLIANCE AND ETHICS PROGRAM MATURITY ASSESSMENT

As discussed in chapter 13, “Conducting the Assurance Engagement,” internal audits that are designed to provide assurance will typically focus on the risks and key controls within a process. However, a compliance and ethics program may be composed of several processes, each unrelated to the other but all designed to achieve the organization’s compliance and ethics objectives. As a result, compliance and ethics programs
may be designed in different ways, balancing the costs of such a program against the desire to achieve certain objectives. While developing tests to determine the design adequacy and operating effectiveness of key controls may still be appropriate when conducting audits of the key components of a compliance and ethics program, such tests may not be sufficient to evaluate the effectiveness of the program as a whole.

Potentially, a more valuable way to assess the effectiveness of a compliance and ethics program is to evaluate the overall maturity of the program. A compliance and ethics maturity assessment can help evaluate the sophistication of an organization’s compliance and ethics program. Using such an approach, key attributes of a compliance and ethics program can be evaluated against a spectrum of maturity for each of the attributes. An organization can have a snapshot of where the compliance activities stand at a particular point in time relative to a spectrum of maturity possibilities. This helps an organization identify gaps between the current state of maturity and the desired state. Exhibit CS 2-4 is an example of compliance and ethics program maturity attributes.

<table>
<thead>
<tr>
<th>Maturity Evolution</th>
<th>Maturity Levels</th>
<th>Maturity Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>World Class</td>
<td>The compliance and ethics program is considered “world class,” based on benchmarking and continuous improvement; many aspects of the program are highly automated and self-updating, thus creating a competitive advantage; extensive use of real-time monitoring and executive dashboards.</td>
</tr>
<tr>
<td></td>
<td>Mature</td>
<td>KPis and monitoring techniques are employed to measure success; greater reliance on prevention versus detection of compliance violations and ethical misconduct; strong self-assessment of operating effectiveness; assignments of responsibilities and accountabilities exist and are well understood.</td>
</tr>
<tr>
<td></td>
<td>Defined</td>
<td>Compliance and ethics requirements are well defined and documented, thus there is consistency even in times of change; overall compliance and ethics awareness exists; gaps are detected and remediated timely; performance monitoring is informal, placing great reliance on the diligence of people and independent audits.</td>
</tr>
<tr>
<td></td>
<td>Repeatable</td>
<td>Compliance and ethics practices are established with some policy structure; formal requirements are still lacking; some clarity on roles, responsibilities, and authorities, but not on accountability; increased discipline and guidelines support repeatability; high reliance on existing personnel creates exposure to change.</td>
</tr>
<tr>
<td></td>
<td>Initial</td>
<td>Compliance and ethics practices are fragmented and ad hoc; generally managed in silos and reactive; lack of formal policies and procedures; dependent on the “heroics” of individuals to ensure compliance and sound ethical conduct; greater potential for violations; higher costs due to inefficiencies; not sustainable.</td>
</tr>
</tbody>
</table>
How is such an approach used to evaluate a compliance and ethics program? The capability attributes described in exhibit CS 2-4 are too broad to provide much guidance in a comprehensive evaluation. Thus, a more detailed set of attributes must be determined for the key elements of a successful compliance and ethics program. Questions related to some of the more common key elements are as follows:

- **Code of Ethics**—How effectively does the code outline management’s expectations regarding ethical conduct?
- **Culture and Consistency**—How does the organization perceive management’s commitment to compliance and ethics?
- **Awareness**—How aware are employees and outside stakeholders of the compliance and ethics program and its requirements?
- **Structure and Accountability**—How effective is the structure for managing the program and enforcing accountability?
- **Process Automation and Integration**—How effectively are compliance and ethics controls and processes standardized, integrated, and automated?
- **Goals and Metrics**—How is success of the compliance and ethics program measured?

Exhibit CS 2-5 (click this [LINK](#) to download) provides characteristics for each of these attributes for all five maturity levels. The internal audit function can use this approach—or one like it that has been customized relative to the organization’s specific compliance and ethics objectives—to assess the maturity of the compliance and ethics program. Typically, this would involve the following steps:

1. Design tests to determine the current state of the compliance and ethics program for each of the key attributes. The case study activities that follow may provide useful insights into the types of tests that can be conducted to assess the current state.
2. Based on the results of the testing, determine the current maturity level for each of the key compliance and ethics attributes.
3. Conduct discussions with key compliance and ethics stakeholders to determine their desired level of maturity.
4. Identify gaps between the current and desired states.
5. Develop recommendations of actions management can implement to close those gaps.

Using a maturity assessment approach to evaluate the effectiveness of a compliance and ethics program can be a very effective way of providing valuable insights when auditing the program.

**SUMMARY**

Effective compliance and ethics programs have become an increasingly important factor in the success and long-term survival of organizations. In recent years, de facto “generally accepted principles” for an effective compliance and ethics programs have emerged, which include a significant role for the internal audit function. This role includes involvement in both monitoring the responses to compliance risks and providing overall assurance on the effectiveness of the organization’s compliance and ethics program. The following case study provides an opportunity to learn how the internal audit function can fulfill its responsibilities for organizational compliance and ethics.
CASE STUDY

Background Information

SHR Corporation is a midsize, publicly traded direct marketer and retailer of outdoor sporting goods based in the United States. Its common stock is listed on the New York Stock Exchange under the symbol “SHR.”

The company prides itself on selling high-quality outdoor sporting goods at competitive prices and providing outstanding customer service. SHR directly markets its merchandise through two major channels—its catalogs and its website—to customers in the United States and nearly 100 other countries. It currently has retail stores and distribution centers in the United States, Canada, and Europe. A salesforce is responsible for dealing with buyers at both the wholesale and retail levels.

SHR Corporation recently purchased MVF Company, a manufacturer of high-quality outdoor sportswear. The manufacturing process involves the use of technology-based machinery to cut cloth into various sizes, sew the cloth to conform with the size requirements of the sportswear, and use a series of dies and chemicals to ensure the colors meet consumer expectations. SHR also purchases merchandise from highly reputable vendors in the United States and several other countries.

SHR Corporation has enjoyed several consecutive years of sustained growth as reflected in the selected financial information, expressed in millions of dollars, presented below:

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2016</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Assets</td>
<td>$700.5</td>
<td>$546.5</td>
<td>$491.3</td>
</tr>
<tr>
<td>Sales Revenue</td>
<td>763.5</td>
<td>665.7</td>
<td>589.8</td>
</tr>
<tr>
<td>Operating Income</td>
<td>57.5</td>
<td>45.0</td>
<td>38.9</td>
</tr>
<tr>
<td>Net Income</td>
<td>34.3</td>
<td>29.0</td>
<td>26.0</td>
</tr>
</tbody>
</table>

Senior management is continuing its efforts to grow the company, increase its market share, and enhance shareholder value by:

- Further expanding its direct sales globally.
- Systematically increasing the number of retail stores.
- Selectively acquiring other businesses that are aligned with its core competencies.

Increasing competition over the past several years has motivated management to continuously pursue new and innovative ways to differentiate SHR’s products, streamline the company’s business processes, and take full advantage of advances in IT. Operating efficiency is a critical component of SHR’s competitive pricing strategy.

The risks that concern senior management the most heading into fiscal 2018 include the following:

- The continuing economic uncertainty may further decrease discretionary consumer spending, which in turn will adversely affect the company’s sales and profitability.
Mounting competition in the industry may make it increasingly difficult to differentiate the company’s high-quality merchandise at prices consumers are willing to pay.

Deterioration of the company’s brand or its positive image in the marketplace may adversely affect sales and profitability.

Failure to successfully integrate newly acquired businesses may adversely affect the company’s performance.

The inability to generate operating efficiencies and leverage IT may adversely affect the company’s profits.

Placing too much emphasis on operating efficiencies may adversely affect product quality and customer service.

During the first six months of 2018, SHR has experienced slower sales growth and higher operating expenses than anticipated. There is growing concern that forecasted performance targets for the year will not be achieved.

Scenario 1: Code of Ethics and Business Conduct

[To illustrate the concepts in this case study, the following scenario changes the facts provided in Case Study 1, “Auditing Entity-Level Controls,” where it was stated that SHR had a written code of conduct.] In the past, SHR has relied on a collection of individual policies to communicate its expectations regarding compliance with laws, regulations, and internal operating practices. The senior vice president – legal, who also is designated as SHR’s CCO, has determined that the company has grown to a size and operating complexity necessitating an integrated code of ethics and business conduct (the “code”). He has assembled a team consisting of personnel from the legal, human resources, and internal audit functions to develop this code.

Scenario 1 Activities

1. Explain why it is important to include representatives from the legal, human resources, and internal audit functions in the development of the code. What other areas of the organization, if any, should also be consulted when developing the code?

2. Based on the background and case facts describing SHR Corporation’s business, identify the types of laws and regulations that the company is subject to and should consider for inclusion in the code.

3. Develop an outline for SHR’s code listing the sections that should be considered to create a robust, comprehensive code. There is no need to develop any of these sections; simply create the outline.

4. Describe ways for communicating the new code and providing the necessary training to employees and new hires.

5. There are other key elements to an effective compliance and ethics program. Discuss the value of the following:
   a. Annual certification of compliance.
   b. Whistleblower hotline.
   c. Escalation and investigation process.
   d. Disciplinary action process.
   e. Compliance program audits.
Scenario 2: Employee Opinion Survey

Many aspects of a successful compliance and ethics program can be evidenced by documentation that supports the effectiveness of the program. However, similar to other entity-level controls (an effective code of ethics is considered an entity-level control), employee perceptions and buy-in may significantly influence the success of a compliance and ethics program. Unfortunately, there is little “audit trail” evidencing whether employees perceive the value and importance of a compliance program. As a result, the CCO has asked SHR’s CAE to develop and conduct a survey to help gain a better understanding of employees’ perceptions of SHR’s compliance and ethics program.

Scenario 2 Activities

1. Design a survey to obtain information about employee perceptions regarding the effectiveness of SHR’s compliance and ethics program. Assume that the survey will be delivered to all employees worldwide (don’t worry about any translation issues).
   - First, you need to determine the scale. For example, you could use a two-point scale (yes/no), a three-point scale (yes/no/unsure; agree/disagree/unsure), or some other scale. Provide justification as to why you chose a particular scale.
   - Next, develop the questions or statements that will be part of the survey. Since the objective is to determine employees’ perceptions, make sure you have a mix of knowledge and perception type questions.
   - Finally, discuss how you would deliver the survey to balance the costs of delivery against the percentage and value of responses. Support your decision.

2. Sample results from a survey can be downloaded from this [LINK]. Analyze the survey results, determine possible issues and root causes, and recommend appropriate actions to be taken. The survey results are contained in a template that can be used to document your analysis.

Scenario 3: Compliance and Ethics Program Maturity Assessment

As discussed earlier in this chapter, it may be more meaningful to evaluate a compliance and ethics program using a maturity assessment instead of following a more traditional controls-focused approach. This helps ensure sufficient compliance and ethics procedures and controls are in place to mitigate the compliance risks from certain regulations, such as the Federal Sentencing Guidelines in the United States, while ensuring reasonable but not excessive resources are applied to the program. The board of SHR has expressed concerns to the CAE about whether the compliance and ethics program is adequate, while senior management has been concerned about the costs of maintaining such a program. As a result, SHR’s internal audit function has decided to conduct a maturity assessment of the program. [Note that some aspects of a compliance and ethics program may contain subtle complexities that require the assessment of a legal professional. For the purposes of this scenario, it is not necessary to be concerned with legal interpretations or opinions.]

Scenario 3 Activities

1. Given the case facts above, including those provided in scenarios 1 and 2, as well as the example of compliance and ethics program maturity attributes shown in exhibit CS 2–5, complete a compliance and ethics maturity assessment of SHR’s program. You may need to make certain assumptions about other SHR facts if such facts were not previously disclosed. Document your assessment in a table similar to the following. For this activity, you will only complete the second column. A template of this table can be downloaded by clicking this [LINK].
2. Building on that maturity assessment, management’s desired level of maturity is provided below. Based on your assessment of the current maturity level, as documented in activity 1, and management’s desired level, determine where significant gaps exist and recommend actions to close those gaps. Complete the third and fourth columns in the table above to document this activity. [Note that not all attributes will have significant gaps.]

- Code of Ethics – Mature Level
- Culture and Consistency – Mature Level
- Awareness – Mature Level
- Structure and Accountability – Defined Level
- Process Automation and Integration – Mature Level
- Goals and Metrics – Defined Level

**Scenario 4: Test of Compliance with SHR’s Gift Exchange Policy**

Given the growth in SHR’s salesforce around the world, as well as management pressures to continue sales growth during more difficult economic times, the internal audit function decided to include an audit of the company’s gift exchange policy in the annual internal audit plan. The objective of this audit is to evaluate compliance with the policy and recommend improvements that may help to ensure ongoing compliance in the future.

SHR’s Gift Exchange Policy is summarized below:

Creating and maintaining good relationships with our customers, suppliers, and business partners are important to SHR’s success. The occasional exchange of gifts, meals, and entertainment of small value are a common business practice meant to provide a legitimate opportunity to interact, create goodwill, and establish trust.

However, it is important to use good business judgment when determining the appropriateness of gifts, meals, or entertainment. Business gifts that are extravagant or would influence behavior are inappropriate and should not be given or accepted. An inappropriate gift might cloud objectivity and decision-making. The exchange of gifts given with the intent to bribe, make a kickback, or place undue influence are illegal and not the way SHR conducts business.

An appropriate business-related gift is:

- Of moderate value, whether given or received.
- Something that will not embarrass or discredit the company.
- Not made in cash or cash equivalent such as checks, money orders, stock, and similar items.
- Gifts, meals, or entertainment that you receive that have an actual or estimated value of over US $500 must be reported to the CCO.
Scenario 4 Activities

1. Based on your review of the policy above, what would you consider the strong points of the policy and what, if any, shortcomings did you notice?

2. Develop key steps to test compliance with the Gift Exchange Policy. Specifically, outline key procedures that might be performed to test the design adequacy and operating effectiveness of controls related to this policy.

References:
3. Ibid.
11. The Internal Audit Foundation based the structure and certain other elements of this model, in part, on “CMMI® for Development, Version 1.2,” CMU/SEI-2006-TR-008, copyright 2006 Carnegie Mellon University, with special permission from the Software Engineering Institute. This model has not been reviewed nor is it endorsed by Carnegie Mellon University or its Software Engineering Institute. CMMI is a registered trademark of Carnegie Mellon University.