

International Compliance 101, 2nd Edition

Chapter 2: The Seven Essential Elements

1. Standards and Procedures

The first of the basic compliance elements in industry guidance recommends that the organization establish standards and procedures to prevent and detect criminal conduct. The standards or code of conduct and the policies and procedures help to create the infrastructure for your compliance program.

The standards of conduct, first and foremost, demonstrate the organization’s overarching ethical attitude and its organization-wide emphasis on compliance with all applicable laws and regulations. The code is meant for all employees and all representatives of the organization. This includes management, vendors, suppliers, and those who are working on behalf of an organization, which are frequently overlooked groups. From the board of directors to volunteers, everyone must receive, read, understand, and agree to abide by the standards of the code of conduct. Having employees sign an annual attestation of receiving the code is a best practice and helps to elevate the importance of the document. The code should be written plainly and concisely in an accessible style. An easy-to-understand reading level is recommended. Plain and concise does not mean generic, however. The contents of the code of conduct will need to be tailored to the organization’s culture, business, and corporate identity. Also, institutions with a diverse constituency should consider providing the code of conduct in other languages, sign language, or even Braille as appropriate. When providing the code in different translations, the organization should “test” that the translation is accurate.

Establishing an organization-wide code of conduct is a key recommendation of the Organisation for Economic Cooperation and Development (OECD), which in 2010, established the “Good Practice Guidance on Internal Controls, Ethics and Compliance.” The OECD’s Working Group on Bribery, which authored the Guidance, urges companies to establish:

1. Strong, explicit and visible support and commitment from senior management to the company’s internal controls, ethics and compliance programmes or measures for preventing and detecting foreign bribery;
2. A clearly articulated and visible corporate policy prohibiting foreign bribery....^[1]

The OECD’s Guidance is contained in its 2009 Anti-Bribery Convention, an internationally recognized document that has been ratified by its 36 member countries and eight non-member countries.^[2] While its primary focus is on preventing bribery, the convention supports compliance programs with a larger focus, stating that its recommendations “should be interconnected with a company’s overall compliance framework.”^[3]

The code of conduct provides a process for proper decision-making, for doing the right thing. It elevates corporate performance in basic business relationships and confirms that the organization upholds and supports proper compliance conduct. Managers should be encouraged to refer to the code of conduct whenever possible, incorporating elements or standards into performance reviews. Compliance with the standards must be enforced through fair and consistent discipline when necessary. Disciplinary procedures should be clearly stated in the standards, and the penalty—up to and including dismissal—for serious violations of the standards of conduct must be mentioned to emphasize the organization’s commitment. (*See Element Number 6 – Enforcement and Discipline.*)

Code of Conduct—Content Checklist

- Demonstrates an organizational emphasis on compliance with all applicable laws and regulations
- Is written plainly and concisely so all employees can understand the standards and responsibility (no higher than the average 14-year-old can read)
- Is translated into other languages, as appropriate
- Includes frequently asked questions or scenarios based on high risk areas
- Includes expectations for employees on interactions with other employees, suppliers and agents
- Mentions organizational policies without completely restating them
- Is consistent with company policies and procedures
- Includes management's responsibility to explain and enforce the code.

Code of Conduct—Communicating to Employees

- All employees must receive and read the standards
- A supervisor or qualified trainer should explain the standards and answer any questions
- Employees should attest annually in writing that they have received, read, and understood the standards
- Employee compliance with the standards must be enforced through fair and consistent discipline when necessary
- Noncompliance with the standards will be disciplined and this should be clearly stated.

Code of Conduct—Purpose

- To present overarching guidelines for employees to follow
- To clearly state expectations for all employees to understand what is required of them
- To provide a process for proper decision-making
- To assure that employees put standards into everyday practice
- To elevate the organization's performance in basic business relationships
- To confirm that the organization upholds and supports proper compliance conduct.

(See Appendix A.1, Sample Letter to Vendors.)

Policies and Procedures

Whereas a code of conduct provides guidelines for business decision-making and behavior, the compliance policies and procedures are specific and address identified areas of risk. Most organizations already have an employee manual that outlines all human resource-related policies and procedures, and they may have other operational policies and procedures specific to certain business practices or operations. Whenever possible,

compliance policies and procedures should be integrated into existing policies, and all policies within an organization should be consistent with laws, regulations, industry requirements, and general compliance. In fact, as part of the implementation of a compliance program and while in the process of drafting compliance policies and procedures, all other policies within the organization should be reviewed and revised as necessary. While it is imperative that the organization have policies and procedures, it cannot be emphasized enough that the only thing worse than not having a policy is having a policy and not following it.

Develop your policies and procedures carefully. Take care that they are realistic and measurable. Be sure your goals are realistic. A non-retaliation policy is critical to the success of your program and should be communicated during annual education each year. It is one policy that every employee should know about.

Two types of compliance policies and procedures should be developed by every organization: structural and substantive. The structural policies create the basic framework of how the compliance program will operate. The substantive policies define the applicable regulations that apply to the organization and how to operate compliantly within those regulations. They also indicate the applicable risk areas to an organization and describe appropriate and inappropriate behaviors with regard to those risk areas. Both the structural and the substantive policies and procedures are essential to a compliance program so that the rules to which employees will be held and the method for enforcing the rules are clearly documented.

Structural policies and procedures should be developed to address:

- Directives or mission of the compliance program
- Revision of existing and creation of new policies and procedures (including distribution and updating requirements)
- Role of the compliance officer
- Role of the compliance committee
- Educational requirements
- Method for anonymous reporting and non-retaliation for reporting: It is important to have a clearly stated policy on non-retaliation and non-retribution in the organization. Let everyone know there will be no retaliation or retribution for bringing forth problems.
- Auditing processes
- Monitoring processes
- Method for responding to reports of possible misconduct
- Method for responding to internal and external requests for documents or other investigations
- Disciplinary action plan which is consistent with HR processes and/or policy
- Record retention/destruction.

Substantive policies and procedures should be developed to address:

- Process for preventing inappropriate actions in specific risk areas for which there are not already policies to address those areas; e.g., conflict of interest, privacy and security of information, intellectual property, export controls, etc.

- Key risk areas where an organization may not have a defined policy and/or business owner; e.g., conflicts of interest, privacy and security of information, etc.
- Documentation requirements.

Policies and procedures, like the code of conduct, must be living documents, not just a binder on a shelf. They must become integral to the day-to-day operation of the organization. That is what forms the basis for an effective compliance program. To determine if that goal is met, consider: How are the policies and procedures applied every day? Are they incorporated into performance reviews? Educational programs? Are they reviewed and updated according to a schedule and on time? Revising policies and procedures is a complex and ongoing process and requires periodic review and revisions to assure they are current. Assure that someone is accountable for every policy and procedure. Again, standards of conduct, policies, and procedures are the tools of compliance, but they must be used and sharpened to be effective.

2. Compliance Oversight

Industry standards recommend designation of a compliance officer to serve as the accountable role for compliance program activities. Whether the position is full time or part time will depend on the size, scope, and resources of the organization. In most cases, the position should be a full-time role and an organization will determine the feasibility and scalability of dedicating resources. Also, assigning the compliance officer appropriate authority is critical to the success of the program. On a specific level, for example, the compliance officer must have full authority to access any and all documents that are relevant to compliance activities. This includes documents such as financial statements and supporting documents, contracts with suppliers and agents, and other accounting records. In the big picture, however, “appropriate authority” comes from the unquestionable backing by the CEO and board of directors or its equivalent, the sources of ultimate authority and respect.

Appropriate authority and the full backing of the board of directors and management are consistent with industry practice. To carry out such operational responsibility, such individual(s) should be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority. This is logical because it is the board that supported the launch of the compliance initiative and approved the hiring of the compliance officer. Board members may even be actively involved in the interviewing of the compliance officer candidates. They also should be involved in the development of the compliance officer’s job description, and an important part of the compliance officer’s reporting structure.

There is concern and some risk involved in having the compliance officer report to general counsel or to the chief financial officer. This reporting arrangement creates real and/or potential appearance of conflict of interest due to their respective roles with management. Separation of compliance from legal and finance when possible, helps ensure that all aspects of the compliance officer’s role will be independent and objective (meaning there is no real or perceived vested interest in the outcome). There are different reporting structures for the compliance officer role and many variables should be considered by the organization for determining what works best for the individual organization. However, the dominant theme in industry on the reporting structure is for the compliance officer to report directly to the organization CEO and/or the internal governing body (e.g., oversight committee, supervisory board, administrative body, board of directors, audit committee) to maintain their real and/or perceived independence. To maintain independence the compliance officer should not be part of management. The size and setting of your organization will influence its reporting structure. It is recommended that the board or its liaison committee have, at minimum, a “dotted line” or indirect reporting relationship with the compliance officer. See below a snapshot view of compliance officer reporting structures, from a 2018 survey conducted by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association.

To Whom Compliance Officer Reports	For profit, publicly traded	For profit, privately held	Nonprofit	Other	Total for all organizations
Board	53%	62%	53%	58%	56%
Chief Executive Officer	13%	18%	22%	20%	20%
Chief Financial Officer	2%	7%	6%	3%	5%
General Counsel	24%	7%	8%	5%	9%
Human Resources	0%	0%	2%	0%	1%
Audit	0%	1%	1%	2%	1%
Other	7%	5%	8%	12%	8%

Compliance Officer Reporting Structure^[4]

The compliance officer's duties also will vary depending on size and scope of the program. The focus of the position should be the implementation, administration, and day-to-day oversight of the compliance program. Primary responsibilities should include the following:

- Designing, implementing, overseeing, and monitoring the compliance program
- Reporting on a regular basis to the organization's governing body, CEO, and compliance committee
- Revising the compliance program periodically as appropriate
- Developing, coordinating, and participating in a multifaceted educational and training program
- Ensuring that those we do business with are aware of the organization's compliance program requirements
- Serving as a source of compliance-related information for employees, management, suppliers, and the board
- Ensuring that appropriate background checks are conducted according to country-specific regulations
- Assisting with internal compliance monitoring and auditing activities
- Assuring management has mechanisms in place to mitigate risks
- Independently investigating and acting on matters related to compliance
- Assuring management takes corrective action to resolve the problems identified
- Assuring the organization has given employees a mechanism for reporting potential issues.

The compliance officer is a unique position requiring an individual who understands the nature of the business or

industry, is capable of understanding and questioning practices in the organization, including financial areas, is knowledgeable of applicable legal requirements that may be imposed in the industry for wrongdoing, has strong written and verbal communication skills, and is firm yet approachable. Whatever the tenure or the educational level, the compliance officer, as “focal point” of the program, must be a figure respected and trusted throughout the organization. Strong interpersonal skills, good listening abilities, and discretion are mandatory. (See *Appendix A.2, Sample Compliance Officer Job Description.*)

As compliance has grown and matured as a profession, it has, like other professions, sought to identify and distinguish those in the field who have, with experience and education, achieved the necessary skill set to be an effective compliance officer.

Moreover, compliance officers are also stewards of a public trust, and therefore the services provided must be of the highest standards of professionalism, integrity, and competence. The Code of Ethics for Compliance Professionals (see *Appendix B*) addresses three principles, which are broad standards of an inspirational nature. They include:

Principle I: Obligations to the Public—Compliance and ethics professionals (CEPs) should abide by and promote compliance with the spirit and the letter of the law governing their employing organization’s conduct and exemplify the highest ethical standards in their professional conduct in order to contribute to the public good.

Principle II: Obligations to the Employing Organization—Compliance and ethics professionals (CEPs) should serve their employing organizations with the highest sense of integrity, exercise unprejudiced and unbiased judgment on their behalf, and promote effective compliance and ethics programs.

Principle III: Obligation to the Profession—Compliance and ethics professionals (CEPs) should strive, through their actions, to uphold the integrity and dignity of the profession, to advance the effectiveness of compliance and ethics programs, and to promote professionalism in compliance and ethics.

These principles and the accompanying rules of conduct should be reviewed and studied—and adhered to—by all compliance officers.

The compliance officer may be the focal point of a compliance program, but he or she cannot be the only point, nor does this role “assure” compliance for the organization. Industry has demonstrated that the formation of a compliance committee can be an effective addition to the program, although the specific composition of the committee may vary according to the organization. The committee will benefit from having varying perspectives such as operations, finance, audit, human resources, and legal, as well as employees and managers of key operating units. This committee will assist the compliance officer in ensuring effective mechanisms are in place to mitigate risk areas, real and/or potential.

The compliance officer’s role with the compliance committee can also vary. In some organizations the compliance officer sits *ex officio*. In others, the compliance officer may even chair the committee. We are finding that as the compliance profession matures and compliance programs evolve, the compliance officer usually chairs the compliance committee. In some organizations you will find two compliance committees, one, a high-level board committee and then a working committee. The working committee usually reports to the board level committee. Regardless of who chairs the committee, the compliance department commonly is responsible for scheduling meetings, preparing the agenda, taking and distributing minutes, and coordinating follow-up.

Compliance committee functions, in addition to aiding and supporting the compliance officer, can include the following:

- Offering advice to the compliance officer
-

- Assisting with evaluating the compliance program
- Reviewing statistics and trends of audit results, reports of non-compliance, etc.
- Assisting with the development of standards of conduct
- Reviewing industry guidance and new information regularly and integrating it into the compliance program
- Determining the appropriate strategy to promote compliance
- Assisting with the compliance risk assessment
- Developing a system to solicit, evaluate, and respond to complaints and problems.

The importance and potential influence of the compliance committee cannot be overstated. Look for committed individuals who will be strong, visible, and vocal advocates for the compliance program. Furthermore, the committee should be composed of individuals representative of each unique department in the organization so that they can communicate to the rest of the committee and the compliance officer the compliance activities and risk areas within their department. The members are also important in providing communication back to their respective departments on the organization's compliance requirements. The committee is a vital source of information both to the compliance officer and the rest of the organization.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)