The Complete Compliance and Ethics Manual 2023
Developing and Implementing Policies for an Effective Program

By Caroline K. McMichen, CCEP, CIA[1]

Together with the code of conduct, ethics and compliance policies are the foundation of an ethics and compliance program. Careful consideration must be taken when developing and implementing them to ensure their effectiveness.

What Do the Guidelines Say?

It is always best to begin with what is required. In the case of the company's ethics and compliance program, the U.S. Federal Sentencing Guidelines are generally considered the standard. The guidelines say that an organization must "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, and other aspects of the compliance and ethics program," to all people in the company (employees, senior management, and the board) and potentially outside agents or third parties who act on behalf of the company.[2]

Standards and procedures referred to here are the code of conduct and other written policies and procedures a company has to mitigate compliance risks, educate employees, and provide guidance to enable them to do the right thing. Together, these written standards provide a framework for consistent business practice across an organization and are the foundation of the ethics and compliance program. They may consist of both principles-based policies, such as the code or corporate social responsibility policies, and rules-based policies such as anti-corruption, antitrust/competition, gift and entertainment, or information security policies. Principles-based policies set up a framework within which employees may make decisions that are consistent with the company's principles and/or values. Rules-based policies provide very specific dos and don'ts for employees and do not allow for much interpretation. A good program includes a combination of these.

We Have a Code of Conduct: What Other Policies Do We Need?

The code of conduct likely covers all of the significant ethics and compliance risks a company/industry faces, but it may not be enough to guide employee behavior. Experience has shown that the most effective codes of conduct are principles-based, rather than outlining specific rules. They are often written at a high level to accommodate a broad, often global, audience. Because of this, they may not provide enough detail on each risk area to ensure employees are adequately informed and prepared to handle any applicable situation that may arise in their work. For risk areas requiring very specific guidelines for employees, rules-based policies are often required to supplement the code. A specific function (e.g., human resources, legal, IT) may adopt additional or complementary policies that are consistent with global policies for use within those functions or specific locations. A sample of this would be a finance-specific or regional policy based on local laws. Also, a global policy may include region-specific information to avoid having multiple policies with the same content.

To better understand what policies may be needed, start by reviewing your company's risk assessment to identify the areas of significant compliance and ethics risk for your company/industry. Next, take an inventory of existing policies and procedures. Are there any gaps? If so, consider whether a new policy is needed. Some things to consider before drafting a new policy are:

- Is this risk area adequately covered by our code of conduct?

- Will an employee know how to comply with the principles outlined in the code of conduct?

- Is this policy specifically required by a law or other commitment?

- Who will this guidance apply to?

- What has been done in the past to provide guidance to employees or resolve issues related to this risk area?

- Will we be able to monitor and enforce this policy, and is its enforcement necessary to achieve company goals?

- Is the investment required to properly develop, communicate, and enforce this policy reasonable in relation to the benefits/risk mitigation obtained?

- Are there other options, i.e., might you be able to amend an existing policy to include this risk area?

- Is the creation of this policy consistent with the company's culture?

(See Appendix 3-H for Sample Policy Prioritization Matrix.)