Developing and Implementing Policies for an Effective Program

By Caroline K. McMichen, CCEP, CIA

Ethics and compliance policies are the nuts and bolts of an ethics and compliance program. Careful consideration must be taken when developing and implementing them.

What Do the Guidelines Say?

It is always best to begin with what is required; and, 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.

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 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, Corporate Social Responsibility or Privacy policies; and rules-
based policies such as Anti-Corruption, 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 do’s 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 in order 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 (i.e., HR, Legal, IT, etc.) may adopt additional or complementary policies which are consistent with global policies for use within those functions or specific locations. A sample of this would be a “finance” or “regional” specific HR policy based on local laws. Also, a global policy may include regional 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, and Appendix 3-E for some sample policies.)

Who Is Responsible To Develop New Policies?

Companies may take different approaches to policy development and management. It may be centralized or decentralized, but it is important to establish ownership and a clear and consistent process so people understand their roles and responsibilities.

In a centralized approach, policy development typically begins at the corporate headquarters with the ethics and compliance team or a cross-functional committee. The central team or committee identifies the need for the policy and prepares a draft that may be circulated to designated people with subject matter expertise in the business units for review. The business units may submit feedback, including possible revisions to address differences in local law or practice. The central team or committee has final approval authority. This approach has the advantages of avoiding duplicate or conflicting policies and ensuring that the company’s overall values and culture are represented across the organization. A disadvantage may be that in order to achieve a common approach, you are unable to provide very specific local guidance to employees who may need it.

In a decentralized approach, policy development is at the local or business unit
level. Local subject matter experts identify a need for a policy and draft the
guidance. This enables them to more fully adapt the policy to local law and
practices. Ownership at the business unit level typically allows for easier
business unit buy-in and distribution to employees. A possible disadvantage is
that there is a tendency to create more policies than may be necessary; and,
without proper corporate oversight business unit policies may not take on the
desired cultural tone or may even conflict with one another. Because of this,
policies are often sent for review by a central team or committee before final
approval even when the decentralized approach to development is taken.

In either approach, there should be a clear owner of the process. That may be
the Ethics and Compliance Department, the Legal Department or a cross-
functional committee. The owner is responsible to ensure that there is an
established process and that it is consistently followed. The process should
include steps such as:

- **Establishing** policy criteria—determining what is worthy of a policy vs.
  procedures or other form of employee guidance
- **Identification** of the subject matter expert or content owner
- **Defining** the process for development, review and approval
- **Planning** for policy communication and/or training
- **Identifying** and maintaining a central policy storage location that is easily
  accessible by employees and ensures one “source of truth”
- **Establishing** policy compliance criteria
- **Defining** a process for ongoing maintenance, such as periodic review and
  revision.

This process may be manual or automated using an internal platform such as
Sharepoint or a third party provider’s policy management tool. These tools
often include document tracking, workflow and storage capabilities, along with
automated alerts for revision and ongoing maintenance.

(See Appendix 3-I for Sample Policy Development Workflow.)
Purchase Login