Falling

Here's some advice on how to develop an EFFECTIVE COMPLIANCE PROGRAM and avoid some common pitfalls.

BY JOHN SCHNEIDER

into Line

IN today's hazy, ambiguous regulatory environment, financial executives have yet another daunting set of tasks to perform. They need to determine exactly how much money to invest to develop a comprehensive corporate governance function. There are many important questions to ask, and one that's at the top of the list is "How much is enough?" This question comes up regularly when executives are discussing the topic of compliance, an Achilles heel for most companies, yet, ironically, one of the most critical but underdeveloped governance functions. Financial executives are continuously faced with the challenge of trying to satisfy regulators while struggling to stay within company-mandated budgets to become compliant. They know full well that an inadequate compliance program could ultimately bring the wrath of regulators and the general public if the company is viewed as trying to cut corners. What would the cost be then?

PLAN STRATEGICALLY, EXECUTE TACTICALLY

Over time, increased attention by investors and the media, coupled with inconsistent regulatory guidance on compliance, has forced some companies to implement compliance program components that might or might not integrate well with existing plans. This "patchwork effect" has a longer-term detrimental impact on governance and compliance budgets.

For various reasons, few executives are able to take a step back from the deluge of compliance paperwork and new regulations to determine—from a 30,000-foot overview—how to maximize the financial spend to align governance activities and ensure that compliance is implemented effectively and efficiently. When comparing "best practices" with "best efforts," how does a company quantify the risk associated with noncompliance and/or additional regulatory scrutiny?

One important step that an organization must take is to determine if it can explain its governance and compliance activities relative to the requirements. Once it can, developing a strategic road map that can be executed over time becomes much easier. Eight steps, which are outlined in Figure 1, provide a process flow or conceptual road map to help build an effective compliance program. In this article I'll focus on the first two and then address some of the common pitfalls that companies should be aware of and avoid.

STEP ONE: ESTABLISH A VISION

Developing a "culture of compliance" is highly dependent on understanding the elements of an effective compliance program and how they fit within your organization. Establishing a consistent message that clearly articulates senior

ILLUSTRATION: DIANE BIGDA/ARTVILLE

management's vision for compliance is an important first step. Then it's critically important for each management team to take this vision, interpret the message, and communicate the message consistently to all parts of the organization. Quite simply, this means transforming compliance activities into actionable and measurable activities that become part of everyone's job responsibilities.

Compliance isn't new for many organizations—it has been a component of doing business in highly regulated industries, such as the financial services sector, for some time. In these organizations, reemphasizing the importance of compliance is more of an art than a science. Even when it comes to communicating senior management's vision, crafting the message in such a way that it is perceived correctly may take a bit of planning and awareness of the organization's history of compliance.

Having a clear comprehension of the cost and effort required to begin compliance efforts is also very important to achieving success. Not surprisingly, many companies have reported that the costs associated with complying with recent regulatory requirements have far surpassed the estimates of regulators, industry groups, and management, and many business leaders have struggled with the costs vs. the benefits of implementing compliance programs. Focusing on the steps that are being taken to address the immediate regulatory requirements and weaving in other compliance efforts by your organization are important components of having an effective vision for compliance.

STEP TWO: ORGANIZING THE EFFORT

Organizing the effort to implement an infrastructure for ongoing compliance with laws and regulations is the most important element in the development process. Always come with an end date for the implementation of

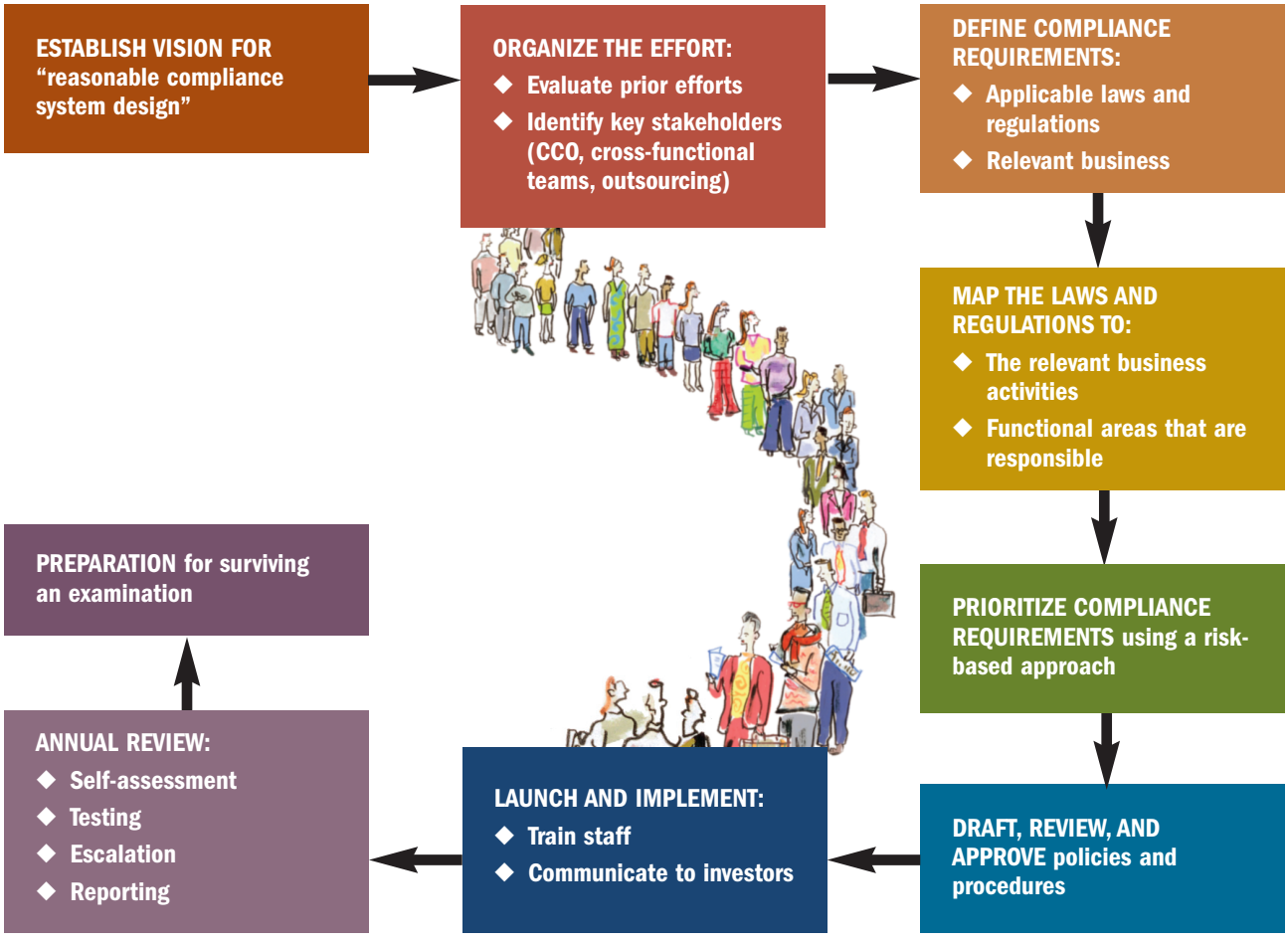

Figure 1: A STEP-BY-STEP APPROACH—A life-cycle approach for developing, implementing, and sustaining compliance programs. Using a life-cycle approach provides repeatable steps that will provide a baseline for developing and implementing a robust compliance program. Following this approach will allow the program to be maintained as a living system within your organization. A critical element for using this approach or any other approach that works for your organization is documenting where your compliance efforts are as of a point in time.

policies and procedures to comply with the new regulatory requirements set forth by the regulators. Knowing the end date, developing a timeline, and allocating resources are critical factors driving a compliance program forward. Identifying and involving the key stakeholders and creating a communication plan are also paramount to success. Without buy-in from everyone involved in the process, a company could undergo intense regulatory scrutiny before it has a chance to implement its compliance infrastructure.

Once the capabilities for organizing the effort are in place, contemplate tailoring the effort to each area within your company. Take the Gramm-Leach-Bliley Act of 1999. This regulation requires organizations to maintain the privacy of client information, so efforts you make to develop and implement enhanced data security may also benefit other compliance efforts, such as records retention. Understanding short- and long-term compliance efforts will help organizations plan more effectively and use their limited resources more efficiently. This thought exercise lets them think strategically but act tactically—at least in the short run. It will also allow the industry and regulators to identify best practices. In many cases, it isn't until after industries have gone through the efforts associated with developing and implementing policies, procedures, and systems to comply with new regulatory requirements that best practices emerge.

TRAPS FOR THE UNWARY

The deltas between what a company's contracts and policies state and what its real, underlying procedures are will be the ultimate measure of noncompliance during an audit. New regulations are usually adopted at a point in time when organizations already have implemented policies and procedures and their business models have gone through several transformations, so implementing comprehensive compliance programs in these environments is particularly difficult. One common pitfall is that compliance programs are implemented as of the required effective date forward. Companies need to look at what has historically been included in contracts and policies, not just current business activities. For example, organizations that have gone through acquisition or divestiture of business units may not have updated contracts or policies to reflect the current business activities. In the case of an acquisition, the new business activities may not have been contemplated in the preexisting policies and procedures.

Companies also should perform a risk-based assessment of the current state of affairs on an ongoing basis. This is particularly important when an organization is going through divestiture, acquisition, introducing new products, and other changes.

Resources for the CFO

Company leaders have steadily keyed in on the importance of compliance, and there has been a corresponding response by outside resources. For instance, CFOs have an incredible amount of information available online that can help them better understand compliance issues in general and those specific to their industry segments. As most companies have compliance requirements specific to their industries, many trade and professional associations have developed compliance education and other resources to assist their members. Also, software that has been developed by independent audit groups is available and can be very useful.

On a more active level, companies that seek even deeper expertise and hands-on help sometimes look to consultants who can offer advice on what a company needs and actually put into place, monitor, and oversee a program. Given the less-than-perfect guidance that's provided in most industries when laws and regulations are promulgated, finding the right assistance is one of the most important decisions a CFO can make. For example, compliance professionals can provide insights about industry best practices and techniques designed to avoid common pitfalls.

Regulators also can provide valuable information and guidance, and interacting with them can often have the benefit of positioning a company as having a strong desire to comply.

How are compliance tools and resources scalable?

Firm size, organizational structure, and product complexity are just a few variables that should be considered when determining the appropriate tools to use. Equally important is determining the plans for growth: new products, new client types, different distribution channels. Once a CFO understands these factors, he/she can better assess the scalability tools and resources needed to develop and implement the appropriate compliance infrastructure.

COMMON PITFALLS

There are a number of common pitfalls companies need to avoid when they're developing a compliance program because these traps can severely undermine their efforts. Developing a good program requires careful documentation, vision, and communication; a deep understanding of the laws; and an equally keen sense of the company's business and business functional units that must be understood in the context of those laws. Here are some of the most common and deleterious pitfalls.

◆ **Organizations don't formally document their vision of a reasonably designed compliance program.** The SEC and other regulatory agencies have made it clear that transparency will be treated favorably during examinations. The first step is to have a road map from the top that documents the organizational vision for compliance. A road map for compliance may include a three-year plan that lays out this way: Year one will be to develop a compliance manual. In year two, an automated repository will be developed for the policies and procedures. Year three will be to develop an automated monitoring program. Realizing that this example is high level, the road map articulates the compliance vision and provides a plan for continuous improvement.

◆ **Senior management doesn't clearly and visibly articulate the organization's vision to each business unit**

Weighing the Costs of Noncompliance

Corporations are still reeling from the recent onslaught of penalties and disciplinary actions that the SEC has levied in the wake of the scandals that have unfolded in recent years. And this trend doesn't appear to be over. As recently as January 2006, SEC Chairman Christopher Cox announced guidance for how the SEC will impose penalties going forward.

Here's a quick summary of the criteria the SEC adopted in January 2006:

Whether the corporation received a direct benefit as a result of the volatile conduct. The Commission said that a corporation's direct and material benefit from the offense, or otherwise unjust enrichment, heavily supports a corporate penalty. Specifically, the strongest case for a penalty arises where shareholders of the corporation received an "improper benefit" as a result of the offense.

The degree to which the penalty will recompense or further harm the injured shareholders. The SEC found that the ability to use a penalty as a source of funds to compensate injured shareholders also supports imposition of a penalty. But the likelihood that a corporate penalty would "unfairly injure investors, the corporation, or third parties weights against its use as a sanction." Section 308 of the Sarbanes-Oxley Act of 2002 (fair funds provision) permits the Commission to collect penalties paid by individuals and entities and disburse those monies along with disgorgement funds to victims. In situations where the noncompliant event resulted in a gain in revenues, the disgorgement funds are a calculated estimate of the revenue for the period of noncompliance.

The Commission also published seven additional factors it considers in determining whether to impose a penalty on the corporation:

The need to deter the particular type of offense. The likelihood that the penalty will act as a strong deterrent to others also impacts the SEC's penalty determination. Conduct likely to be repeated by those involved or others similarly situated is a factor favoring a penalty.

The extent of the injury to innocent parties. The SEC will consider the egregiousness of the harm, the number of victims, and the extent of "societal harm" if the conduct goes unpunished.

Whether complicity in the violation is widespread throughout the corporation. The pervasiveness of the violation within the corporation also favors use of the penalty. The SEC indicated it is more inclined to seek a corporate penalty where violations are widespread within the organization as opposed to the isolated conduct of a few individuals. The SEC will also consider whether the corporation has taken appropriate employment action against culpable individuals.

The level of intent on the part of the perpetrators. The SEC will more likely impose a penalty where the conduct at issue was deliberate and shows fraudulent intent by the perpetrators.

The degree of difficulty in detecting the particular type of offense. The SEC says that offenses that are particularly difficult to detect require penalties significant enough to deter organizations from noncompliance.

Presence or lack of remedial steps by the corporation. Prompt remedial action by management will weight against the use of a penalty. In contrast, the SEC states it is more inclined to insist upon a penalty where management fails to take the appropriate remedial steps.

Extent of cooperation with the Commission and other law enforcement. Consistent with the SEC's previously stated factors for evaluating a corporation's cooperation with its investigation, the SEC's penalty determinations also depend upon the degree to which a corporation self-reports the offense and otherwise cooperates with the investigation and remediation.

Now for the underlying question: How much will compliance cost? Based on recent regulatory changes that have resulted in spending on compliance, such as SOX, the cost can be considerably higher than the estimates provided by the SEC. Given the significance of the potential cost for compliance, companies need to develop a meaningful strategy that is underpinned with well-defined tactical action steps. This will create the transparency that the SEC is looking for and enable organizations to implement an effective compliance program over a reasonable period of time and in a meaningful way.

and employee to establish a "culture of compliance." Not having a clearly articulated vision can result in inefficient and ineffective programs. For example, a program that is implemented without a clear vision often results in a lack of ownership. In many compliant organizations, the common ingredient is that management at all levels makes it clear that compliance is everyone's responsibility.

◆ **Organizations don't consistently document the evolution of the compliance program, which includes:**

- Evaluation of past efforts,
- Identification of industry challenges,
- Compliance issues noted during internal and external exams, and
- How the program addresses industry challenges.

◆ **Organizations might not accurately identify all laws and rules applicable to each business.** The SEC has made it clear that if an organization adopts a policy or program that includes requirements that aren't aligned with present business activities, the organization will be held accountable. As a starting point, an investment advisor may begin with compliance policies and procedures, which broadly cover all activities permitted by the Investment Advisors Act of 1940. If a firm doesn't conduct an activity, such as contracting for a soft-dollar arrangement, but the policy manual states that these arrangements exist, the SEC will take the view that controls should be designed and implemented in accordance with the policy.

◆ **Organizations frequently don't assign or "link" business/functional units to each policy/procedure nor identify the compliance officer responsible for the policy.** By not identifying the individuals responsible for the compliance activities, organizations may not capitalize on the primary step in delegating responsibility for compliance. Clearly communicating who is responsible for specific compliance activities and ensuring that the responsible parties *are responsible* is a critical factor that contributes to a successfully implemented compliance program. It's also important to distinguish the difference in the responsibilities delegated to the compliance function and the business. Specifically, an effective compliance program dictates that the business is responsible for the control activities that are designed to ensure compliance. The compliance function has an oversight responsibility to monitor the efficacy of the program.

WHAT YOU MUST DO

To ensure that your organization's approach to compliance is effective and cost efficient, you must take a few basic steps:

◆ Develop risk criteria—i.e., how does the organization define "high, medium, and low" risk?

◆ Assign each business activity and its associated policies/procedures a "risk profile" that prioritizes potential compliance risks.

◆ Provide evidence of the approval/adoption of the compliance programs. One example of how an organization can demonstrate that a compliance program has been adopted is in the minutes to a board of directors. A risk assessment will ensure that the compliance program is tailored to your organization's products, operations, and systems capabilities. Such a methodology will also create a level of transparency that allows resources to be spent strategically.

TRAINING AND MONITORING

Becoming compliant is more than putting policies and procedure in place. Truly developing a "culture of compliance" requires leaders who clearly articulate the importance of compliance to the organization and who follow through with in-depth training for everyone. Employees at all levels must understand their responsibilities and how they support the organization's compliance efforts. Training should be an ongoing effort, not just a crash course. Conduct an annual review, self-assessment, and monitoring process. Also develop incentives and disincentives that are linked directly to the compensation system.

A fair amount of regulatory scrutiny has recently been focused on the insurance industry. In fact, an SEC inquiry into two firms resulted in large settlements. On February 10, 2006, American International Group (AIG) agreed to pay $1.6 billion to settle charges that it used misleading accounting to artificially inflate financial results. This settlement is approximately double the settlement Marsh McLennan paid last year for charges of bid rigging. This seems to indicate a trend that the escalation in the settlement amounts being assessed could continue.

Given this current trend, the time has come for compliance to be brought into center court. As Warren Buffett has said, "Berkshire can afford to lose money, even lots of money; it can't afford to lose reputation, even a shred of reputation….There is plenty of money to be made in the center court. There is no need to play around the edges." ■

John Schneider is a director in the Business Advisory & Operations Consulting practice at Navigant Consulting. You can reach him at (617) 748-8317 or jjschneider@navigantconsulting.com.

Risk management is a topic at IMA's Annual Conference June 17-21. For details, visit www.imaconference.org.