Building a Compliance Department

By Sterling Miller

THOMSON REUTERS®

If you work as an in-house lawyer in a large, mature company, odds are good that the company has a well-functioning compliance department. But, if your company is small or newer, there is a good chance this isn't the case. As in-house lawyers, we constantly look for ways to avoid or lessen risk to the company, and a compliance function is an important part of risk reduction at companies of any size. As a result, in-house lawyers should get behind the creation of a compliance group if there isn't one.

A compliance department moves the company from reactive to proactive in detecting and preventing wrongdoing. Besides avoiding trouble, this can lead to substantially reduced fines with regulators who, as a first step, usually zero in on whether the company has a robust compliance program or not. A compliance department also helps establish the right ethical tone at the company, making it easier for employees to make the right choices.

Many companies don't see the value of a compliance function. Others do but they don't know where to start. If your organization is the latter, here are the basics of setting up a compliance department:

Start at the top

The single most important task of any effort to set up a compliance department is obtaining buy-in from the C-Suite, along with the Board of Directors. Both should be especially supportive of setting up this function as regulators are focusing enforcement against executives individually vs. the company generally. Assuming such support, the senior management of the company is an important part of the program, primarily through its support and its actions, and by regularly communicating the importance of compliance to employees. Support from the upper levels is what regulators expect to see. For example, under the U.S. Sentencing Guidelines, credit is given to companies showing, among other things, the following:

- Strong, explicit, and visible support for company's compliance program from the executive team and the Board of Directors
- That the compliance program has sufficient stature and support within the company
- The right culture is fostered at all levels, but especially at the top
- Emphasis on the role compliance plays and the value it brings to the company
- Regular communication of the company's standards and procedures

Perform a compliance audit

Compliance programs are not "one size fits all" – they must be customized to the needs and challenges faced by each company. Some companies may have a relatively simple program, while others have more complex programs. The U.S. Sentencing Guidelines require companies to tailor compliance programs to their specific needs. This means a review of the different compliance risks faced by your company. Ideally, this audit is performed by an independent third party, but not every company has the budget. If not, you can start with using your own internal resources to scope out the relevant issues. Here are a handful of compliance risks companies may face:

- Anti-bribery laws
- Antitrust and competition laws
- Securities law
- Environmental regulations
- Sexual harassment issues
- Cyber-risk
- Government contracting
- Trade sanctions
- Export compliance
- Internal theft

And the list can go on and on, depending on the type of business you operate and its geographic location(s). To conduct a useful audit, interview employees from across the different lines of business and staff groups. As information about compliance risks is collected, create a work plan setting out the risks and different objectives regarding each identified risk, along with timelines/deadlines to complete those objectives. It can seem daunting to start from scratch, especially when conducting this audit on your own. If so, don't try to identify everything right away. Start with your company's biggest compliance risks and address those first. You can embellish the program later after the most immediate issues are dealt with.

Once your compliance department is established, periodic third-party audits of the function and its effectiveness can be very helpful and valuable. They can also provide benchmarking, which is helpful when seeking budget, implementing new policies, or responding to C-Suite or Board questions around "how are we doing?"

Appoint a compliance officer

Someone needs to be responsible for the compliance function, so it's important to appoint a compliance officer. Often, it's the general counsel but it doesn't need to be. In fact, there is a growing debate about whether the legal department should run compliance or not. Regardless of where it sits, the compliance function should have a direct line into the CEO and the Board of Directors, typically through the audit committee. There should be nothing between the compliance officer and reporting issues to the highest authority in the company. Additionally, it is crucial the compliance officer have the staff and resources to do the job properly. It doesn't need to be an empire, but it needs to be appropriate given the size of the company and the range of compliance risks presented. Nothing fails faster or looks worse to an investigator or regulator than an understaffed, underfunded compliance department.

Draft a code of conduct

The most important document for a compliance function is the employee code of conduct (sometimes called a business ethics policy). This document sets out expectations for all employees along with which behaviors and practices will not be tolerated. Your company may already have a code of conduct/ business ethics policy. If there is no compliance department, it is probably overdue for an overhaul and should be number 1 on your to-do list. Likewise, a compliance department needs policies and procedures, including its process for conducting internal investigations and how it will report out results. Preparing a core set of these is number 2 on your to-do list. Finally, the code of conduct and other policies need to be easily available to employees, such as a prominent place on the homepage of the company's intranet and regular reminders of where to find the code and policies.

Coordinate internal teams

A common misperception is that the compliance department is responsible for all compliance. That's not true. As you probably know, many different groups within the company are responsible for various aspects of compliance. For example, HR is responsible for sexual harassment claims, Legal handles antitrust and import/export, IT security handles data privacy and security training, Internal Audit deals with employee theft, and so on. The compliance function handles certain aspects of compliance directly, but often acts as the quarterback of the company's compliance efforts.

In this role, job one is determining whether all areas of company risk are sufficiently covered and, if not, how to incorporate it into the overall compliance program and determine which group is responsible. Job two, then, is to establish regular meetings of the different groups to ensure coordination between them, along with sharing best practices, common issues, and so forth. One of the most important tasks for the compliance officer is to create the right policy to ensure different compliance issues are routed to the right group and there is no duplication of effort or groups operating at cross-purposes. Finally, the compliance officer must ensure a reporting process into the C-Suite and the Board, so they are aware of material issues before they become a public headline. Similarly, the Board will probably want regular reporting of what compliance issues came in and how they were handled. Reporting to the Board is a great place to utilize benchmarks, so they can see how the company compares in terms of number of complaints, type of complaint, and other similar metrics.

Don't forget about international locations

One common mistake when it comes to compliance issues is forgetting about foreign locations. There are a few considerations needed to ensure compliance with international offices. First, if you have foreign locations, you need to translate your code of conduct, training, and other materials into the primary language of those locations if not the same as headquarters. It is difficult to convince a regulator you have an effective in-country compliance program if it is available in only one language – and it's not the native language of those employees. Second, get input from your foreign offices about how effective the policies and training are, and if there are any local compliance issues not properly covered by the main policies and procedures. Don't assume the only compliance risks are those you can identify at headquarters. Third, find ways to underscore the importance of compliance at remote

offices. Don't miss any opportunity to appear live. Finally, be sensitive to cultural differences when it comes to compliance. In some cultures, whistleblowers are viewed poorly, so relying on them to come forward presents challenges. Likewise, in Europe, many countries do not permit the use of anonymous "hotlines" and that needs to be factored into your program as well.

Focus on training

Having a code of conduct is great, but it's useless unless all employees are trained on it, including executives and the Board. Consequently, a robust training program is a must. Most training today is done online, but don't pass up an opportunity to conduct live training. Online is fine, so long as the training is tailored to your company's specific needs and risks, and is refreshed regularly. Where possible, make training fun. The gamification of compliance training is growing and is especially effective in terms of ensuring employees take the training and retain the information. One thing to always keep in mind with training is keeping it simple. Complex legal concepts are lost on the employee base. Go for big issues, in easy-to-understand language and examples. Save the law school exam-level training for your legal team. When training employees, ensure there is emphasis on the spirit of the law as much as there is on the letter of the law. Employees should understand the company wants them to do the right thing and compliance makes the company better and keeps it from getting entangled in lawsuits or regulatory actions.

One tough problem you might face is the group of employees who won't get around to completing the training. Here are a few ideas for troubleshooting:

- Ensure all the senior leadership team has completed the training. You can tell the recalcitrant employees they cannot be busier than the C-Suite, which found time to complete the training.
- Give the group a short but reasonable amount of time to get the training completed, e.g., 10 business days. Inform them that failure to complete it by the deadline means their access to company systems will be suspended.
- If they still fail to complete it by this deadline, give them one day with the note that if they fail to complete it then, they will be ineligible for any discretionary bonus payment.

Make reporting easy

Crucial to any compliance program is ensuring employees understand when they need to report something and how to do so. The code of conduct should contain a section describing all the ways employees can raise issues, including a toll-free hotline, a monitored compliance email address, their manager, the general counsel, the head of HR, and so forth. Focus on making it as easy as you can for employees to raise issues. It may seem like you are setting yourself up for a lot of work, but it is far better to have employees raise issues than to have those problems buried until it's too late. It is equally important the company have and enforce a no retaliation policy and make sure every employee knows there will be no retaliation for bringing forth a good-faith issue. Likewise, ensure there is a general policy around ensuring confidentiality for both the person bringing the complaint and any employees implicated by a complaint.

Lock down internal investigations

When a complaint comes in, there should already be a preset process for how it will be investigated. It should be assigned to the right department, and procedures should be in place to guide how the investigation will proceed, establish the expected timeline, and create interview reports and other documentation so there is a consistent "look and feel" to all the company's investigations. There should be a mechanism to report back to the person raising the issue, so they know the company took the complaint seriously and investigated. Finally, there must be consistent punishment for any employee found in violation of the code of conduct, including executives. If there are different outcomes for different employees, there will be little faith in the process. Lack of faith in the compliance process is deadly.

Setting up a compliance department is a tough job. But the alternative is very risky. If you can get the support of top executives and the Board, including the appropriate amount of funding and people, you can build a viable compliance team in a relatively short time. The basic building blocks are straightforward. The keys are understanding the compliance risk profile of the company, creating the right policies and procedures, and ensuring any complaints are properly investigated and dealt with. If your company needs such a function, now is the time to get the issue in front of the decision makers. A *proactive* legal department is a *valuable* legal department.

About the Author

Sterling Miller has spent almost 25 years as an in-house lawyer, including three stints as general counsel. He is certified by the IAPP (CIPP/US). You can read his award-nominated blog "Ten Things You Need to Know as In-House Counsel" at www.TenThings.net and follow his regular posts on LinkedIn or Twitter @10ThingsLegal. His second book, *Ten Things You Need to Know as In-House Counsel: Practical Advice and Successful Strategies,* was published by the American Bar Association in 2017.