COSMOS
Navigate the Compliance Universe

Compliance Today - January 2023

Amy B. Boring (aboring@kslaw.com) is Partner at King & Spalding LLP, Atlanta, GA.

Stephen P. Cummings (scummings@kslaw.com) is Counsel at King & Spalding LLP, Atlanta, GA.

The importance of a robust third-party compliance program

By Amy B. Boring and Stephen P. Cummings

Each year, companies devote vast financial, technical, and staffing resources to implement and maintain effective corporate compliance programs. Generally, an effective compliance program has seven essential elements, including standards, policies, and procedures; compliance program administration; screening and evaluation of employees, vendors, and other agents; communication, education, and training; monitoring, auditing, and reporting; discipline for noncompliance; and investigations and remedial measures.[1] For example, American hospitals spend almost $39 billion annually on regulatory compliance activities.[2] Understandably, most compliance work is focused on a company's internal business operations, including ensuring that the company's employees are familiar with applicable policies and procedures; receive regular training; know how to report compliance concerns; and that there is a process in place to investigate and resolve compliance concerns and complaints.

But increasingly, companies are turning their compliance focus to include a more robust examination of a company's third-party vendor relationships because there is growing recognition that third-party vendors can introduce significant compliance risk into a company's business environment. This renewed focus is reasonable considering the increased interest regulators are showing concerning third-party relationships. Indeed, the U.S. Department of Justice has issued explicit guidance that called out third-party management as an essential feature of a well-designed corporate compliance program.[3] Therefore, it is important that companies take steps to ensure that their existing compliance programs comport with the current guidance for what constitutes an effective third-party compliance program.

The third-party vendor relationship life cycle

Without question, third-party vendors are vital in many companies' business operations, but using third parties also creates substantial regulatory and enforcement risks. As such, it is imperative that a company compliance program includes an effective process to manage and mitigate potential third-party vendor risks.

An essential first step in the creation and implementation of a third-party compliance program is identifying all third parties that need to be included in the compliance process, which consists of all third parties that touch any aspect of a company's business environment—both upstream and downstream with respect to sales, products, personnel, and services. The next step in the process is the development of a program that addresses all facets of a third-party vendor relationship, which includes:

- Business rationale or justification
- Risk-based vendor due diligence

- Contracting to limit the risk of vendor noncompliance
- Onboarding
- Monitoring and auditing of vendor compliance
- Concluding the relationship

Business justification

The initial phase of the third-party vendor relationship life cycle is to have a defined process for determining when there is an actual business need to engage a third-party vendor. The process should, at a minimum, include the purpose of the vendor, who requested the vendor, who approved the hiring of a vendor, and the creation of a file where the information pertaining to the other vendor life cycles is collected and maintained.

The importance of knowing whom you are doing business with

The second phase of the life cycle ensures the company knows who it proposes to do business with by conducting risk-based diligence. A risk-based approach to diligence is crucial because not all vendors require the same amount of due diligence. In implementing a risk-based approach, a company should have a defined process to evaluate what level of diligence is required for each vendor type.

For example, if a hospital hires a vendor to supply paper for copy machines, this business activity appears to involve minimal compliance risks, so a lower level of diligence is likely appropriate. In contrast, if a hospital engages a vendor to manage its electronic health records, the potential compliance risks associated with this business activity are substantial, so a much more vigorous diligence process is required.

One potential challenge in knowing your business partner is that if potential red flags are identified during the diligence process, these flags must be resolved and documented to avoid a situation where a regulator second-guesses the decision to engage a particular vendor. Another challenge is maintaining the historical diligence file so that a company can demonstrate the reasonableness of its diligence process after the fact. There are also circumstances where postcontractual diligence may be appropriate, especially when a vendor has access to highly sensitive information or in the cases of long-term contracts where it may be years before a vendor undergoes another diligence review.

Contracting to limit risk

The third phase in the life cycle is using contracts with regulatory compliance standards to mitigate potential third-party vendor risks. Indeed, depending on the nature of the business activity, it may be advisable to adopt specific regulations or legal standards in the contract. For instance, in the hospital example relating to electronic healthcare records, it may be advisable to have contractual provisions that explicitly address compliance with HIPAA, confidentiality, privacy, and cybersecurity. Another way that a company can seek to limit its risk is by including contractual provisions that require a third-party vendor to use written policies and procedures, conduct regular compliance training, maintain a compliance program, and report compliance violations.

Suitable onboarding

The fourth phase is the use of an onboarding process that clearly spells out compliance expectations and requirements. The amount of onboarding will vary depending on the third party's business activity; however, it can include acknowledgment of receipt and review of applicable policies and procedures, initial and annual

training requirements, and familiarization with compliance reporting requirements. The last point is particularly significant because it is not uncommon for third-party vendors to be unfamiliar with how to report compliance concerns in a timely manner and/or to the appropriate persons.

Monitoring and enforcement

The fifth phase—and the single best way to mitigate the risk associated with third-party vendors—is to adopt a comprehensive monitoring process to ensure that the vendors comply with all applicable contractual provisions and legal obligations. But monitoring by itself is not enough. A company must also have a process for reviewing and resolving any potential red flags identified during the monitoring process. This includes making sure the investigation is documented, including documentation for why an event is not a compliance risk. Moreover, compliance violations must be remediated, and where appropriate corrective action should be taken and documented. Additionally, if there is a pattern or practice of violations, the company should take steps to address any systemic deficiencies, which may include additional training, modifications of policies and procedures, or additional monitoring/auditing.

Concluding the relationship

Once a third-party vendor relationship ends, this should be noted, and the appropriate records retention policy should maintain all relevant files. In addition, there should be a process to ensure that the vendor no longer has access to confidential business information and that it returns all company property and information. For example, when a vendor's contract expires, access to the company's business offices and network should be terminated immediately and all property and information belonging to the company that is in the vendor's possession should be returned.