Supply Side

Making vendor risk assessment an organizational priority

Establishing an effective program for contracting with and monitoring service providers can be a means of fortifying risk management initiatives, especially for companies that face significant regulatory oversight, cybersecurity, and privacy concerns. ***Jerry Ravi*** *and* ***Lena Licata*** *of* ***EisnerAmper LLP*** *discuss vendor risk management programs that help companies thrive within the boundaries of sound and practical risk management policies.*

Vendor risk management (VRM) is defined as the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance.

MCC: What are the key considerations when establishing a vendor risk program?

Licata: First you need to identify the company's full population of vendors, including what they do and how the contracting process works: Is it handled centrally, or can each business unit contract on its own? Who are your advocates in this process? Will legal be responsible for knowing the program parameters and distributing a list of reviewed, embedded vendors, or is accounts payable ensuring that vendors are fully vetted before money goes out the door?

Ravi: These questions arise frequently in our work with highly regulatory companies such as financial services, insurance, and life science companies. In our role as risk managers, we take a phased approach in assessing each vendor's risk profile, which begins before decisions are made to contract with the vendor. Typically, we recommend classifying vendors in tiers. For example, tier-one vendors carry the greatest risk due to their access to higher-risk data and the potential to disrupt a company's operations.

Licata: Data mapping is a critical part of the process. Here, we look at what vendors are doing with that data. Are they just storing it or passing it on to sub-vendors? Is data located only in U.S. territories, or will EU safe-harbor issues be implicated? Once mapping is complete, the next step is to generate a list of approximately 10 quick questions to establish each vendor's risk ranking, and all subsequent action is based on that process.

Ravi: And to complete the process, companies need to implement monitoring programs that comprehend the various risk tiers and establish appropriate controls. Obviously, the higher-risk vendors get more monitoring. Internal controls need to be assessed to ensure service levels and expectations are met.

MCC: For companies that haven't yet paid attention to this process, what's your advice for making the most intelligent start, and what realities do they face right out of the gate?

Licata: We advise starting from both ends of the spectrum. On one side, confer with IT to understand data locations and flow, and then with the business folks to understand what is the *critical* data within the organization, after which the data mapping process can begin. On the flip side, ask your accounting people to identify your payees and which business unit needs the service. From here, we suggest developing a company-specific questionnaire for the purpose of risk ranking vendors.

Strategically, you don't want a massive program that takes years to complete. You want to start by chipping away at it in blocks: phase 1, data map; phase 2, determine the population of vendors; phase 3, questionnaire them; and phase 4, place them in a program.

Ravi: As far as reality is concerned, let's face it: Outsourcing is now the norm. It's happening in every industry, and start-ups are certainly going down that path more often because it's cost-effective and allows them to be nimble. As it stands for many companies, employees are signing contracts and bringing in rogue vendors without ensuring that all the legal elements – such as the rights to audit and get your data back – are in place. Legal has to be involved in the contracting process, but is often neglected.

In my experience, some companies face a difficult reality just in trying to figure out who they work with. The risk-based approach that Lena described can simplify that process and enable organizations to determine where to focus attention in protecting their crown jewels, meaning their most important data. By following data, you can follow vendors that are touching it, vet them properly and put them in a program.

Let's face it, outsourcing is the norm now.

MCC: You mentioned IT, legal and audit as vital functions involved in a vendor risk program, but who within an organization should spearhead this process?

Licata: It might be the CFO or CIO, and sometimes leadership comes directly from the CEO, depending on the size of the company. Because vendor risk programs permeate the entire organization, they tend to be treated as a separate function assigned to a dedicated person. In fact, one major challenge in launching a project like this is that no single department wants to own it. Certainly, a company can hire an external party like EisnerAmper to get it up and running, but the ongoing program does end up being an internal person's job.

Ravi: It's very similar to an enterprise risk management (ERM) or any other compliance program. Everybody is involved, but someone needs to own and assist with monitoring the process. This can often fall to legal, the CFO or CIO, but new programs have to start with someone at the top. From there, vendor risk management can flow into the enterprise risk management structure.

MCC: How does vendor risk assessment tie in with regulatory compliance?

Licata: A good regulatory compliance program simplifies vendor risk management programs. Having strong policies helps in formulating a vendor risk questionnaire because you already know what controls are important to your organization, and you can tie specific controls to those policies.

Ravi: There are alternatives, such as using a standard information-gathering questionnaire (SIG), and there's even a SIG-light that comes out of the BITS Shared Assessment Program. But if you already have a compliance program, the vendor program essentially becomes an add-on that can be managed efficiently with existing resources.

For example, a vendor working with a client in the healthcare industry will have to be prepared to answer all questions about data privacy, including policies around incident response – an area where many companies fall down in vendor assessment. When something happens, companies need to have an established plan with each vendor. How do I engage them? What if something actually happened on their side? Are we holding them accountable for letting us know?

MCC: After the questionnaire is completed, what do you do with the information?

Licata: You look at it and decide what matters most. No company is perfect, so this process is about developing action plans and remediation plans with individual vendors to clear up issues, set time frames and stay on top of efforts to strengthen a vendor's control environment – really as a condition of a continuing relationship. The legal component is crucial because if you have no standing on the right to audit, you may find yourself stuck with a 10-year contract for services when you would rather go with another vendor that has a more secure environment. It's important to understand these

Jerry Ravi
Partner in the Consulting Services Group of EisnerAmper LLP.
jerry.ravi@eisneramper.com

Lena Licata
Senior manager at EisnerAmper LLP.
lena.licata@eisneramper.com

issues from a legal standpoint and build certain controls and conditions into the contract.

Some vendors will be more receptive than others to a company's remediation demands following a risk assessment, but companies that make the up-front effort and then monitor the outcome will face fewer issues going forward. This is notably true on the regulatory side, where you might find yourself facing questions such as: What did you do to fix this problem? Answering those questions can be a cumbersome job, especially when tracking a roster of 50 or more vendors, all with different issues and remediation schedules, but it's also where you can derive value from a vendor risk program that includes a solid monitoring process.

Strengthening its control environment should be a condition of a vendor's continuing relationship.

MCC: Talk about the value-add in bringing in a firm like EisnerAmper that already knows how to turn this situation around for companies.

Licata: At the beginning stages, hiring an external firm will draw attention to a project that internal people who have a daily job to do may not want to focus on. As an independent party, we can more easily bring departments together, facilitate vendor reviews and do the initial program setup – and yes, experience counts in making that process efficient and well-conceived. Often, we will get a program off the ground and then hand the reins back to the client. Once vendors are on board, it's a repeatable and fairly stable process.

Ravi: Other times, we help clients through the entire vendor risk management lifecycle, which includes onboarding of new vendors, handling the due diligence and making sure that selection is done with the right risk mind-set. There are a number of documentation and reporting elements there. Once vendors are on board and monitoring is in place, we get involved in oversight, making sure there's accountability and doing an independent review. If we have to go on site, that's not a problem, and we can look at other assurance reports to get comfort that appropriate controls are in place.

In a world where business happens in the cloud, these oversight capabilities are a big value-add, and companies are asking for help through the entire lifecycle so they can hire the right vendors and make sure they're meeting strategic objectives, especially in high-risk situations. Imagine the importance of supply chain vendors to a pharmaceutical company or a contract manufacturer. They are the lifeblood of those companies, so it's simply critical to have operational excellence from each vendor.

MCC: When you step into a company and think about enterprise risk, can vendor risks uncover larger issues?

Ravi: We work under the umbrella of enterprise risk management, and the goal is to make decisions that facilitate success on the business side within the parameters of a company's risk mitigation strategy. That's really what a vendor risk program is designed to do, and you certainly can derive larger benefits from the process of exposing and managing risk in this context.

If we are talking with a company about where they're headed – let's say they want to double in size over the next 18 months – there's a lot of risk that comes with that. If they're looking for funding, we will look broadly at reputational risk and then peel it back to see how far its tentacles reach within the organization. We may look at the data mapping and cyber risk, or we may make sure the company's financial reporting is sound, especially if it is being shared with investors.

In the broadest sense, we are setting up a company to be prepared for any risk. That's the overarching enterprise risk management approach: Establishing a context, creating a program, and eventually looking at it from the standpoint of risk that needs to be monitored going forward. We may not look at every single risk, frankly because it's cost prohibitive and we're looking to create value, but we will look at everything in terms of operational risk, and we will assess performance via metrics and monitoring toward achieving the company's strategic goals. In that sense, we're embedded within the organization, and that's where the real value is gained.

In-House Teams

Continued from page 43

In the future, we may have third parties who hold survey data, at the very least, or certify that the data is as represented by the survey report. More than that, someone might run some simple calculations to see if the date is clean and has been analyzed reasonably (e.g., if data is missing, it is not a zero!). Data reproducibility should not be confused with an assessment of whether the quantitative analytics are smart or dumb, comprehensive or partial, or useful in the real world or not. It simply verifies that the collection and preparation of the data can be matched step for step so that the results can be corroborated.

All of us who care about the contribution data can make to legal managers and their decisions should push for standards of data reproducibility in industry surveys.

To take the no-cost survey, use this link: https://novisurvey.net/ns/n/GCMetrics2015.aspx.