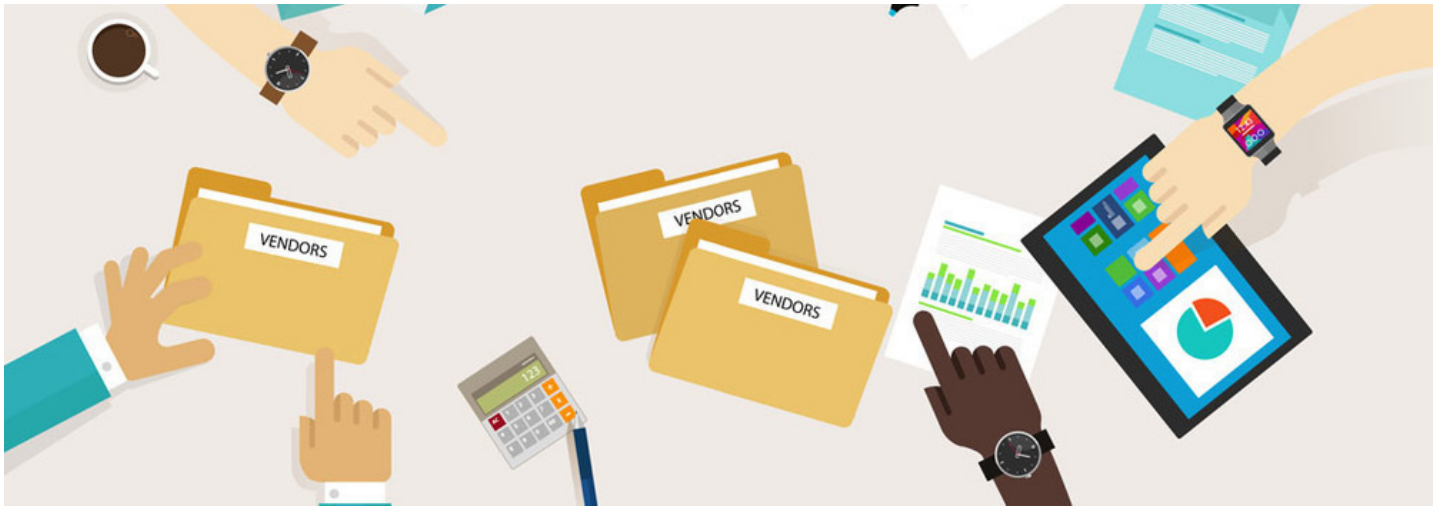
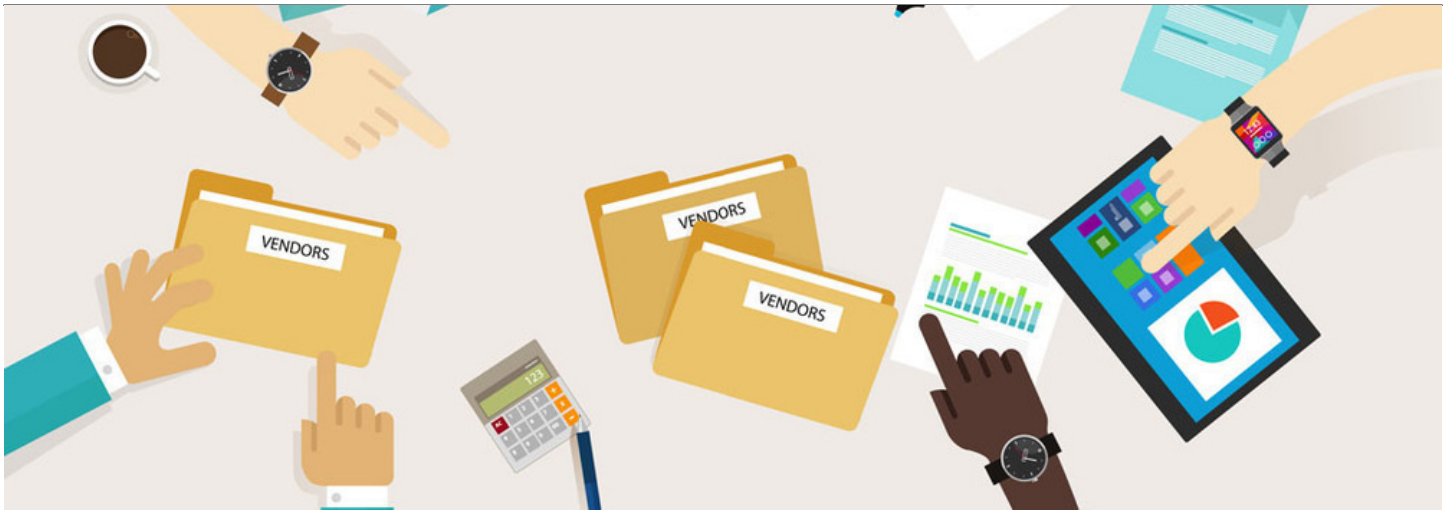
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# How to Build the Vendor Oversight Program of Your Dreams

## Commercial and Contracts






Vendor management is a topic that does not grow stale, given the scope of oversight now required under a variety of laws. The way in which organizations manage their vendors can become quickly outdated. Whether the oversight is specifically related to your industry and rules that target your risks, such as the US Health Insurance Portability and Accountability Act (along with subsequent amendments, HIPAA), or applies to all organizations engaged in certain activities like doing business in foreign countries or managing personal information, the expectations for organizations are gaining in both scope and strength. Enforcements, too, are growing.

Implementing a vendor oversight program that is appropriate for your organization is critical. There are several considerations that factor into setting up your program, similar to building a house. Do you have a set of plans? Did you engage an architect who approved your plan? You need a solid foundation, a framework that fits both function and form, a well-positioned structure that covers it all, and the internal and external components that make it comfortable and appealing, along with providing safety and security. The analogy isn't perfect, but it works.

## Preparation

Before building, invest time in your preparation; rework is time-consuming and expensive. Determine why you are building a vendor oversight program. Is it because of laws that require it or clients demand it? Is it the significant risk that outsourcing incurs? No matter the reason, an oversight program that is properly designed and evaluated before the construction starts is the best way to satisfy the various compliance drivers.

Privacy-by-design (PbD) begins in this phase. PbD is not an add-on or an afterthought similar to adding six-foot walls and razor-wire to the perimeter once the building is complete. First, those are security, not privacy controls (although security is instrumental in achieving privacy, it should be in the initial design, not merely added later). Second, PbD assists in building properly. PbD will identify if you are building in the right location, have the proper permits, and identify how to build the structure to maximize capabilities and minimize loss. Of course, like building inspectors, you should also have your privacy officer or data protection officer verify that all is being built to specification, and bring her in to inspect each step as you progress. It is astounding how quickly the scope of the project changes beyond the original intent as you involve key stakeholders.

## Foundation

The foundation of a successful vendor oversight program should be built on drivers for compliance and risk tolerance. Drivers for compliance comprise contractual obligations and requests, laws and regulations, and risk from outsourcing. It is typical for an organization to only consider one aspect of this when first building their program, but consider the totality of the compliance needs that exist. Contractual obligations are mandatory, but also consider lost opportunities or where contracts are stalled in negotiations over vendor issues.

Certainly the laws are critical, but also consider enforcement actions and court decisions. Assess settlement decrees, if available, to determine what factors sway the decision-makers. Evaluate the thresholds where laws might apply to identify what may drive the next level of compliance. For example, if the California Consumer Privacy Act (current predecessor to the California Privacy Rights Act that was voted in as a ballot initiative in November), has one threshold for applicability of US$25 million in revenue and you are below that threshold, but close to it, consider including California's requirements into your foundation.

Lastly, in the foundation, include your risk tolerance. This is driven by industry, activity level, publicly held vs. private, years of being in business, board of directors, and a variety of other factors that may be unique to your organization. Risk appetite and tolerance drive a significant amount of the compliance level of the organization and it is not unusual to have varying levels among departments, locations, or subsidiaries. Risk must also be considered within the cultural setting, which may also drive variations across the organization. The key is knowing the variations and drivers and laying a foundation that accommodates those.



## Framework and roof

Building a frame may be accomplished by a team of people working collaboratively, like in the days of yore, when communities came together to raise a barn. Unfortunately, in a commercial organization, determining one framework may be a challenge. Each functional department has both their priorities and their compliance needs.

The foundational decisions you made in the prior section may blend seamlessly with determining a framework and many of the same considerations apply, such as compliance drivers and risk tolerance. This is where a decision needs to be made to manage the vendor oversight through a centralized or decentralized manner — or perhaps a hybrid of the two works well. Some compliance needs naturally fit within certain departments. In the United States, compliance with Sarbanes-Oxley falls to the finance and legal departments and would not fit comfortably within the privacy department. Likewise, compliance with the UK Bribery Act might not be a good fit for the facilities department.

In the privacy and security space, there is often a decision to be made on adopting a voluntary set of requirements, such as NIST (US National Institute of Standards and Technology) or ISO (International Organization for Standardization). Deciding what voluntary standards to follow is akin to deciding whether to use the metric system or the imperial system. The critical consideration is

whether everyone knows what system is being used. Is there a common language, and does everyone involved understand the expectations? Your processes should be clearly defined and personnel should be able to repeat them. It is important to adopt a set of standards that defines processes and expectations. Standards breed consistency. And consistency breeds compliance.

Thus, you need to identify the compliance needs across the organization and determine how compliance is managed on a daily basis. Even an appointed compliance officer may not be directly responsible for all compliance needs. However, that person might be accountable for all compliance needs. Responsibility can be shared. Responsibility is largely task-oriented. Accountability, on the other hand, is having ownership of results and should be intentional. Accountability without authority is ineffective. It may help to engage in a RACI (Responsible, Accountable, Consulted, Informed) or DACI (Driver, Approver, Contributor, Informed) process. An effective vendor oversight program is reliant on an effective compliance program. This is the framework of authority, accountability, and responsibility.

## Internal and External Elements

Until now, this article has focused on risk and compliance. What does this have to do with vendor management? It's because risk and compliance drive outsourcing and oversight. Although there may be some truth to the adages "doctors make the worst patients" or "plumbers have leaky pipes," that approach cannot work for vendor oversight. Organizations must have a solid compliance program that identifies the compliance needs, the risk tolerance, and a management system, whether centralized or decentralized.

The vendor oversight program sits on top of the compliance program, like a roof. And homeowners know a leaky roof leads to all sorts of other problems. How the vendor oversight program functions, with triggers and thresholds for contract review, are key measures that must be bespoke for the organization. The vendor oversight program must fit the company's culture, needs, and growth. It must be effective, efficient, and scalable. Vendor oversight is not something that you just throw over the wall and hope it lands right-side-up. It is an integral part of a successful compliance program and should be integrated into the foundational components, the structural execution, and every person in the organization should understand their responsibilities. This is what makes the vendor oversight program part of the home — it's not too big and not too small. It's just right.

Make the program appealing. Be transparent and proud of the measures that are put in place. Show it off! This is a program that should be well known and discussed throughout the organization. Make sure to add the security features that were mentioned at the beginning. If your risk considerations are minimal, as long as it matches your needs, you have a program to be proud of and to maintain. If the organization requires a more complex program, then make sure the right tools for maintenance are available. One person cleaning a skyscraper with a broom and mop is not effective or sustainable. Keep your compliance house clean and secure, right-sized, and legal.

## In conclusion

Location. Location. Location. That is the driving mantra for real estate and it works for oversight. Make sure you focus your efforts where they are most needed. Make sure you are monitoring the right places and keep an eye on any changes in your environment. Know where you are now. Know where you want to go. Know how to best get there. Build it right. Build it strong. You can bedazzle a shack, but it's still a shack.

## K Royal



Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.