PROCESS UNITY

BUILDING BETTER VENDOR RISK ASSESSMENTS

INCREASING THE QUALITY & EFFICIENCY OF YOUR VENDOR RISK PROGRAM

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655

BUILDING BETTER ASSESSMENTS

This white paper is the fourth in a series about creating an effective vendor risk management program. Previous installments include:

- **Part I:** Four Keys to Creating a Vendor Risk Management Program that Works
- **Part II:** Identifying Vendor Risk: The Critical First Step in Creating an Effective Vendor Risk Management Program
- **Part III:** The Vendor Manager's Guide to Risk Reduction

INTRODUCTION

Creating an enterprise-wide vendor risk management (VRM) program from scratch is a challenge that daunts many risk management professionals. If you're lucky, you get to start with an accurate list of vendors and strong executive sponsorship. More than likely, however, you will start with an outdated list of vendors and will have to build a business case for funding the program. Either way, staring at blank pages that have to become the policies, processes, procedures, and standards for your VRM program can be overwhelming.

Empowered with the executive sponsorship and the funding to make a go of it, in the first year of your VRM program you'll likely:

- Inventory and categorize your vendors to understand the risks inherent with your vendor portfolio
- Develop and communicate expected controls standards for your vendors
- Develop methods of assessment (commonly questionnaire-based) to assess vendors' controls
- Assess your critical vendors
- Manage the remediation of any issues identified during the assessments

This can be a lot of work but, with diligence and focus, it's completely achievable. After that first year, you should have some knowledge of what worked well with your process, and what didn't. At this point you can put your assessment methodology into a continuous improvement cycle.

You will want to reevaluate what you are doing and consider how you can improve the process in order to gain an even better understanding of your vendors and the risks they might pose to your business. A regular review of your assessment process also provides the opportunity to incorporate any new regulatory expectations into your vendor assessments.

How do you build better assessments as your VRM program matures? To improve your VRM program, you should evaluate these four elements:

- **Quality**—How did you perform against your objectives during the previous year? How can you improve the consistency of your program and other aspects of what you're already doing? What are the lessons learned?
- **Alignment**—Is your VRM program aligned with your business and its regulatory requirements? Have you taken into consideration changes in your business and new regulatory guidance?
- **Veracity**—Are you testing controls in a way that makes sense and is efficient? Are you sufficiently testing where the control execution risk lies? Or, are you burning cycles with ineffective or unnecessary testing?
- **Efficiency**—When assessing the above three areas, it's easy to fall prey to scope creep. Are you doing what's required to keep the program within your resource constraints while maximizing the usefulness of those resources?

By addressing these areas, you can develop a more thorough and effective assessment process.

QUALITY: RESOURCE ALLOCATION, EFFECTIVE COMMUNICATION, REPRODUCIBILITY, AND THE CASE FOR CENTRALIZED MANAGEMENT

Whether you've just finished running your VRM program for the first year or the fifth, it's time to look back and reflect on what could have been better. One of the more difficult things to do, particularly in the first year, is match the scope of your assessment methodology to your available resources. There are two fundamental questions you should ask yourself:

- "Were we able to assess all of the vendors we wanted to assess?"
- "Were we able to manage the remediation of all of the issues identified by those assessments?"

If you were too ambitious, your answer to one or both of these questions may be, "no." It can be easy to get bogged down as you work to help vendors understand the initiative, wait for responses, and clarify your questions. Assessing fewer vendors than intended isn't really all that bad; it's a normal growing pain. But, it does help identify where you might need to be more efficient: can you clarify your communications with your vendors, can you better train your assessors, should you do fewer site visits, or should you re-visit vendor criticality and prioritization?

As we discussed in detail in The Vendor Manager's Guide to Risk Reduction [download], the real danger can be under-resourcing your remediation management. If you don't work with your vendors to resolve the issues identified during their assessments, the very investment in those assessments is marginalized.

You may actually reduce more risk by attempting fewer or smaller assessments and ensuring that the issues identified are resolved. Remember – your goal is to reduce risk. Balancing vendor coverage, assessment scope, and remediation management to resolve the most and highest risk issues is what matters.

Once you've looked at the alignment between the scope of your program and your resources, the next question you should ask yourself is, "Does my assessment methodology effectively address the risks I intend for it to address?" In other words, do my vendors understand the questions I'm asking AND do their responses make sense? Take a moment and look at the places where you've asked a question but consistently gotten answers on a different topic. For example:

"What wireless security features do you use?"

Without a doubt, the author of this question knows exactly what they're asking. But, does the respondent? Is this a question about wireless computer networks or mobile telephones? Regardless of how carefully you develop your questionnaire, you'll invariably have a few questions that are ambiguous or confusing. Paying attention to the responses you receive throughout the year will help you identify and improve these questions. Getting well-aligned, clean responses to your questionnaire will improve not only the accuracy of your results but your efficiency as well.

Similarly, if you're rating your vendors or scoring their responses, do those scores make sense? As you look at the risk ratings assigned to issues identified, do the high risk findings truly pose more risk than the medium risk findings? This may seem inconsequential but if your goal is to reduce the most risk with the resources you have and if your methodology calls for prioritization based on these scores, then getting this right is critical to the overall effectiveness of your program.

Once you're happy with your assessments on an individual basis, the next question to ask is, "Am I consistent from assessment to assessment?" Inconsistent results can be an indication that your VRM program needs tighter processes and procedures. In addition, it can also mean that your assessment team, which will inherently include professionals with different backgrounds and levels of experience, may need more orientation or training on the program. Driving toward consistency is key because it assures a minimum standard for the assessment work and gives you a baseline for program improvement. These, in turn, give you the ability to reliably compare and contrast vendors.

VRM programs often begin within existing centers-of-excellence within an organization. For example, it is common for information security departments to develop third party information risk assessment methodologies. However, it is not always a natural fit once the VRM program is fully operationalized. By transferring the responsibility for third-party risk assessments to a group such as the procurement department or a vendor management department, the VRM program can be more tightly aligned with other activities central to the management of vendor relationships - such as managing service level agreements (SLAs), insurance and bonding, and invoice accuracy. This type of centralization often brings VRM out of disparate business units into a centralized function which, in turn, reduces overlapping efforts and improves consistency.

You can also use process automation tools to boost the quality of your assessments. Clear management reports and well-designed workflow systems are essential for ensur-

1. If your VRM program includes scoring models for vendor criticality, inherent risk, and issue severity, as it should, you'll want to appropriately validate these models, particularly when rolling up this information for enterprise-wide reporting.

ing consistent, reproducible results across assessments. Furthermore, automated vendor risk management tools can generate the reports necessary for management to monitor the VRM program, to enable accountability to business constituents and auditors, and for model risk management activities.[1] More importantly, your VRM solution can give risk managers a clear picture of the third-party risk to your organization and track open issues.

ALIGNMENT: TAILOR YOUR VENDOR ASSESSMENTS TO YOUR BUSINESS NEEDS

Business needs can change over time. In a first-year VRM program, the goal is usually just to get some number of assessments done in order to determine where you stand with your vendors and find and remove some risk along the way. These initial assessments tend to fall into one of three groups:

- Ad-hoc – where you don't have formal criteria of any kind
- Standards-based – for example basing an information security assessment on ISO 27002
- Extended enterprise – where you attempt to compare your vendors to your own internal standards

None of these approaches is ideal but, of the three, standards-based assessments and the extended enterprise assessments are preferred. From there the questions you should ask are:

- Do the standards I've chosen match the needs of my particular business?
- Which of my internal controls also apply to my vendors?
- Does the scope of the assessment capture the regulatory requirements applicable to my vendors?
- Have I addressed the areas of risk unique to my vendor relationships?

This is, in essence, a requirements review and a gap analysis between those requirements and your assessment program.

When in doubt, use industry standards as a starting point; they help make sure you don't forget the fundamentals. For information security, ISO 27002 with its 114 controls is an excellent start. Other standards provide equally sound starting points for the industries and risks they address. If you haven't already done so, build your assessment questionnaires and methodologies from these materials.

Next, tackle your regulatory obligations. These are the must-dos of your industry so you should address them up front. Map the questions in your assessment to what your regulations expect from your vendors. If you're a financial services firm subject to GLBA, you'll want to refer to the FFIEC handbook, OCC guidance, and similar publications. If you're in healthcare, you'll want to refer to the HIPAA Security Standards Matrix.[2] Regardless of your particular regulatory burden, the concept is simple.

Make sure you know how your questionnaire and assessment address the regulatory obligations and, if any regulatory obligations aren't addressed, extend your assessment and ask those questions of your vendors too.

It is important to consider the difference between how you should approach assessments and how you should approach compliance. The assessment is how you collect information from your vendors and form opinions about that information. With your assessment completed, you can evaluate your state of compliance by using the relationship between your assessment materials and your regulatory requirements as a framework for evaluating the regulatory implications of your findings. Starting with regulations and going the other way is impractical because regulations are narrowly scoped and not intended as frameworks for building security programs or any other kind of program for that matter.

2. Appendix A to Subpart C of Part 164 of the US CFR

Once your regulatory requirements are addressed, you can use your discretion to make sure your vendor assessment program meets your particular risk management needs. What's changed about your business that may impact what you expect from your vendors? Do you have any risks that aren't addressed by your regulations-enhanced, standards-based methodology? Are there any hot topics within your organization that you want to make sure you address with your vendors? If any of this is missing, now is the time to add it. This is not to say that you want to assess your vendors in the same way that you do your own internal controls assessment. In fact, much of what you do internally may not be applicable to outside organizations, no matter how critical those organizations may be to your business. Instead, only borrow from your internal risk management programs those things that truly apply to your vendors.

After reviewing and incorporating so much content to the scope of your assessment, now is the time to consider which information to cut in order to make your assessment more concise. If there are any questions in your assessment that don't directly relate to a regulatory or business requirement, you should drop them. They may be good ideas, but if they don't apply to your vendors or the work they do for you, answering them only adds time and unnecessary expense.

Now look at what you have left. Do you have the resources to manage such an assessment? If not, cut some more. Cut the questions that map to low impact risks. Cut the questions that go deeper into the details than is really required. If necessary review these decisions with your regulators. What you have left should meet your business and regulatory needs while focusing your resources on the areas of highest risk. And, because you've conducted a proper requirements analysis along the way (and documented the tough decisions you've had to make) you can defend your methodology against critics and make educated adjustments in the future.

VERACITY: SAMPLE CONTROLS THAT AFFECT YOUR CORE BUSINESS

You've sent your questionnaire to a vendor and they've replied, "Yes, we do these things." This sounds good but, how do you know? This is where the sampling of evidence comes in. If you're like most organizations, you ask for copies of policies and other things that are supposed to provide the proof. Policy conveys the intent of management, but it doesn't guarantee a vendor is actually following the policy and doing the work. Receiving policy documents as evidence is certainly one kind of sampling – but it only samples whether the vendor has a policy. If, instead, you want to know if the vendor actually performs the controls required by those policies, you have to sample evidence of the actual control performance, for example screen shots showing antivirus software enabled and running is more convincing than a copy of an antivirus policy. Since it can be prohibitively expensive to sample all of a vendor's controls, you should sample only those controls that matter the most to your business.

For example, if you are concerned about data security, you can test small statistical samples on controls such as system hardening, patching, application security, and antivirus protection, in order to verify that these actions are really being performed as required by policy. Correctly testing a small number of key controls provides a much better indication of managed risk than a comprehensive analysis of a vendor's policies.

Another method to improve veracity is to accept your vendor's own testing. Before a vendor solicits your business, you would like it to have its own house in order. You want to know that a vendor has hired an auditor or assessor to conduct an appropriately scoped and aligned audit of its own business so that its management team can assert that the company is operating properly (and controlling its own risk).

Beyond proof of an engaged management team, where vendors have done an audit, you may be able to leverage the information in the audit report to accelerate your vendor assessment. Consider that IT service providers typically have their own operations assessed by independent auditors, who generate a Service Organization Controls (SOC) report. SOC reports are specifically designed to help service organizations—organizations that operate information systems and provide that service to other entities—build trust and confidence in their service delivery processes and controls. SOC reports cover core aspects of the vendor's business, such as policies, access controls, backups, and change management. Therefore, if you trust the opinion of the auditor, you don't need to test those controls directly.

A word of caution: Make sure you understand the scope of the outside assessment you are relying on, as the audit may not align with your needs. There are two modes of scope: content and assets. In terms of content, ask if the independent assessment covers your topic of interest. For example, your vendor may present a clean Sarbanes-Oxley (SOX) audit opinion in which the report includes extensive IT controls testing. But, because SOX is focused on financial controls rather than on services provided to clients, you have no guarantee that the same controls apply to the work being done for you.

Sampling actual control performance is the only way to know the difference between a vendor's intent and their actual ability to address risk. However, sampling is expensive. These expenses can be kept in check by limiting sampling to key controls in areas where incidents are most likely, by limiting the size of the sample itself, and by relying on the results of audits and assessments conducted of a vendor by independent third parties that you trust.

For a vendor to lie when completing a questionnaire is actually rare. For a vendor to identify a gap they didn't know they had until you asked them to provide an example in a screen shot is, unfortunately, all too common. The good news is that sampling finds these gaps.

EFFICIENCY: DO MORE WITH YOUR RESOURCES

So far, we've discussed optimization and efficiency in terms of:

- Prioritizing on high inherent risk vendors;
- Balancing resource allocation between assessment and remediation phases;
- Using quality and consistency improvements to speed assessments and enable continuous improvement efforts;
- Streamlining assessment scope and content while meeting business and regulatory requirements;
- Focusing sampling efforts on the riskiest control areas and using effective sampling to identify risk;
- And, reusing the work of independent third parties such as SOC audits.

Your organization can continue to drive efficiency by looking for controls where your vendors, as a group, are consistently successful versus areas where successful risk management is more challenging. Where your vendors are consistently successful, you may be able to cut the content from your questionnaire. When Denial of Service attacks first emerged, a common and successful countermeasure was to tune kernel parameters on Web servers to accept a larger number of connections and discard them more quickly when unused. For a time, it was critical to ask Web hosting vendors about this configuration detail. Within a few years, these re-tuned kernel parameters had become the default setting for operating systems, set directly by their publishers. As a result, this vulnerability is now rare. There's no reason to ask questions about these kernel parameters

any more. In contrast, it's likely that your vendors have wildly different practices around managing mobile devices. Such areas, where views on industry best practices can themselves be inconsistent, deserve increased focus and discussion.

You can save time and money by concentrating your assessments on these more troublesome areas.

Deduplication of effort is also a critical technique for assessment program optimization. It's as simple to understand as it is to overlook. If you ask the same question twice in your questionnaire or have multiple business units using the same vendor. You may have an opportunity to optimize.

As mentioned above, automation tools can help you standardize your assessments and be much more efficient in your processes. Many companies use spreadsheets to maintain their vendor questionnaires, which work fine up to a point. However, if you need to assess more than a handful of vendors, a purpose-built VRM solution will increase your efficiency and effectiveness. Not only will software speed tasks such as communicating with vendors and securely exchanging information but also, software-based vendor risk management solutions will help:

- Consistently identify high risk vendors
- Accelerate reporting to management and regulators
- Provide for easy tracking of program progress and issues remediation
- Streamline portfolio-wide vendor risk reporting
- And facilitate the analysis needed for continuous improvement efforts

CONCLUSION

What makes a vendor assessment "better?" We can look at the crispness of a questionnaire, our ability to assess more vendors faster, or the degree of satisfaction of our regulators. But, the real answer is, a vendor assessment program is "better" any time we can identify and eliminate more risk. That our budgets and other resources are finite adds efficiency as a necessary variable to the equation.

Improving the quality and consistency of your assessment materials and methodology helps improve your VRM program by increasing the accuracy of the information you collect about your vendors, by balancing resources between assessment and remediation cycles, and by providing the basis for continuous improvement exercises. Improving alignment with business and regulatory requirements helps ensure that the assessments have the appropriate scope of content and are risk-aligned to your available resources. Improving veracity by sampling control execution helps identify easily resolved risks that might otherwise go unnoticed. And, throughout all of these opportunities to improve a VRM program we overlay efficiency. Not necessarily the efficiency of assessing more vendors or the efficiency of testing more controls but the efficiency of resolving more risk.

PROCESSUNITY & VENDOR RISK MANAGEMENT

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company's software-as-a-service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes.

ProcessUnity's cloud-based Vendor Risk Management solution helps companies effectively identify and mitigate risks posed by third-party service providers in critical risk areas such as information security, service delivery, supply chain processing, financial processing, reputation, and regulatory compliance. ProcessUnity provides organizations with clear visibility into the business impact of third-party risk via direct links from vendors and their services to specific business elements such as processes and lines of business. Powerful assessment tools enable evaluation of vendor performance based on customer-defined criteria through automated, questionnaire-based self-assessments as well as through detailed audits of vendor controls. Flexible reports and dashboards enable ongoing monitoring of vendor ratings, assessment progress, and status of remediation activity. Learn more at www.processunity.com.

ABOUT PROCESS UNITY

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company's software as a service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes. For public companies and regulated industries, ProcessUnity Risk Suite delivers effective governance and control, vendor risk mitigation, and regulatory compliance. For benefit plan administrators and other financial service firms, ProcessUnity Service Delivery Risk Management (SDRM) controls complex product offerings and strengthens client service experience. ProcessUnity is used by the world's leading financial service firms and commercial enterprises. The company is headquartered outside Boston, Massachusetts and is funded by Rose Park Advisors and other private investors.

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655