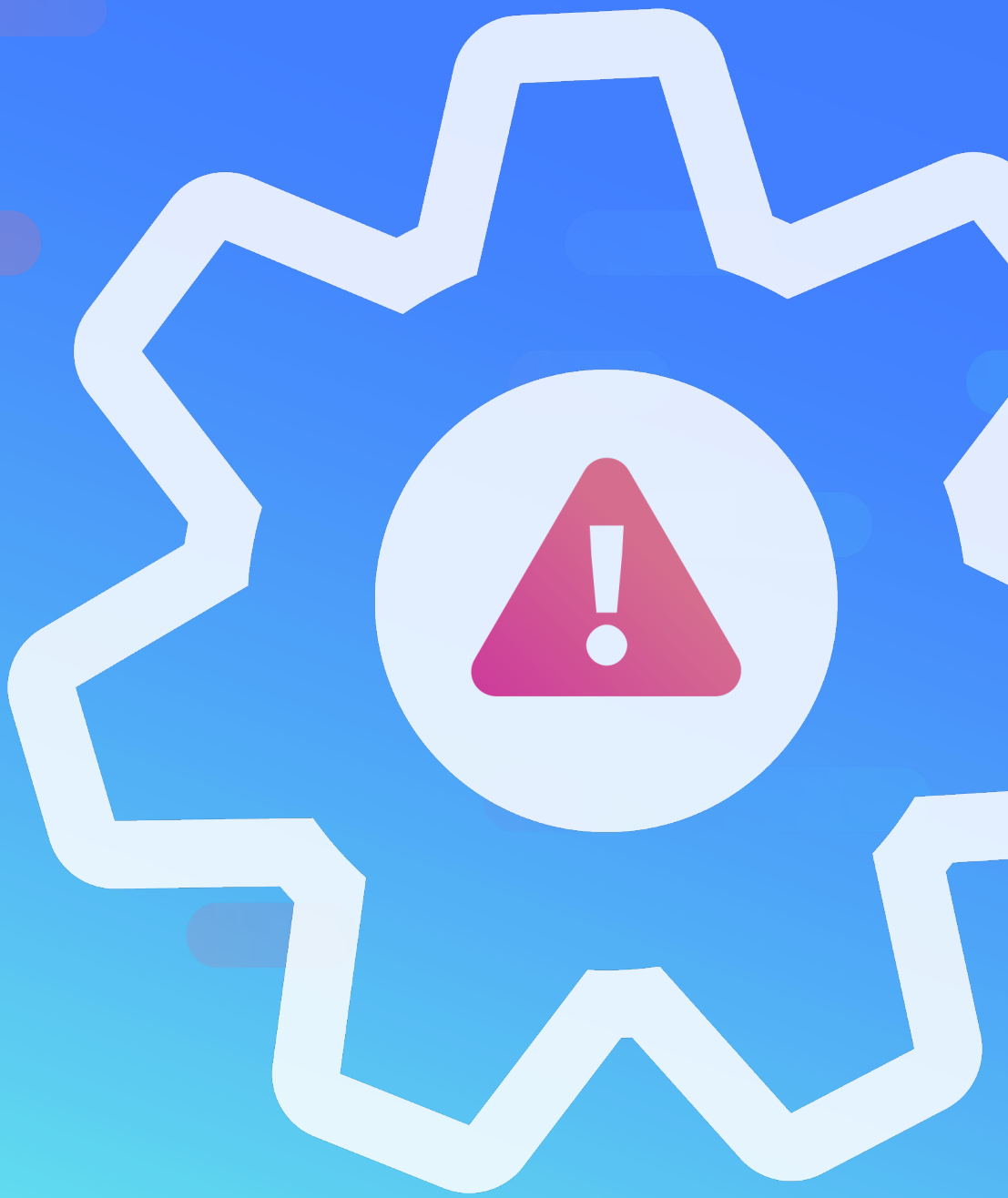
GUIDE

7 Steps to Effective Vendor Risk Management

Smarsh Vendor Risk Management



smarsh®

7 Steps to Effective Vendor Risk Management

Wherever an organization's vendor risk management program is in its evolution, a key to success is to simplify and streamline the entire process through iterations that will make it sustainable. This paper presents 7 key steps that incorporate cross-industry best practices to guide that process and equip your organization with a top-tier approach to managing third-party risk.

BUSINESS DEPENDENCE ON the third-party supply chain ecosystem has never been more complex. As client, market and regulatory pressure relentlessly increases, the risks associated with widespread reliance on third parties compounds. Supply chain risk can come in many forms. Top of mind is cybersecurity, but the pillars of risk extend much further. For instance, privacy has quickly become a critical issue. Business resiliency (business continuity and disaster recovery), financial, brand and reputational risks are also important vendor evaluation criteria.

Whether you have a handful of vendors or thousands in your portfolio, the process can be daunting and time-consuming. There is a lot of data to track. Many organizations that have a formal vendor risk management (VRM) program in place find keeping up with requests for security reviews to be a constant challenge. Other growing organizations may be building a program from scratch and struggling with how to start. In either situation, risk management, IT and security teams tend to be understaffed. Executives across various industries have reported that solid, properly trained resources are often difficult to acquire and retain, and the amount of work required continues to increase.

The following steps will help you and all the relevant stakeholders develop a VRM plan, regardless of your current program's state of maturity.

Step 1.

Design the program and assemble your team

VENDOR RISK MANAGEMENT is not something to be undertaken ad hoc. It requires planning and infrastructure to make it work effectively. This is about protecting a long chain of data and assets that are vital to your organization's success.

It starts with buy-in

Fundamentally, the success of any VRM program requires leadership buy-in and organization-wide adoption. That begins with winning internal support.

If you operate in a regulated industry, stating the case is fairly straightforward. In such businesses, security and compliance must have equal weight with other decision-making criteria for selecting who you work with. Your clients are starting to demand it, and regulations emerging across multiple industries are already requiring it.

Here are a few organizations that have had high-profile third-party data breaches or incidents, but there are countless more that do not make big headlines:

AIRBUS (2019) Hackers targeted Airbus' suppliers in a series of attacks trying to gain trade secrets.

DOORDASH (2019) A third-party data service that DoorDash leveraged was hacked and exposed personal data on 4.9M DoorDash customers.

MARRIOTT (2020) Login credentials for two Marriott employees were stolen and used to breach personal information of 5.2M hotel guests.

Regulators like the New York Department of Financial Services (DFS), the Federal Energy Regulation Commission (FERC), and the State of South Carolina have implemented new laws shifting the responsibility of third-party risk assessments to enterprises. With the precedent set, more states and regulatory bodies will surely follow suit.

They may already be asking questions, such as:

- Do you have a third-party assessment program?
- Is there a review process in place for third parties that have access to client data?

If this is the case, you can use these inquiries to your advantage by including them as justification for budget — either to outsource the process or stand up a program internally.

If you aren't receiving assessment requests like these from clients, there are plenty of other places to look for justification. Remember, every company is a data owner in today's environment, so following the data through the value chain is critical.

When you evaluate which of your own third parties have access to sensitive data, consider the risks to your organization if this data were exposed. If one of them had a breach, would you be comfortable responding that you assumed they had appropriate controls in place? One of the most difficult things to repair after a breach is an organization's reputation, although that often isn't considered.

Use that perspective along with actual breach examples (we've mentioned some, but there are many more) to justify the cost of the VRM program and build internal support. Everyone from the top-down needs to understand that data security, and specifically third-party data security, is not just an IT issue. It must be part of an organization's broader risk assessment culture that means holding all stakeholders accountable for following and maintaining best practices.

Be sure to take the current environment into account. Testing financial viability and business continuity measures is critical. If a supplier is forced to terminate or furlough employees during a recessionary period, how will that impact your business and their obligation to meet SLAs?

Build the program foundation

Set the tone by clearly stating the VRM's objective. To have the greatest impact, that should come from senior leadership beyond the IT department. Define the policy with quantifiable minimum standards of conduct and security, and a process to approve exceptions to those minimum standards.

Next, scope the program. Consider what assessment methodology will be used. Decide which vendors should be part of the assessment process and how frequently should they be assessed (step 3 will discuss tiering vendors by criticality). Focus first on evaluating existing vendors, then expand to vendors under consideration for partnership. To that end, be sure to incorporate contract management evaluations into your process.

For the program to be successful, the appointed VRM team should consist of stakeholders across multiple functions. Assign a team leader to manage the coordination and process; that responsibility often falls under IT security or compliance. Other VRM team members should include business unit leaders, procurement, general counsel, finance/accounting and representatives from senior leadership — those authorized to accept or reject any risks third-party vendors may pose.

Long-term success starts with planning, communication and buy-in. Developing a mature vendor risk management program requires transparency throughout the organization. The role of vendor risk management teams is to scrutinize a supplier despite a business need. Be prepared to defend your decisions. A formal policy, approved by senior leadership, will make that a lot easier.

Step 2.

Select which third parties to assess

DEVELOPING A COMPREHENSIVE list of vendors may seem straightforward, but certain vendors can be overlooked. A Ponemon study from late 2018 found that only 34% of companies maintain a comprehensive list of the third-party vendors, suppliers and partners they work with. If you're part of the 66% who don't have a comprehensive list, here's how to approach creating one.

Keep in mind it's not one-size-fits-all. The list needs to go well beyond IT or IT-related vendors to include all third parties who pose a potential risk to your organization. Here are three groups to consider:

- **THIRD PARTIES** that interact with your networks, components or information systems including software, hardware and professional services
- **THIRD PARTIES** that provide physical security and support services like security guards, janitorial or CCTV
- **PARTNERS** who access your APIs and have access to your data and/or systems

The VRM program leader should work with legal, procurement and accounting departments to develop an accurate vendor inventory for third parties. We recommend these first steps:

- **REQUEST A DOWNLOAD** of all payments made to third parties over the last 12 months
- **COMPLETE THE COMPANY NAME** and a point of contact for each third-party, as well as the internal relationship manager for the account
- **DETERMINE THE SERVICE** provided by the third-party, and if they store or access any data or have network access

Evaluating partners may require deeper scrutiny. If you expose an API, chances are data is transferring hands. Do you really know who has access to it and how it is being used, processed or stored once that access is in place?

There may be challenges associated with assessing these parties; they may be revenue sources for your company so you will need to tread lightly. But do remain firm, as the need to assess is becoming increasingly important. Talk to your strategic partnership teams for help gathering this information and establishing relationships where appropriate.

Developing your list of vendors can be a frustrating, time-consuming process. You will be required to speak to many divisions within your organization, ask these resources to do extra work, and request data in a format you can digest. Don't get discouraged. This is a very important step and gives you the opportunity to communicate with internal teams on the importance of vendor risk management. Implementing a VRM program is a great time to do a comprehensive review of your vendor portfolio and ensure accurate tracking of all your current vendors.

Step 3.

Categorize third parties by risk tier

ONCE A COMPLETE vendor inventory is compiled and each vendor is categorized by their data access, then you can determine each vendor's criticality to the organization and assign them to a risk tier. This step is vital to ensuring your assessment is tailored appropriately for the risk posed by each vendor. To ensure consistency across all vendors, the VRM team develops a list of weighted critical questions to evaluate how each vendor mitigates risk. It's more science and less art.

Use a straightforward question-based approach. Develop 10 to 15 questions you could ask internal stakeholders to help define third-party criticality. Thinking back to step 1, this is a perfect example of cross-functional roles and responsibilities. The business teams have greater insight into the role the vendor will play in the organization, their data and physical access, and the impact on operations in the event the vendor suffers a breach or ceases to operate. This community effort will ensure all stakeholders are bought-in to the process and understand the impacts of each process stage.

Below are a few examples of questions that will determine the level of assessment required for each vendor. Classifying your vendors based on data access or business function is a part of a mature vendor risk management program. Note these are just examples for you to review and may not be comprehensive. Smarsh Vendor Risk Management has developed a Risk Tier Calculator that can assist in your question selection.

- **DATA ACCESS**
  Is this third-party storing or accessing critical data?
- **NETWORK ACCESS**
  Will the third-party have direct access to our network?
- **GDPR & REGULATORY REQUIREMENTS**
  Is this third-party subject to regulatory requirements themselves that, if violated, could impact our service level?
- **INCIDENT RESPONSE**
  Will a failure by this third-party activate our incident response plan?
- **BREACH NOTIFICATION**
  If this third-party suffered a breach, would we be required to notify our clients, regulators or insurance company?
- **COMPLIANCE & REPUTATION**
  Is this vendor working from overseas? Will they process credit card transactions?

This questionnaire then becomes your Third-Party Inherent Risk Analysis Calculator that can be used to tier third parties. This brings stakeholders together, drives the depth of your review process, sets the timeline for reassessment, and forces all parties to have alternative options for vendors deemed business-critical.

Here is a useful tiering classification scheme:

RISK TIER 1
Risk Tier 1 vendors are classified as business-critical, with the greatest access to your organizational or client sensitive data. These vendors must receive your most comprehensive security assessment, including rigorous inquiries into their policies, procedures and network architecture.

RISK TIER 2
Risk Tier 2 vendors are classified as medium risk. They should receive a less exhaustive security assessment than Tier 1. However, the Tier 2 assessment should still include questions that identify their policies, procedures and architecture.

RISK TIER 3
Risk Tier 3 vendors are classified as low risk and warrant a more focused security assessment as compared to Tier 2. While these vendors don't have the same access to organizational or client data, assessment questions should still cover the main risk categories.

If you work with a minimal number of third parties, you may be able to easily find the information needed for appropriate tier classification. If you have many, it may be harder to gather. The key is to source the information from the business unit who owns the third-party relationship or is working to onboard them. The team or individual who will be responsible for overall third-party risk management should act as the facilitator of the process.

Step 4.

Design the questionnaire: standardized, custom, or a combination?

TIERS OUTLINED IN step 3 help define how your organization will execute the assessment process. Develop a security assessment methodology designed to evaluate your organization's tolerance to risk, your regulatory requirements and best VRM practices. Creating a proprietary questionnaire from scratch is always an option, but we suggest using content developed by third-party risk management experts instead of reinventing the wheel.

Thoroughly research questionnaire content options

There is a fine line between standardization and customization in the security assessment process. Risk is contextual; it must be measured through the lens of each organization's risk tolerance.

It's helpful to use industry standard frameworks (e.g., NIST, ISO or CIS) as guidelines; or consider agnostic and/or industry-focused assessment content such as The Shared Assessments Standardized Information Gathering Questionnaire ("SIG"), the AITEC-AIMA Due Diligence Questionnaire (DDQ) (for investment advisory firms), or the Higher Education Community Vendor Assessment Tool ("HECVAT"). Adhering to any one framework is difficult, and adherence to overlapping frameworks is often necessary. But the more you can utilize standardized assessment content, the less friction there will be in getting responses from your third parties.

Some of this content is subscription-based, but Smarsh Vendor Risk Management offers most of it at no additional cost to clients, and helps you choose what questions to ask. If your risk management team is small or doesn't have the time to develop and maintain a custom assessment, this can help you hit the ground running. Our team has curated over 35 industry-standard questionnaires covering many of the risk domains discussed in the prior steps.

Tailor your assessment and expand the conversation

While the SIG offers precompiled templates like the SIG Core (800+ questions good for Tier 1 assessments) and SIG Lite (365 questions for Tiers 2 or 3), you may need to make adjustments to what's relevant for your approach, vendors and internal policies. Customize to whatever subset of those 1100+ questions fits your needs. Your enterprise likely has talented individuals with independent views on the greatest potential risks third parties may pose to your organization. Expand the conversation beyond just the team working on the assessment, then add, edit or remove questions based on the feedback received.

Assign weights to questions

It's important to have a common scoring methodology for your assessment process. One clear and simple way to do that is to calculate a weighted average risk score for each vendor. Assigning weights to questions lets you tailor how much each question impacts the average risk score.

Assess yourself

When your questionnaire content is chosen, answer it yourself. Capture information around how long it took to complete specific questions that were tricky to answer, and which risk areas seemed to lack coverage. Not only will this completed assessment come in handy for future questionnaires you may receive, it will give you a better understanding of what you view as an acceptable answer for each question.

Building risk assessment questionnaires is a moving target that requires continuous evaluation and revision. Changes to your business, external regulations or your risk threshold are all triggers that should require a re-evaluation of your questionnaire.

Further, Smarsh VRM will update our questionnaires annually or more frequently to ensure you have the most recent content. The Shared Assessment SIG is reviewed every year, tracking against market changes that follow the reassessment timelines for critical vendors. That's discussed in the next step.

Step 5.

Implement vendor assessments and review results

DEVELOPING A STREAMLINED process for distributing the assessments to third parties, scoring the submission, and reporting results are key to every successful third-party risk management program. Implementing and formalizing your program management function allows you to leverage data to develop an auditable and contractible repository of risk information. No matter how you choose to manage your program, you'll need a well-defined process that includes the assessment trigger, distribution management, scoring and reporting the results.

Assessment trigger – new vendors

Incorporating vendor risk management into your procurement process can be challenging. It involves many stakeholders, potentially slows the buying process, and may result in additional contract language or accepting a certain level of risk. Historically, procurement decisions have had two main factors: price and business efficiency. In today's environment, security and privacy must have equal value in your purchase decision.

If you followed step 1 properly, all stakeholders will understand and appreciate the need for a new vendor risk review. It can take between 1 to 4 weeks for a vendor to respond to an assessment depending on the questionnaire you use. That's why we suggest common frameworks that can be expedited when done as part of the procurement process. Vendors' sales teams don't like delays, so involving them can be a good tactic to get results faster.

Then at what point should you send a security assessment to new vendors being onboarded? We always recommend launching your assessment once the business teams have narrowed their decision to 2-3 finalists or are close to making a final decision on a product. From our experience, launching the assessment process before this point can cause confusion and vendor pushback.

Communication at this stage is critical. Have the business teams inform the prospective vendor that the assessment is part of the relationship evaluation process; more often than not, vendors will comply. Make sure the vendor (and their security team) understands this is standard operating procedure and is being completed in the spirit of a partnership between your two firms. Emphasize the importance of honesty, and explain that not having certain security measures will help facilitate a dialogue but is not an immediate disqualification.

If you issue RFPs, the assessment can be worked in during the response period. Vendors can provide their completed assessment as part of their proposal submission. Again, we suggest including this as part of the initial RFP process, but only require finalists to complete the assessment.

When you need to manage the risks posed by new API partners, launch an assessment at the time the partner completes an integration or after a certain number of API calls. This may be especially important if sensitive data like Personally Identifiable Information (PII) is shared through the API. These may be sources of revenue for your business, so be sure revenue teams are included as this can be a bit delicate.

Emphasize the importance of honesty, and explain that not having certain security measures will help facilitate a dialogue but is not an immediate disqualification.

Be sure to develop a well-defined assessment process and communicate it internally. Like a policy, these processes are only effective if the right people know they exist and have acknowledged that they will adhere to them.

Assessment trigger – current vendors

New risks are always emerging, so you'll need to regularly assess your incumbent vendors to ensure they're evolving their controls over time. Check in with them on a regular schedule to verify that nothing has changed. Use your risk tiers to apply a risk-based approach to assessment frequency. For example:

RISK TIER 1
Assess annually or more frequently as preferred

RISK TIER 2
Assess every 18 months or more frequently

RISK TIER 3
Assess every 24 months or more frequently

Managing the assessment workflow

If you're thinking of using a spreadsheet or word processor to execute your assessment process, you'll face some challenges that need to be planned for ahead of time:

LACK OF VISIBILITY

When you send out the assessment, you'll need to either send each vendor a unique email or bcc all of the vendors and attach the questionnaire. As soon as you send that email, you lose all visibility. You can't tell if a vendor has started the assessment unless you email them again and ask.

SOLUTION

As the assessment due date approaches, you'll need to send reminders to vendors who have yet to submit. Some vendors may have questions, so your outreach also creates an opportunity to interact. SaaS platforms like Smarsh Vendor Risk Management can help to automate the reminder process.

VENDORS WHO REFUSE TO COMPLETE THE ASSESSMENT

In some cases, third parties will refuse to complete the questionnaire. They may provide a security packet or some other information or certification they think is sufficient.

SOLUTION

This may not be a problem if your organization is willing to accept a certification or audit in lieu of an assessment. We only recommend this approach for certain tier 3 parties — for small to midsize organizations simply accepting a certification from a Tier 1 or even a Tier 2 vendor is not a best practice in our view. There are exceptions to every rule, but always communicate the need for consistency in your evaluation process aligned to your assessment questionnaire. Larger organizations such as Amazon, Microsoft and Salesforce often fall into our Too Big to Assess category. So for them, a certification is usually an acceptable method of review.

One of the benefits of using the SIG is that third parties often already have a completed version they can share upon request. If you use a custom assessment and still want them to complete it, discuss the reason why and emphasize that your intent is to manage risk with the most current, timely and applicable information possible.

Scoring the assessment - remediation or termination?

Once you have a vendor's response, the next step is to score their assessment. This may present some challenges, so here's how to prepare for them:

SCORING ASSESSMENTS QUICKLY WITH A COMMON APPROACH

You'll have to review each vendor's response and write comments in each individual submission spreadsheet. Consequently, vendor data is siloed and not easily available for team collaboration. You need to ensure the scoring process is standardized, efficient and prompt. Otherwise, risks to the business will linger.

SOLUTION

Since your scoring methodology was already set up earlier, this should be a fairly straightforward process. If you are using a spreadsheet, create a master workbook that scores the responses. As each vendor replies, input their responses and calculate their risk score.

SaaS tools like Smarsh Vendor Risk Management usually offer an auto-scoring capability that automatically scores responses as they're submitted. Multiple business units or risk assessment team members can be easily granted access for collaboration.

Alternatively, you can set up a cloud-based shared drive to store the data and control versions. Remember, this is sensitive information that needs to be treated with a great deal of care.

Keep the scoring mechanism out of the file you send to the vendors so they do not see their overall risk score.

Visualizing results

The VRM program leader will need to report on this data and show results to senior leadership to demonstrate results that validate the program's cost.

GRAPHICALLY PRESENTING TIMELY RESULTS

Centralize all results and manually create graphs and charts as required by leadership. These will need to be regularly updated, and require on-demand generation. They need to be clear and easy for busy executives to understand.

SOLUTION

If using a spreadsheet, centralize your scoring process within a master file. We recommend creating simple plot graphs showing the risk rating by third-party. Grouping third-party risks into categories like tier, department or type can show where the greatest risk lies. Smarsh Vendor Risk Management and other SaaS tools have reporting and visualization capabilities built in. That makes it easy to create reports and visualize assessment data on-demand.

Terminate or remediate?

In some cases, it simply may not be worth going through the remediation process with a particular vendor. Determining whether a specific score will fail a vendor can help you make important decisions when deciding to use or continue working with them. Making this determination helps your company focus resources on remediating high-risk issues from third parties that are critical to your business.

Step 6.

Remediation management

Reviewing the assessments will yield a comprehensive analysis of policy, risk and third-party risk mitigation procedures. You'll need to discuss each third-party's results with them to relate any problems or concerns. Be sure to include the business in the discussion, especially if a finding will restrict or delay the use of a vendor. Transparency is essential to developing a strong relationship and a culture of security.

You'll need to formulate remediation items for each identified risk. We recommend using a three-part approach when creating and managing the remediation process:

Part 1: Context

The best way to receive a quick response is to first lay the cards on the table. Describe why having a specific policy or control is important. Let's use an information security policy for example:

"Regardless of organization size, a documented information security policy defines the rules and procedures internal employees and/or third parties should follow when accessing information and assets. This policy should be communicated, reviewed and acknowledged by stakeholders to help ensure its effectiveness."

Part 2: Actions to be taken

After identifying a risk, follow up with the vendor and write up your remediation requirement. Each vendor will need its own email explaining the requirements applicable to them. Managing this communication and reporting on vendor progress can be time-consuming. Continuing with our information security policy example:

"Please create a robust information security policy that is communicated, reviewed and signed off on by every employee in the company."

SaaS tools like Smarsh Vendor Risk Management make it easy to draft remediation requirements on a question-by-question level. You can use the tool to send the item to the vendor, then use it to check on receipt/read status. Smarsh Vendor Risk Management can then automatically send reminder follow-ups if the vendor hasn't yet viewed the ticket, or resend items quickly if needed.

Part 3: Remediation approval, risk score adjustment, and/or risk transfer

We frequently see organizations communicate remediation requirements to third parties, and then simply forget about them. The risk continues. Instead, as part of the remediation process, request that the third-party provide evidence of their remediation actions to validate that they have met your requirements. If they have, make sure to give credit. Adjust the risk score accordingly from your original review.

However, if the third-party is unable or unwilling to remediate the issue, then an internal discussion is needed. Ask yourselves:

- How critical is the finding?
- What is the potential impact to your organization?
- If the vendor stores highly sensitive data and they have major gaps, who is responsible if there is a breach?

The risk management or security team then needs to make a determination if they are willing to accept the risk. If not, an exception protocol should be put in place that transfers the risk to the business. The business manager must accept and describe the value of the risk, which could have a significant impact on the company.

Bottom line — remediation management, communication and risk acceptance are critical to the vendor risk management process. Yet they can often be overlooked in organizations that are starting their programs. All stakeholders must be made to understand that no third-party is perfect and acceptance of certain risks may be necessary.

Step 7.

Continuously monitor

Technology and security risks are evolving rapidly. Your team needs to assess your vendors regularly to maintain the most up-to-date risk information. As your VRM program matures, augmenting it with continuous monitoring solutions is also necessary.

Reassessments and ad hoc assessments

Maintain and adjust your reassessment schedule for each vendor tier. Defining the reassessment schedule and sticking with it keeps your team up to date on changes occurring in the vendor's security position. You may even need to administer ad hoc assessments depending on current industry threats or incidents. For example, if a vendor has a breach, you should assess them again. Alternatively, there may be a new high-risk, zero-day security flaw publicized. Send an assessment to your vendors to ensure the gap has been closed on their end.

Real-time data: security, financial or other

There are many tools available that offer continuous monitoring services. Some use publicly available information to generate additional automatically updated risk ratings for specific risk domains. For instance, you may need to monitor the financial health of your Tier 1 vendors or continuously monitor their dark web data exposure. There are tools that can help you achieve this automatically.

A word of caution: it's best not to rely on these tools as a sole method for assessing your vendors. A security questionnaire PLUS a continuous monitoring solution achieve the most effective approach to vendor risk management.

A security questionnaire PLUS a continuous monitoring solution achieve the most effective approach to vendor risk management.

Moving forward

A sound vendor risk management program is critical to a comprehensive security strategy. It's simply no longer optional. Set a policy, stick with it, and communicate it to all vendors and stakeholders. While nothing is 100% foolproof, following the 7 steps discussed in this paper will help ensure transparency and keep risk in check across your entire value chain.

Move one step at a time and be diligent in setting up your processes and controls. Use internal and external resources to help think about data your organization maintains and shares. What communication processes are in place in the event there are business changes that impact your third-party program? Take advantage of questionnaires and content developed by industry experts — there is no reason to recreate the wheel. Then, use technology as a force multiplier to streamline and centralize your vendor risk management process.

Building a mature VRM program will require up-front work and resources, but it will have a long-term, positive impact on your organization and build trust with your customers.

If you have any questions or want to explore ideas, feel free to contact Smarsh at www.smarsh.com. We have also provided some additional resources for you to research as you build and strengthen your program.

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals in in today's in-demand digital communication channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Guide - 07/23

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh