ProcessUnity

GRC World Forums

The Complete Guide to the Vendor Risk Management (VRM) Lifecycle

Contents

04 Summary

05 Sourcing

06 Onboarding

07 Due Diligence

09 Ongoing Monitoring

10 Performance Reviews

11 On-Site Control Assessments

12 Contract Management

13 SLA Monitoring

14 Issue Management

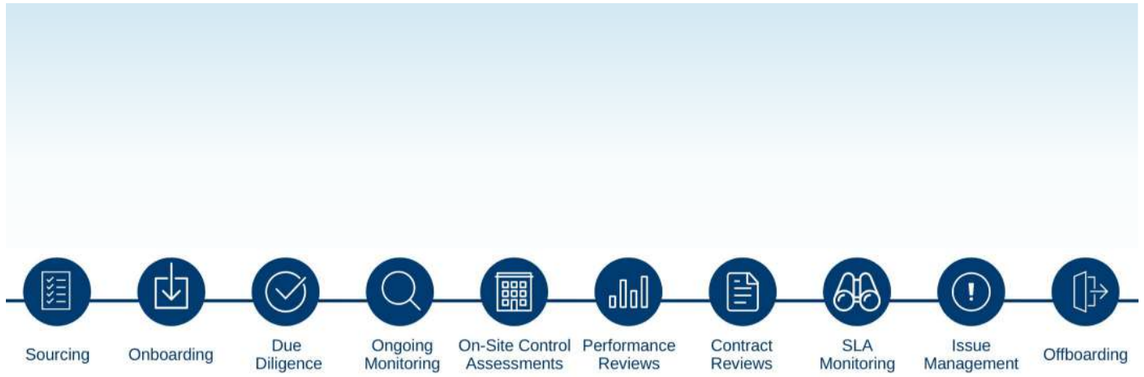
15 Offboarding

16 VRM Lifecycle Best Practices

16 Conclusion

17 About ProcessUnity

‘The VRM lifecycle allows companies to acknowledge the importance of their vendors and incorporate them into their overall strategies.’



The vendor risk management (VRM) lifecycle outlines an end-to-end vendor management approach to help you manage third parties, suppliers and business partners in an organized and transparent manner.

The lifecycle starts during sourcing and continues all the way through to the termination and offboarding of the relationship. You must employ the right systems and controls throughout the lifecycle to effectively identify and mitigate risks stemming from third parties.

The VRM lifecycle allows companies to acknowledge the importance of their vendors and incorporate them into their overall strategies. Companies that have strong vendor relationships are better able to manage their overall risk posture and ensure business continuity.

Throughout the lifecycle, it is important to review areas of potential exposure and determine whether those risks can be mitigated properly.

This eBook will walk you through the ten stages of the VRM lifecycle and provide information on the common challenges organizations face at each stage. It will also provide you with tips and tricks on how to get beyond these challenges.

The sourcing stage of the VRM lifecycle means conducting your initial search for suitable vendors. Sourcing is a mature process that can be challenging for many organizations. Let us consider some of the difficulties inherent to this early stage of the VRM process:

Non-Standard Sourcing Procedures:
Sourcing vendors in large or complex companies can be a disorganized process. Departments responsible for conducting vendor evaluations can receive poorly articulated requests and struggle to properly document and rationalize their sourcing approach. Ultimately, these organizations lack a fair, predictable vendor selection process that complies with company policies.

Sourcing a Strong Pool of Prospective Vendors:
For any given service, there are many vendors willing to provide it. Before you start thinking seriously about bringing any specific vendor onboard, you will need to find candidates with sufficiently clear and transparent policies and practices. Sourcing high-quality vendors is impossible if you have not clearly articulated your risk exposure.

Receiving Proposals and Awarding Business:
Let us be honest—the process of sourcing vendors can be a mess. When is the last time your process was completed on schedule? Organizations may publish a request for proposals (RFP) along with a schedule setting out key dates. But many vendors fail to meet these targets or end up submitting inappropriate proposals.

A lack of clarity at the start of the vendor lifecycle can have knock-on effects further down the line.

Overcoming Sourcing Challenges

The sourcing stage of the VRM lifecycle is your opportunity to implement good risk-management practices from the very start:

Integrate Initial Vendor Risk Assessments into Sourcing Processes:
There is no better time to keep risk out of your organization than before you sign a contract. Even better, why wait until vendor selection to understand if a vendor's weak security practices prohibit you from doing business with them? Be sure to incorporate high-level questions into RFPs and other requirements documents to weed out poor vendors earlier in the process.

The sourcing stage does not require a detailed investigation of an individual vendor—that comes later. But bringing forward some of those risk-management principles to the sourcing stage will make the subsequent VRM process easier.

Implement a Consistent, Automated Sourcing Process:
Keep your sourcing process organized and well-documented. Using a unified VRM platform for receiving, documenting, and evaluating vendor responses will help you stay in control, select the right vendor faster and move smoothly to vendor onboarding.

'Sourcing high-quality vendors is impossible if you have not clearly articulated your risk exposure.'

Onboarding

Overcoming Sourcing Challenges

The "onboarding" stage involves approving a vendor and bringing it into your operations. Here are some of the challenges involved in onboarding vendors:

Avoiding Over-Complication:

Many professionals find their company's onboarding process to be a headache. That is often because it is too complicated and contains too many steps. In fact, one organization counted 89 steps in its company's onboarding process. That is 89 separate steps simply to get a vendor set up and integrated into the company's processes.

Determining Inherent Risk:

For many businesses, onboarding is a disorganized process. Using multiple platforms, spreadsheets, and relying on email can lead to an inconsistent and illogical onboarding approach. An inefficient onboarding process will prevent you from gaining a clear understanding of inherent risk. This may mean you end up carrying out unnecessary due diligence—wasting time and resources—or failing to carry out necessary due diligence—increasing risk.

Making the onboarding process as simple as possible—for your third-party risk management department, the requestor, and the vendor—benefits everybody. Take these steps to improve onboarding:

Establish an Enterprise-Wide Process:

To help determine a vendor's inherent risk score, draw on the knowledge of the person making the vendor request. Do this by asking the requestor to complete an internal inherent risk questionnaire. You should have a standardized, relevant set of questions to send to the vendor requestor, such as:

- Will the vendor have access to sensitive or personal data?
- Will the vendor provide customer-facing services?
- Are the vendor's services essential to the operation of the company?

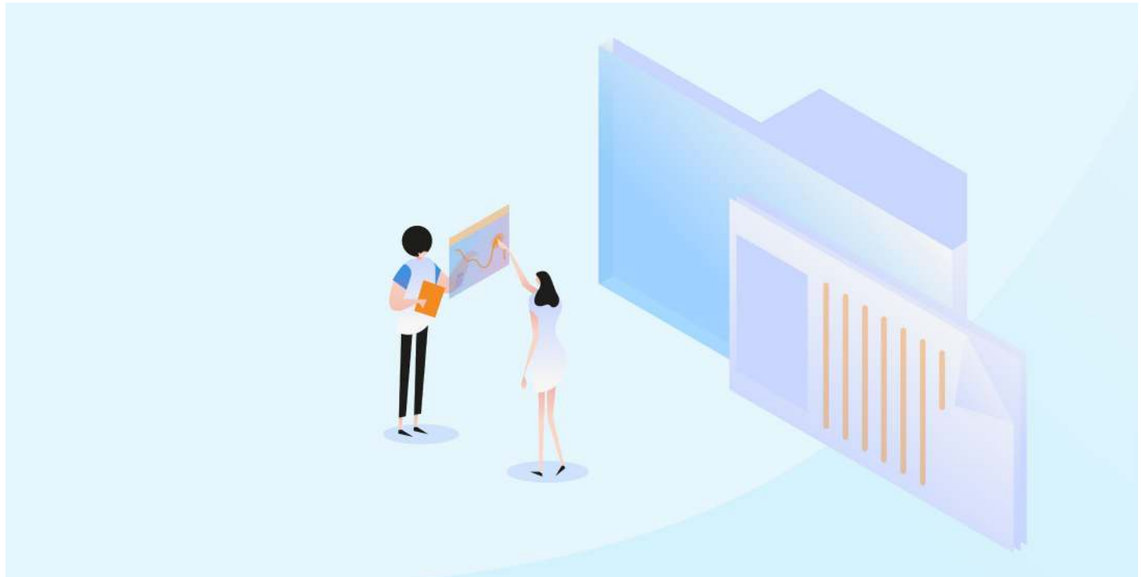
The vendor requestor should be able to answer these questions using your VRM platform for automated inherent risk scoring and vendor classification.

Replace Manual Processes with Automation:

One key change that will transform your onboarding process is automation. Automation will help you bring down your onboarding steps, scope vendor questionnaires appropriately, and ensure an efficient and consistent, and objective onboarding process.

Use one unified platform to generate internal and external vendor questionnaires, drawing from a library of questions. This library can include basic questions for all vendors—regardless of inherent risk—and advanced questions tied to regulatory standards. An automated platform will also ensure you keep comprehensive records and produce a clear audit trail.

Due Diligence



Due diligence means collecting and checking information about a prospective vendor's practices and compliance. Initial due diligence occurs during the onboarding phase of the VRM lifecycle, and it might not be necessary for every vendor.

Here are some of the challenges associated with conducting due diligence.

Properly Determining Risk:

During the onboarding process, you will determine whether a given vendor can proceed straight to contracts or whether it requires a full due diligence investigation first.

But many businesses lack a systematic approach to due diligence, driven by a clear understanding of inherent risk. A poorly organized due diligence process can be disastrous -- slowing the start of a vendor service, or worse, exposing your company to substantial legal and reputational problems.

Inconsistent Analysis and Review:

Even if an organization has properly determined a vendor's risk score, it can still take an inconsistent, illogical approach to reviewing, analyzing, and acting on the results.

Applying inconsistent risk analysis can expose you to unnecessary risks and cause you to accept inappropriate vendors—or reject appropriate vendors.

Slow or Incomplete Responses:

Many businesses find they do not receive a timely response to their due diligence questionnaire. Or sometimes, the questionnaire can come back incomplete or contain irrelevant information. This back-and-forth with vendors can be costly, inefficient, and result in lengthy delays to onboarding.

Overcoming Due Diligence Challenges

Getting due diligence right is a crucial way of managing your risk exposure. An effective due diligence process is consistent, systematic, and driven by automation.

Enforce Objectivity:

Every step in your due diligence process must be clear, rational and repeatable. Being consistent in due diligence ensures a better understanding of risk, better documentation and better vendors. Following an automatic, consistent process for sourcing and initial vendor onboarding puts you in an excellent position to conduct due diligence.

Create Meaningful Vendor Questionnaires:

The questionnaire you send a vendor will determine the need for any further due diligence. It is vital that you ask the right questions and use the results to calculate a meaningful and rational inherent risk score.

Vendors with low inherent risk scores can proceed to full onboarding with minimal delay. You may only need to obtain basic information for these vendors, such as their contact details and an overview of their services.

For vendors with a higher inherent risk score, you will need to scope the questionnaire appropriately. Higher-risk vendors or suppliers that are more important to business operations need to be vetted deeper than lower-risk or less important vendors. The questionnaire needs to be adjusted based on the nature of the vendor service. For vendors tasked with processing payment data, for example, need to be asked if they are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

Reduce Due Diligence Steps:

There are three broad steps to carrying out due diligence:

- **Internal investigation:** Determine your risk exposure. Consult with internal stakeholders. Search for the vendor on publicly available sources, such as government watchlists and third-party databases.
- **External investigation:** Submit inquiries directly to the vendor and request relevant documentation and certifications.
- **Assessment:** Analyze the results of your internal and external investigations. Decide whether to reject the vendor, accept it, or accept it with conditions.

Automate the Due Diligence Process:

You should conduct each due diligence step in a comprehensive, consistent, and rational way using an automated VRM platform. Automating your due diligence process has numerous benefits:

- You can create an appropriately scoped questionnaire from a library of pre-determined due diligence questions.
- You can carry out the entire due diligence phase using one platform: sending and receiving vendor questionnaires, assessing vendors, and documenting the process.
- Vendors can use your platform to submit information and documentation.
- An automated assessment system—based on numerical scoring—leads to more consistent and rational vendor adoption.

‘An effective due diligence process is consistent, systematic, and driven by automation.’

Ongoing Monitoring

Ongoing monitoring takes place post-contract—after a vendor has passed your onboarding and initial due diligence checks. While your vendor might initially meet your organization’s standards, this can change over time as risk profiles change. You will schedule regular dates on which to review a vendor’s performance and compliance.

Here are some of the challenges you are likely to face when conducting ongoing monitoring:

Obtaining Meaningful Information:

Your vendor contract should require the vendor to report any important issues. But you cannot always rely on the vendor to volunteer such information.

Vendors can be very responsive to your requests for information in the pre-contract stages of the VRM lifecycle (because they are hungry to win your business). But once the vendor has your business, you might find that they are less enthusiastic about being reviewed again and information is less forthcoming.

Too Many Vendors to Assess:

You may find that your list of vendors is simply too large for you to monitor them all effectively. Regularly checking for new and relevant information about every vendor can become a resource-heavy, disorganized process -- especially when adding more vendors each year.

‘Get ongoing monitoring wrong, and you could miss vital information about a vendor that leaves you liable for their activity.’

Overcoming Ongoing Monitoring Challenges

Get ongoing monitoring wrong, and you could miss vital information about a vendor that leaves you liable for their activity. Here is how to create an efficient and organized ongoing monitoring program:

Incorporate External Expert Ratings:

Vendors operating in high-risk and complex fields should be monitored across many different metrics: financial health, cybersecurity, and other more. You should consider using expert third-party ratings to receive insights and analysis on vendors.

Using an external risk-monitoring service provides access to a virtual analyst that can compare expert ratings against your own due diligence efforts and highlight any discrepancies. You can also set alerts to signal any new intelligence about a vendor—and notify the relevant risk manager to reassess the vendor as a priority.

Scope Ongoing Monitoring According to Inherent Risk:

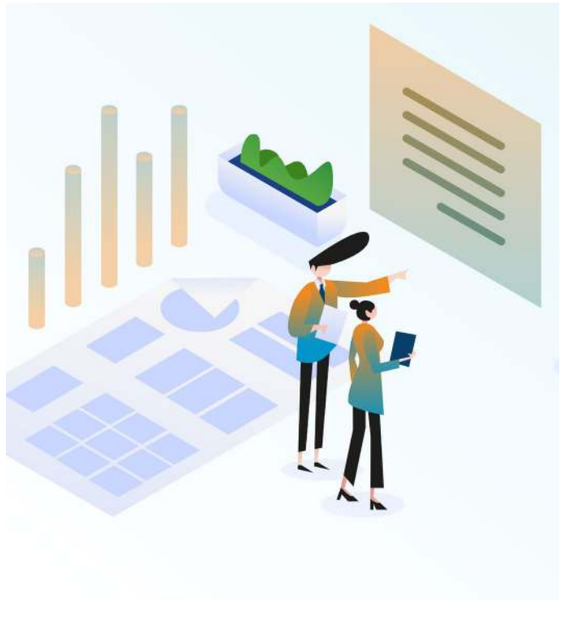
Like with all aspects of VRM—not all vendors require equal attention. Following the onboarding and due diligence phases, you will have a clear understanding of your vendors’ inherent risk scores. Use these scores to help you determine:

- The scope of your ongoing monitoring (the level of detail required)
- Your ongoing monitoring schedule (how frequently you need to monitor a vendor)

Streamline Your Processes:

Managing many vendors can lead to analyst fatigue, resulting in sloppy or shallow ongoing monitoring. This is another reason it is crucial to have all VRM activities taking place on one platform. Once vendors are onboarded, you should use the same interface to plan, implement, and track your ongoing monitoring program.

On-Site Control Assessments



On-site control assessments involve attending a vendor's premises to ensure first-hand that they are meeting your standards. Here are some of the challenges many organizations face when conducting on-site control assessments.

Obtaining Meaningful Information:
Conducting an on-site control assessment is a resource-heavy process. And if you begin the process with a vague set of objectives or unclear metrics, your visit will be wasted.

Gaining Access to Vendors' Premises:
Sometimes, it can be a challenge even to get your foot in the door. A vendor may be reluctant to provide on-site access—or external factors, such as pandemic restrictions, may make on-site control assessments impossible.

Documenting and Evaluating Results:
Having carried out an assessment, you need to put your observations into action. If you are relying on manual, disjointed processes for documenting and evaluating what you have learned during the visit, you are missing an opportunity to extract real value from this data.

Overcoming On-Site Control Assessment Challenges

On-site control assessments are a vital element of your VRM program, particularly for high-risk or heavily regulated vendors. Here is how to make the most out of this important process.

Use Inherent Risk to Scope Controls:
Your good practice in the preceding VRM lifecycle stages means you will have a clear understanding of your vendor's risk score from the start. This means you know which vendors require on-site control assessments and which do not.

A systematic, risk-driven approach can also help you assign relevant and comprehensive controls to each vendor according to its sector and its services. Assessors should be able to choose from a library of controls within your VRM platform.

Create Clear Guidance:
When your analysts arrive at the vendor's premises, they should have clear objectives and a coherent method for meeting those objectives. Planning and foresight can ensure that time conducting on-site control assessments is well-spent. At the end of the assessment, you should have a set of metrics that accurately measure the vendor's performance.

Automate the Analysis:
Once you have gathered all the information required from a vendor's premises, you should put that data to the best possible use. Use your VRM platform to conduct a standardized analysis that applies to all vendors and combine your results with other data about the vendor to contribute to an overall vendor risk health score.

Taking this consistent approach to on-site control assessments, you can make objective, actionable inferences about the results. Using an automated process is the only efficient way to achieve this.

Performance Reviews

Performance reviews are regular, scheduled assessments of a vendor's performance. By undertaking periodic performance reviews, you can check that a vendor's risk score remains accurate and ensure that the vendor is providing a good quality service. Done right, vendor service reviews weed out underperforming vendors in favor of better business partners. Here are some of the challenges organizations typically encounter when undertaking vendor performance reviews.

Lack of Meaningful Performance Indicators:
Performance reviews are an opportunity to dive deep into a vendor's practices. Without a logical, comprehensive set of key performance indicators (KPIs) against which to measure the vendor's performance, you are exposing yourself to significant risk.

Inappropriate Review Period:
Managing many vendors can lead to problems and inefficiencies in the performance review process. For example, it can be hard to know how often to review a vendor's performance. Review too frequently, and your review process could end up shallow and inefficient. But review too infrequently, and you may miss critical changes to the vendor's performance.

Inconsistent Scoring Methods:
Establishing a set of meaningful KPIs is important. But you also need a consistent, rational approach to scoring and interpreting a vendor's ability to meet these indicators—otherwise, the data will provide no useful insight into a vendor's overall risk score.

> **'Done right, vendor service reviews weed out underperforming vendors in favor of better business partners.'**

Overcoming Performance Review Challenges

Now let us look at some tips to help you conduct the best possible performance reviews:

Use Inherent Risk to Scope Performance Reviews:
Use everything you have learned about a vendor's inherent risk to scope the contents of a performance review, assigning relevant but comprehensive benchmarks that are appropriate to the vendor's inherent risk.

A vendor's overall risk health score should inform which KPIs you assign to it and how often it comes up for performance reviews. High-risk vendors require more frequent reviews.

Manage With Consistency:
When reviewing a vendor's performance, use a numerical scoring approach tailored to each vendor according to its individual risk. A rational approach to scoring ensures your performance reviews will be consistent, systematic, and logical.

Take a Holistic Approach:
The performance review is one of many ways to monitor your vendors' ongoing compliance with your standards—and it should not occur in isolation. By combining the performance review process with your ongoing monitoring efforts, you will be acting with greater efficiency and gaining a more holistic insight into your vendors' overall performance.

Using an automated VRM platform, you can combine the results of a vendor's performance review with data obtained from ongoing monitoring and on-site control assessments. This method will reveal a comprehensive overall vendor risk health score.

Contract Management

So many vendors. So many complex documents to manage – from contracts, statements of work and myriad related appendices.

Here are some of the challenges you might encounter with vendor contracts.

Lack of a Contract Repository:
It is hard to enforce contract terms if you do not have access to the contract itself. Many companies have disjointed mechanisms for managing legal documents.

What Has Been Agreed to? With Whom?
Sometimes just knowing exactly what is in a contract is a challenge. Which vendors have KPIs or service-level agreements in their contracts? Which vendors have non-standard clauses in their agreements? What is our annual spend on a per-vendor basis?

Overcoming Contract Management Challenges

When one of your vendors fails to meet their contractual obligations, it could be a disaster for your business. Let us look at some strategies that can help you prevent contract risk.

Develop a Vendor Contract Review Process:
You should take a consistent and systematic approach to reviewing vendor contracts. Here are just some of the vendor contract sections you should be reviewing and that should appear on your vendor contract review checklist:

- Scope of services
- Service Level Agreement (SLA—we will look this in detail below)
- Duration and termination clauses
- Costs (including any right to modify prices)
- Security and confidentiality
- Audit requirements (ensure you can conduct on-site control assessments, where necessary)
- Reports (for ongoing monitoring purposes, e.g. compliance reports and financial statements)
- Subcontracting
- Indemnification
- Limitation of liability
- Arbitration and governing law

Using an automated platform, you can ensure that consistently high standards apply to vendor contract reviews.

Build a Library of Contract Terms and Clauses:
Keep a repository of frequently used contracts, contract terms and clauses and link them to the vendors that have agreed to them.

Always Consider Renegotiation:
Once you have reviewed a vendor contract, identify any sections that fall below your expectations. Never accept a standardized contract without carefully considering whether it is fair. Do not hesitate to go back to the vendor to renegotiate individual terms. This is where an organized, consistent approach to contract review is essential—it helps you to set your expectations and clarify your standards.

Carefully Monitor Changes:
Always keep on top of contract review and expiry dates. You can do this by assigning a responsible party periodic reminders to review a given contract.

Thoroughly scrutinize the contract detail at each review, comparing it to previous versions and noticing any modifications. Check whether any changes fall within the scope of the contract's modification provisions.

If you retain copies of all previous versions of a contract on your VRM platform, you can track any changes across the history of your relationship with a vendor.

SLA Monitoring

The Service Level Agreement (SLA) sits at the heart of the vendor relationship, providing clear, binding performance requirements. SLA monitoring means ensuring vendors are meeting their obligations under the SLA.

Here are some of the challenges you might face when conducting SLA monitoring:

Disorganized Monitoring Approach:
For too many organizations, vendor performance data -- if collected at all -- is scattered across multiple spreadsheets and databases, oversight is assigned to inappropriate people, and record-keeping is inconsistent. This haphazard approach prevents you from collecting meaningful data and getting the best performance out of your vendors.

Unclear Expectations:
Some SLAs set ambiguous expectations or use imprecise metrics. Unclear expectations can make adhering to the SLA difficult for the vendor—and cause SLA monitoring to become frustrating and meaningless.

Lack of Long-Term Insights:
You can collect reams of data about each vendors' SLA performance, but unless you have a way to process and analyze that data, you will not know which vendors are meeting their obligations and which vendors should be billed for a violation.

Overcoming SLA Monitoring Challenges

Here is how to ensure your SLA monitoring program is as efficient and effective as possible.

Create a Library of Performance Standards:
By creating a set of standardized performance standards, you can assign SLA metrics to each vendor in a fair, consistent way. Reports detail which metrics apply to which vendors.

For example, if your vendor provides customer services, you might assign it an SLA called "average time to answer a call," together with a performance metric, such as "within 10 seconds."

Using a unified VRM platform, you can record whether a vendor has met or exceeded each performance standard and to what degree. You can also record and calculate any financial penalties associated with failing to meet a given standard.

Clearly Assign Responsible Parties:
Who is checking that a vendor meets your performance standards? You should assign oversight for each performance standard and provide responsible parties with clear and actionable duties.

Your VRM platform should provide all the necessary tools for a responsible party to:

- Collect relevant data
- Track a vendor's performance over time
- Hold the vendor accountable

Monitor Performance Trends:
Your automated VRM platform should collect analytics data about vendors' adherence to their SLAs, allowing you to analyze individual and aggregate data about vendors' performance.

Conducting this sort of strategic, long-term SLA monitoring enables you to:

- Detect poorly performing vendors early and take appropriate action
- Revise your performance metrics and thresholds to ensure you are holding vendors to high but realistic standards
- Use real performance data for contract renegotiations
- Improve your vendor sourcing process

Issue Management

Issue management means staying on top of problems—the ongoing process of tracking, addressing and mitigating issues arising out of the vendor relationship.

As any third-party risk management professional knows, working with some vendors can be a headache. Let us look at some of the challenges that can arise when managing vendor issues.

Anticipating Issues:
Any vendor relationship can be problematic—but it is not always clear what issues will arise. If you cannot anticipate the sorts of problems that might arise with a given vendor, it will be harder to spot issues, understand their impact on your organization and respond effectively.

Monitoring Issue Resolution:
Once an issue has arisen, organizations can fail to resolve it efficiently and permanently. Part of the problem is when companies do not actively monitor the resolution process. This means they lose track of who's responsible, what action needs to be taken, and how to stop the problem from re-occurring.

Mitigating the Impact of Issues:
The impact of an issue can be particularly severe if you do not have a clear procedure in place for containing and mitigating it. A disorganized approach to issue management can exacerbate the damage caused by even a minor problem.

Overcoming Issue Management Challenges

To stop vendor issues spiraling out of control, take the following steps.

Anticipate Issues Early
Good planning will help you stop emergent issues in their tracks—or prevent them from arising in the first place. Having taken a systematic approach to risk management at all previous stages of the VRM lifecycle, you should be able to anticipate potential issues early. This means you can put policies in place for mitigating issues once they arise and integrate issue management into your vendor's contract or SLA where appropriate.

Formally Track Vendor Issues:
An automated, organized approach lets you closely track issues from emergence to resolution. Your VRM platform should allow you to:

- Flag issues as they arise
- Assign ownership of a given issue
- Set out the steps that must be taken to resolve the issue
- Track the progress towards resolution

Invite Vendors to Contribute:
Working closely with vendors to resolve issues is crucial. On the same platform you are using to manage and monitor issues, you should be able to invite vendors to submit the actions they have taken to resolve a problem.

To ensure the issue resolution process remains organized and, in your control, you should provide pre-determined elements for a vendor to respond to, such as a checklist of actions it needs to take.

Learn From Issues:
Ensuring an issue is not repeated is just as important as managing it in the first instance.

Good record-keeping and reporting are key. Your VRM platform should enable you to produce reports on issues that can be filtered according to vendors or constituents.

Offboarding

At the end of the VRM lifecycle, you must remove a vendor from your systems, a process known as "offboarding." Offboarding a vendor is no simple task—missing critical steps in the process can lead to security risks and expose your company to liability.

Here are some of the challenges organizations sometimes face when offboarding vendors:

Revoking Access to Data:
Once a vendor is no longer under your control, you must revoke any access it might have to customer or company data. Failing to cut a vendor out of your systems properly can lead to unauthorized access to information—which could qualify as a data breach for which you are liable.

Revoking Physical Access to Premises:
A disorganized approach to vendor management can lead to unauthorized entry to your premises. If a vendor had physical access to your buildings, you must ensure that you revoke such access when offboarding the vendor. You are putting your staff and your assets at risk unless you closely restrict access to your company's property.

Settling Accounts:
Failing to settle your accounts with a vendor can lead to late penalties and reputational damage. If vendor information is scattered across multiple documents, it can be difficult to ensure that accounts are up to date at the end of the vendor relationship.

'Bringing a proper close to your relationship with a vendor is just as important as any of the previous steps in the VRM lifecycle.'

Overcoming Offboarding Challenges

Bringing a proper close to your relationship with a vendor is just as important as any of the previous steps in the VRM lifecycle.

Here are some tips to help you offboard vendors properly.

Keep Comprehensive Records:
Your VRM platform should contain a list of all the data, facilities, and equipment that are accessible to every vendor. Keeping proper records from the start—and retaining all relevant data in one centrally accessible location—will ensure that no vendor falls through the cracks when it comes to offboarding.

Create an Offboarding Checklist:
Use automated VRM software to create an offboarding checklist and assign ownership of each step to responsible employees. This checklist should include blocking access to data, revoking access to premises, and settling accounts. You should also set your VRM platform to remind you of when contracts are due to expire, or a project is reaching completion.

Integrate Offboarding from the Start:
You can use your knowledge of a vendor's inherent risk to scope each stage of the VRM lifecycle. If you know that a vendor will require access to sensitive or personal data, ensure your contract includes a requirement to return or delete any such data in the vendor's possession at the end of your relationship. Including such a clause in vendor contracts is a legal requirement under certain laws, such as the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR).

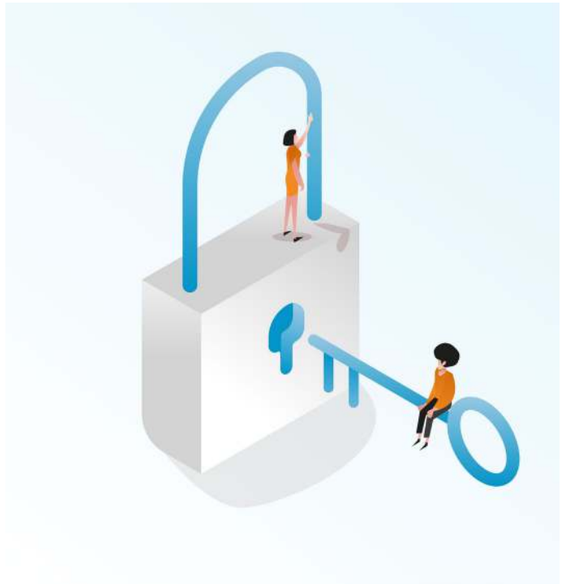
VRM Lifecycle Best Practices

There are two key best practices that you should implement throughout each phase of the VRM lifecycle.

Establish KPIs to Measure Vendor Performance:
Establishing your company's acceptable performance levels—and then monitoring each vendor's adherence to them—reduces risk, reduces waste and expense while building value, growth, and savings.

Continuously Assess Vendors to Manage Risk:
The threats to an organization are continuously changing—whether financial, reputational, or operational. Ensure that you continuously monitor the internal and external environment of the organization and assess the effectiveness of your controls. If you find issues, update them as required.

This level of due diligence will help you minimize vendor-related risks and ensure vendor performance.



Conclusion

Organization goals, stakeholder expectations, regulatory requirements, and risks will shift over time.

By following the VRM lifecycle and implementing a software solution that can quickly adapt to changes, you can make the entire VRM process easier—for all parties involved.

'Organization goals, stakeholder expectations, regulatory requirements, and risks will shift over time.'

ProcessUnity

DVV solutions

About DVV Solutions

We are an authorized ProcessUnity Managed Service Partner (MSP). Our managed services and solutions are proven to improve your ability to assess, analyse and manage more third-party risk domains, utilizing the full power of ProcessUnity's Vendor Risk Management platform to provide:

- Programs for organizations of all sizes and maturity
- Built-in best practices
- Unparalleled subject matter expertise
- Short deployment times
- A documented history of successful client partnerships with hundreds of successful implementations

To learn more about ProcessUnity Vendor Risk Management...

Talk to one of our experts

Contact

ENQUIRIES@DVVS.CO.UK

DVV SOLUTIONS

@DVVS-TPRM

Grosvenor House, Stockport
SK1 3TZ, United Kingdom