THE BEST PRACTICES GUIDE TO VENDOR RISK SCORING

Practical advice to improve scoring and scoping within your Vendor Risk Management program.

ProcessUnity

PROCESSUNITY WHITE PAPER

INTRODUCTION

There's good news and bad news regarding vendor risk management (VRM).

First, the good news: Aside from the OCC guidelines for financial institutions, there is no one legal or professional standard for creating and maintaining appropriate VRM policies—you have a great deal of leeway in establishing your program.

Now the bad news*: Aside from the OCC guidelines for financial institutions, there is no one legal or professional standard for creating and maintaining appropriate VRM policies.* Risk exposure and mitigation is entirely driven by your specific business context: the nature of your work, the range and depth of your exposure, the potential impact of security breaches.

Given this ambiguity, *your organization* is obligated to set standards that encourage confidence within your organization and among regulators. **That's why it's critical that your VRM program rest on a consistent, objective foundation for determining your potential risk exposure (scoring) and the amount of due diligence you must fulfill with any given vendor (scoping).**

The level of inherent risk drives the scope of the due diligence; therefore, the greater the potential risk, the deeper your investigation of third parties. By creating a standardized scoring model, you increase consistency, reduce subjectivity, and accelerate compliance processes. Consistent scoring allows you to prioritize the depth and reach of your due diligence by directing your resources to the vendor relationships with the greatest potential risk, helping you mitigate risk more efficiently.

Keep it simple

To start to create this standardized scoring model, add a third "S" word to scoring and scoping: simplicity. Resist the temptation to create an all-encompassing model, once and for all, that can account for every risk and vendor variable.

Instead, begin with the more reasonable assumption that your model will mature over time. Know that requirements will change and as you learn from experience, you will revise your model to be ever more in line with the risks and realities you genuinely face. Start simply with a system you can run now, anticipating adjustments and improvements you can incorporate as your program evolves.

Fortunately, scoring and scoping need not, and should not, be complicated. In the following pages, you'll discover the essential building blocks for a successful scoring and scoping model, supported with practical insights and suggestions for efficient execution.

01 ASSESS YOUR STATUS

Successful third-party risk management begins with one party: your organization. Only you can see the full range of risks you may be exposed to, and the relative significance of these risks. Before you implement anything new, review your current status. Consider:

- How well *defined* is your program? How much complexity can it absorb or handle?
- What *resources* are available to run and maintain your program?
- What *policies and procedures* do you have in place?
- *Who* are your vendors and how do you monitor your relationships with them? Do you understand what they do on your behalf?
- Most importantly, what are your *key areas of risk* and what controls do you have in place to mitigate them?

If you're beginning from scratch…

The best starting point is to *catalog* your current third parties. At the most basic level, you'll need to know:

- Legal name of the third party
- Primary third party contact information (name, phone, email, address)
- Relationship status (active, terminated, etc.)

As your program matures, you can add:

- Links to relevant contracts
- Links to previous due diligence and follow-up assessments
- Internal assignments—who's responsible for the relationship

Where can you find this information? Usually your accounts payable department is a great place to start: they must have the necessary records to fulfill payments. If you have a procurement department, they can be a useful resource for vendor information and contracts.

02 IDENTIFY YOUR INHERENT RISK

Remember, risk drives scope: The amount and depth of due diligence requirements are entirely determined by the potential risk exposure in any given vendor relationship.

Yet "risk" is not a fixed value, but one that depends on the nature of your work and your appetite and/or comfort level. You must assess your exposure across a variety of dimensions, including by not limited to:

Financial risk: How much money is on the line? Is it entirely your own, or are you responsible for the finances of other parties, such as clients or partners? How much loss can you, or would you, be willing to absorb?

Information Security risk: Consider both your physical *and* your digital assets. What's open to, or shared with, your third parties? How deep is their access? How sensitive is the data that might be exposed?

Regulatory risk: Are you in an industry that must report to regulators? If so, do you have a clear understanding of their expectations? What issues/exposures might trigger their alarm?

Reputation risk: How public or visible is your business? What impact might third parties have on your brand/reputational presence? Are there potentially explosive areas (e.g., child safety, consumer health, data breach) that could adversely impact your reputation?

Geography risk: Do your third parties operate in nations or regions exposed to natural or political disasters? Do they operate within jurisdictions under laws at variance of your native country?

Continuity risk: Is the work your third parties provide integral to your business continuity? Do they have plans in place for disaster recovery? Are they consistent with your plans?

"Inherent" vs. "residual" risk

Risk comes in two related but distinct forms:

Inherent risk refers to the potential for damage *before* you consider the controls that the vendor has in place. Your assessment of inherent risk determines scope: how much due diligence you need for any given vendor.

Residual risk refers to the exposure that remains *after* you've assessed the existing controls. The level of residual risk determines both the cadence (frequency) of third-party risk reviews, and their level of depth.

Look forwards, write backwards

Here's a handy shortcut for composing good questions: look ahead to the reports or scorecards you may be obligated to create (as a matter of internal policy and/or regulatory compliance). Anything you need to report should be reflected in the questions you ask.

Creating the internal inherent risk questionnaire

The principle instrument for monitoring inherent risk is an internal questionnaire, fulfilled by people with your organization, for each third party you have or wish to onboard. Ideally, this would be completed by the relationship manager or someone with comprehensive knowledge of the vendor and services being provided. Because the inherent risk questionnaire defines your initial risk, your questions must be targeted at key risk areas and should be asked consistently across your vendor population; the results will later drive the level of due diligence.

Step 1: Identify your key risk areas

Where is your most significant risk exposure? With your customer interactions? Among your retail branches? With the distribution of sensitive data? In your physical plant? Your questions should be grouped in clusters that target areas meriting your attention.

Step 2: Determine your risk appetite

For each of the risk areas you identified, how much risk can you absorb or feel comfortable with? This appetite can be scaled as granularly as you wish, but at minimum should be classified with low, medium and high designations that reflect relative exposure for your company, and the amount of effort you must invest in risk assessment and mitigation.

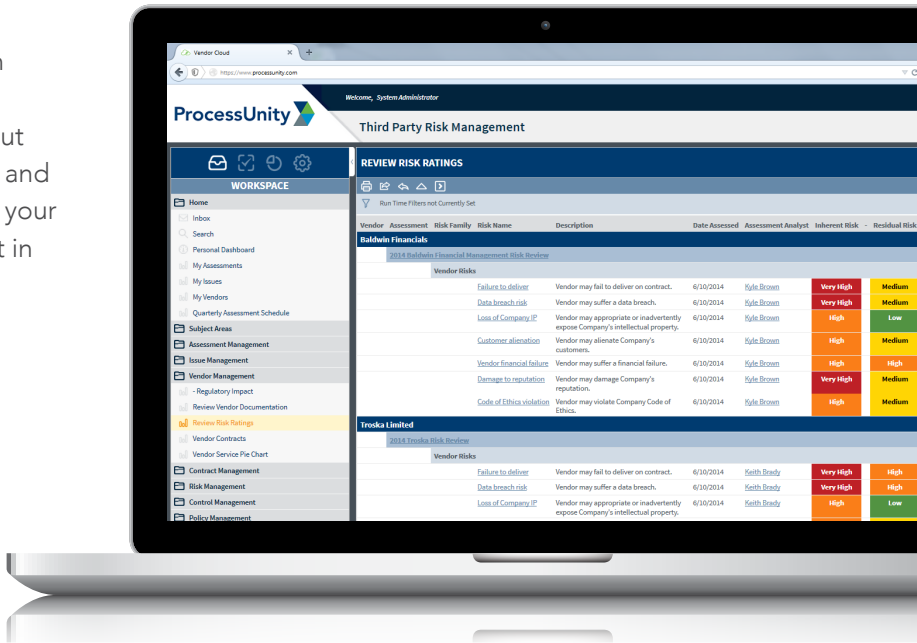
Step 3: Construct your questionnaire

Aside from fundamental contact information, your questions should solicit data reflecting the risk areas you established in Step 1. Your risk appetite, determined in Step 2, drives both the volume of questions for a given area and their depth of inquiry. The inherent risk questionnaire can, and should be, simple; many excellent ones have fewer than ten questions. After all, the goal is only to determine which vendors merit due diligence.

Step 4: Assign vendors to risk categories

After you've completed the inherent risk questionnaires, you assign vendors to risk categories that correspond to the amount of due diligence required. This risk matrix should match your risk appetite, and may be as simple as a three-tier "high, medium, low" rubric. The important point is that the categories have a *meaningful* relationship to both the amount of identified inherent risk, and the amount of due diligence you are willing to invest for that level of risk.

Not all inherent risk assessments are equal. The greatest level of attention should be applied to the key areas of risk in which you hold a low risk appetite.



ProcessUnity

03 IMPLEMENT DUE DILIGENCE

The length and depth of the due diligence process can be tailored for each vendor. Your due diligence investment will be determined by the vendor's risk category, assigned as a result of the inherent risk assessment your internal team conducted.

Your due diligence process mirrors your inherent risk assessment, except that the principle instrument, the due diligence questionnaire, will be completed externally by each vendor, not internally by your team.

Many organizations create a master questionnaire with as many as 500-1000 questions or more, and distribute this to all third parties. In practice, however, it makes sense to pick and choose *which* questions apply to the vendor under scrutiny. The subset of applicable questions should reflect the areas of risk in which a vendor may be involved. A cleaning service, for example, would not need data security clearance, or investigation of its location. But a third-party data center must be assessed for its security policies, its backup and disaster recovery plans, and the relative exposure of its physical location.

Crafting the due diligence questionnaire

Choose relevant questions

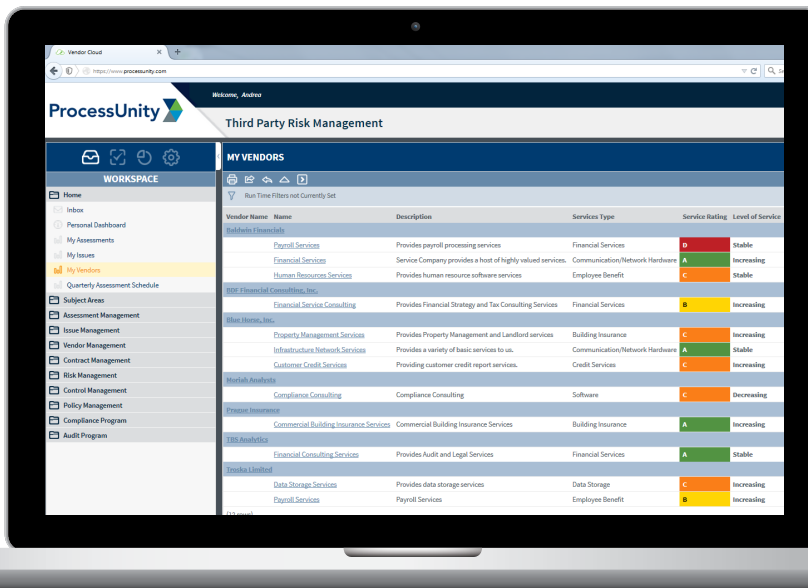
Be selective: Give each vendor subsets of questions relevant to the risk areas that were surfaced in the inherent risk questionnaire. Your payroll provider will need to prove that they are protecting employee data; your lawn crew just needs to prove that they perform background checks on their staff and that the company is insured.

Write meaningful questions

Your goal is to collect answers that quickly reveal the essence of any potential risk. You want precision, not ambiguity; specificity, not abstraction; clarity, not clutter. To get more meaningful answers, craft more meaningful questions:

- **Speak in plain English:** Avoid jargon-heavy "regulatory-speak" and express your questions as simply and directly as possible.
- **Limit the number of open-answer questions:** Open-answer questions are too open to interpretation. Reduce confusion by writing as few of these as possible; when they cannot be avoided, keep them simple: you want facts, not explanations.
- **Use pick lists**: Provide radio buttons or check lists of items respondents can choose among. These lists reduce ambiguity and increase precision.

Pick lists make your questionnaires easier for respondents to fulfill while providing you with more precise, factual answers.



ProcessUnity

04 WEIGH YOUR RISK

The due diligence questionnaire surfaces facts; to assess their significance, you must weigh the responses. There are two fundamental approaches to weighting questionnaire answers:

Numeric

In the numeric approach, you assign a point value to each question. The sum of the cumulative point values gives you a number you project onto your previously defined risk appetite. For example:

- A sum of 0-50 may indicate low risk that requires little or no further investigation.
- A score of 51-80 might trigger a basic due diligence process that includes a questionnaire submitted to the vendor, plus necessary follow-up.
- Anything above 80 could lead to deep due diligence, perhaps a more lengthy vendor questionnaire plus in-person visits to confirm that controls are in place.

You may score the entire questionnaire as a whole, or create scores for individual risk area question sets; the latter method gives you the flexibility to stagger your vendor due diligence, touching lightly on areas of low risk, while pursuing high risk areas in more thorough detail.

Issue-based

Issue-based evaluation reviews responses to *identify gaps* in policies, procedures or controls. Based on your business policy or protocol, these gaps can be severity rated. The "score" of this assessment would be based on the number and severity of the gaps identified during the process.

Example:

- More than 1 High severity gap = Unsatisfactory
- 1 High or 3 Medium severity gaps = Requires Attention
- 0 High, < 3 Medium severity gaps = Satisfactory

With the assessment score as a guide, actions may be required to mitigate or accept the risks identified. All findings should be tied to the key risk areas and/or company standards identified within your third party policies and procedures for applicable management and audit requested reporting.

Pros and cons of assessment approaches

Numeric:

Pro: Limits personal subjectivity, supports weighted averages, calculation oriented

Con: Can create unnecessary complexity, important evidence of risk may be obscured within the larger quantitative valuation

Issue-based:

Pro: Reduced false positives, more readily targets important risk areas, limits attention to trivia

Con: Introduces greater subjectivity, can require higher skilled resources for due diligence review, may lead to some inconsistency across vendors

What to do with your scores

Many organizations are concerned, even anxious about, the regulators' response to their scoring methodologies. In ProcessUnity's experience, and in the experiences of its clients, examiners have little interest in challenging your policies. Instead, they want to see that you have a scoring system in place, that it rationally corresponds to your exposures, and that it is applied consistently across your vendor population.

Further, just as your vendor lists and identified risk areas should be periodically reviewed to ensure relevance, you should anticipate regular reviews of your methodology to be sure it accurately captures the risks that naturally evolve in character and consequence over time.

Anticipating follow-ups

Your vendor's responses to the due diligence questionnaire, and your scoring, determine what subsequent steps, if any, may be required. Inform your judgment by:

Assessing your residual risk

Given the controls in place, how much residual risk remains for each vendor? The amount, depth, and potential consequences of residual risk drive the amount of follow-up due diligence.

Addressing open issues

Upon review, some third parties may require further due diligence, such as on-site visits or due diligence of *their* vendors. Be sure you have a process in place that assigns follow-up responsibilities and provides a means for recording issue status. VRM applications with workflow tools can automate the process and provide an easy window for monitoring progress.

Planning subsequent reviews

Managing third-party risk is an on-going effort. But just as the amount of initial due diligence is determined by risk level, so too is the amount and cadence of subsequent reviews; the greater the residual risk, the more frequent your subsequent reviews; the less risk, the less frequency.

ProcessUnity

CONCLUSION

Do you follow these best practices?

VRM can be so much easier and more efficient when you standardize the way you score and scope your third party vendors. Use the following checklist to assess your current status.

If you're unable to answer "yes" to most or all of the questions below, it may be time to talk to a VRM expert at ProcessUnity by writing info@processunity.com, visiting www.processunity.com, or calling 978.451.7655.

YES	NO	I DON'T KNOW	
○	○	○	Do you know the nature and/or extent of your current third party risk management program?
○	○	○	Have you assembled one complete catalog of third party vendors?
○	○	○	Have you identified *your* key areas of risk?
○	○	○	Have you assessed your risk appetite?
○	○	○	Can you determine your inherent risks in crucial business areas such as finance, security, reputation, continuity, etc.?
○	○	○	Do you have a master inherent risk questionnaire?
○	○	○	Does your inherent risk questionnaire accurately reflect your genuine risk areas?
○	○	○	Can you appropriately weight your answers by relative risk exposure?
○	○	○	Do you have a system, numeric or issue-based, for assigning weights?
○	○	○	Do you use your scores to drive the scope of due diligence?
○	○	○	Are your due diligence questionnaires correctly tailored to your vendors?
○	○	○	Can you write meaningful questions that reduce ambiguity and reveal specific facts?
○	○	○	Do you have plans for follow-up due diligence?
○	○	○	Can you automate the follow-up workflow?
○	○	○	Do you use your assessment of residual risk to set the cadence for subsequent reviews?

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 customerdefined 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

Organizations as small as community banks and as large as Fortune 50 companies rely on ProcessUnity for effective and efficient vendor risk management. Ready to learn more? Watch a five minute demonstration or click here to contact us today.

View Video

ProcessUnity

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States