BUILD AND SCOPE BETTER VENDOR DUE DILIGENCE QUESTIONNAIRES

ProcessUnity

PROCESSUNITY WHITE PAPER

The business world is more fast-paced than ever, and it's common for companies to outsource work to keep up. You don't have to be the best at everything, so long as you can hire the best. However, delegating work to third-party vendors can expose your company to unexpected risks. And it is critical that you appropriately identify, assess, and manage that risk.

You can outsource a service, but you can't outsource the risk that comes with it. It's necessary to perform vendor due diligence to ensure that you keep tabs on any risk your third party may expose you to so you can enable your organization with secure, high-quality partnerships.

The importance of doing due diligence right can't be understated. According to Black Kite's 2022 Third Party Breach Report, there were "more than 200 publicly-disclosed headline breaches and thousands of other inherent ripple-effect breaches throughout 2021." With thorough due diligence, you can significantly minimize the chance that your organization becomes the next victim of Log4j or Solarwinds, potentially saving your reputation and financial standing. This whitepaper will discuss how to protect your organization from third-party risk while saving money and time with proven scoping strategies for vendor due diligence.

> "There were more than 200 publicly-disclosed headline breaches and thousands of other inherent ripple-effect breaches throughout 2021."
>
> BLACK KITE'S 2022 THIRD PARTY BREACH REPORT

ProcessUnity

VENDOR DUE DILIGENCE

Due diligence is the process of fulfilling legal requirements and researching a vendor before investing in their services and/or products. Think of it like doing a home inspection before signing a mortgage — you have an obligation to your company to ensure any vendor you bring in meets your company's standards.

Why do we perform vendor due diligence?

Due diligence measures and mitigates your company's potential exposure to risk through the relationship.

Potential risks (not all-inclusive):

- Data breaches
- Regulatory fines
- Employee turnover
- Customer dissatisfaction
- Missed opportunities
- Damaged brand reputation
- Product failure
- Financial loss
- Business failure

Vendor Due Diligence Timing

Although due diligence is a continuous process, it occurs in three stages:

1. **Pre-Contract**
2. **Post-Contract**
3. **Event-Driven**

Pre-contract

During pre-contract due diligence, you identify and mitigate potential risks prior to onboarding the vendor relationship. This includes determining the scope of the relationship, building a questionnaire to send to third parties, and evaluating risk based on responses. A platform that stores questionnaires, flags preferred/non-preferred responses, and compiles vendor risk assessment scores is indispensable here.

There are many industry-standard questionnaires that can properly assess risk in target areas, such as SIG Core and SIG Lite. However, it may be necessary to create hybrids to account for constantly changing roles and regulations. Be sure to consult with a vendor risk assessment expert to determine the best path for your company's needs.

Post-contract

After the contract is signed, you must implement ongoing monitoring cadences to identify changes in a vendor's risk posture. Reevaluate each vendor's risk levels on a regular basis to cover contract renewals, regulatory changes, and anything that may have changed since the last risk assessment.

Regulatory changes happen often, and there's a recent push by agencies like the Securities and Exchanges Commission (SEC), Federal Deposit Insurance Corporation (FDIC), and more to tighten regulations. These changes come on the heels of an Executive Order on Improving the Nation's Cybersecurity from the White House.

Event-driven

Unexpected risks come up due to events out of your control, like the Coronavirus pandemic. You should break from the review schedule when unexpected risks occur to ensure you're assessing risk in light of current events, like negative news, a cyberattack, natural disasters, financial events, geopolitical events, and other business-altering occurrences.

What are Some Common Due Diligence Challenges?

Although meant to pinpoint risks before they can pose long-term problems, due diligence has challenges of its own. Accounting for these obstacles is essential in developing and executing a workable strategy. Here are six common challenges to expect when conducting due diligence in manual processes, outdated tools, or ineffective workflows:

1. **Due diligence processes** are labor-intensive and there may not be adequate resources to properly vet the entire vendor portfolio of a company.
2. **Lengthy, one-size-fits-all questionnaires** need to be built and maintained, completed by vendors, and reviewed by risk analysts on schedule.
3. **Response timeliness** is better pre-contract, as both organizations and third parties can become complacent during an existing relationship.
4. **Response Completeness** can affect the accuracy of vendor risk profiles. It's important to get complete answers from each vendor and follow up on any ambiguities.
5. **Too many vendors to assess** will bog down a manual process. This leads to assessment fatigue and backlogs, which could potentially cause you to onboard a risky vendor without the appropriate controls.
6. **Disconnect across various frameworks,** regulations, and standards can make it difficult to determine exactly how to assess your vendors.

Why Proper Scoping is Key

It's important to properly scope every vendor risk assessment, as not all vendors pose the same risk. Think about it: a landscaper who only works outside has much less access to internal systems than an IT vendor. The inherent risk that a vendor poses to your organization determines the scope of a vendor's interaction with your company resources. You will have far more questions to ask a higher-risk vendor than one with lower risk and less company resource interaction.

Does the third-party service have access to your technical infrastructure? This might be one of the most important questions you can ask during due diligence. If the response is a 'yes,' you will need to ask the vendor a list of questions about their own security practices and policies. It's critical that you assess every vendor that touches your data, assets or systems with the right questions to prevent a potential breach.

Performing the same amount of due diligence on every third-party vendor by distributing a one-size-fits-all questionnaire poses the risk of over-assessing lower-risk vendors and under-assessing higher-risk vendors. When you scope your questionnaires right, you only ask relevant questions to your vendors based on the nature of the service. **As a result:**

- Vendors will respond faster
- Your team will review only what's necessary
- You measure risk more accurately
- You can effectively assess more vendors in less time with the same resources

Risk Domains

Depending on the vendor's service type, the risk that they present to your business may fall within one or more key domains. Understanding the importance of each of these areas to your TPRM program will help you to better prioritize the scope of your assessments.

These include:

- Business Continuity
- Compliance
- Cybersecurity
- Financial
- Fourth Party
- Geography
- Information Security
- Legal
- Physical Security

What's In-Scope?

There are certain factors that are important when determining the right scope of assessment for each vendor. This is not a comprehensive list of questionnaire topics, but simply a starting point to ensure your due diligence covers the necessary areas.

Business Information

- Articles of Incorporation / Charter
- Business License
- Company Structure
- Ownership Information
- Executive / Board Member Bios
- Service Deliver Location(s)
- References

Financial standing

- Financial Filings / Annual Report
- Tax Documents
- Balance Sheets
- Assets & Liabilities
- Compensation Structure

Reputation

- Watch Lists / Sanction Lists
- Politically Exposed Persons
- Negative News
- Negative Reviews / Public Complaints
- Legal Cases
- ESG Record

Insurance coverage

- General Liability
- Cybersecurity Insurance

Tech infrastructure

- Control Audits / Statement of Controls
- Incident History
- Business Continuity / Resilience Plan
- Disaster Recovery Plan
- Penetration Tests / Cyber Ratings
- Training / Awareness
- Policies and procedures
- Information Security
- Customer Support
- Privacy
- Data Retention
- Hiring / Termination
- Diversity

Changing with the Scope

Scope varies throughout the vendor lifecycle as both your business and the market change. Adapting to these changes while adjusting your scope keeps your target in focus. **The following are common questions to ask during the pre-contract and post-contract due diligence phases, along with risk domains to keep an eye on:**

Pre-Contract Scoping

- Is this an existing or new supplier/service?
- What is the nature of the product/service? (All vendors/services/locations/facilities are not equal)
- How essential/critical is the product/service to your business operations?
- What level of access is the third party granted?

Post-Contract Scoping

- What is the risk level of the relationship after the appropriate controls have been implemented?
- What is the vendor's inherent/residual risk tier – high, medium or low?
- Have there been any changes to the vendor's risk level since their last assessment?
- Is the assessment driven by a contract renewal or amendment?

TIPS AND TRICKS TO BUILD AND SCOPE YOUR DUE DILIGENCE QUESTIONNAIRES

Due diligence is an intricate process that requires planning to execute well. The tips and tricks below will help you rethink how you approach your pre- and post-contract due diligence:

1. Building Due Diligence Questionnaires (DDQ)

Using a master DDQ as a template to build refined questionnaires speeds up procurement, assesses vendors uniformly, reduces the need for on-site assessment work, and keeps risk out of the business, both pre- and post-contract. As mentioned above, consider using an industry-standard questionnaire as a starting point, but be sure to personalize it to your specific business needs.

Questionnaire Tips

1. **One Size Fits All** = One Size Fits None
2. **Build a Library** of question sets specific to frameworks, regulations, and standards, including:

- NIST
- NYDFS
- PRA
- ISO
- CCPA
- PCI
- GDPR
- EBA
- HIPAA

Keep in mind that these standards change regularly, and you'll be held accountable to them regardless of whether you're informed.

3. **Industry-Standard Questionnaires** give faster response times and more complete responses while lowering vendor fatigue. However, you may need to send additional questions to construct a proper assessment for your business' unique concerns. The industry-standard questionnaires below are a great starting point for your DDQ.

- Standard Information Gathering (SIG) from Shared Assessments
- Consensus Assessments Initiative Questionnaire (CAIQ) from Cloud Security Alliance (CSA)
- Best Practices Questionnaire (BPQ) from TruSight

4. **The Hybrid Model** lets you select relevant questions/sections from an industry-standard questionnaire and augment them with your own propriety questions/sections. This lets vendors submit their completed industry-standard questionnaire and only respond to the questions not already covered. Ultimately, it speeds response times and helps ensure completeness.
5. **Auto-Scope Sections** based on factors like service types, inherent risk, and facility location. An automated assessment tool that uses conditional logic to show vendors relevant questions based on based on their in-flight responses. For example, if a vendor has access to personally identifiable information (PII) on citizens of European countries, then the GDPR question set will automatically be added to the assessment.

   Dynamic in-flight scoping will help you to ensure that your questionnaires are relevant to the vendor's unique profile, reducing both vendor and analyst fatigue.

6. **Other Considerations include:**

- If you have a question-level scoring system, do not show the vendor. They may be tempted to change their responses to improve their score.
- Limit text-based answers as much as possible to ensure consistency/objectivity in analyst reviews.
- Require attachments only where necessary and only ask for what's relevant to the review.

2. Scope Based on Service Type

To fit the risk that each vendor presents, leverage different question sets and scoring systems based on characteristics, like:

- Service type
- Contract amount
- Service location
- Data access

Do your best to formalize a base rating system regardless of the service and scope. This will give you the clearest picture of your overall organizational risk across all vendors, considering each level's access to and effect on internal resources.

3. Post-Contract Due Diligence: Scope Based on Inherent Risk

Inherent risk drives assessment scope for ongoing due diligence. Not all vendors in your database require the same level of attention throughout the relationship. But it's also important to understand possible hidden risks that weren't identified during onboarding. For instance, smart technology (including Wi-Fi connectivity) is hidden in seemingly innocent places like an aquarium or coffee maker, both of which have compromised businesses in the recent past. Scoping due diligence based on inherent risk helps you to monitor for these incidents based on priority, such as access level or risk criticality.

A low-risk vendor requires lighter scope than a medium, high, or critical risk vendor. The DDQ that each vendor will receive is scoped to the level of risk they present based on the inherent risk assessment. Additionally, inherent risk can determine the frequency at which you assess a vendor. A lower-risk vendor should be assessed on a less frequent basis than a higher-risk vendor.

Formalize a base rating system. This will give you the clearest picture of your overall organizational risk across all vendors.

4. Use Expert Vendor Intelligence in Scoping

Vendor risk intelligence can be difficult to obtain objectively. You shouldn't take the data you get from vendors during due diligence at face value, as subjectivity can insert itself even with targeted questions. Today, it is a best practice to validate data gathered during due diligence with external content such as ratings and reviews. **There are several trustworthy sources to verify data from both a customer, regulator and employee perspective, including:**

Cybersecurity Ratings

- BitSight
- RiskRecon
- SecurityScorecard

Financial Health Scores

- Rapid Ratings
- Dun & Bradstreet

Environmental, Social, Governance

- EcoVadis

ABAC / UBO and Adverse Media

- Refinitiv
- Sprout Social
- Muck Rack

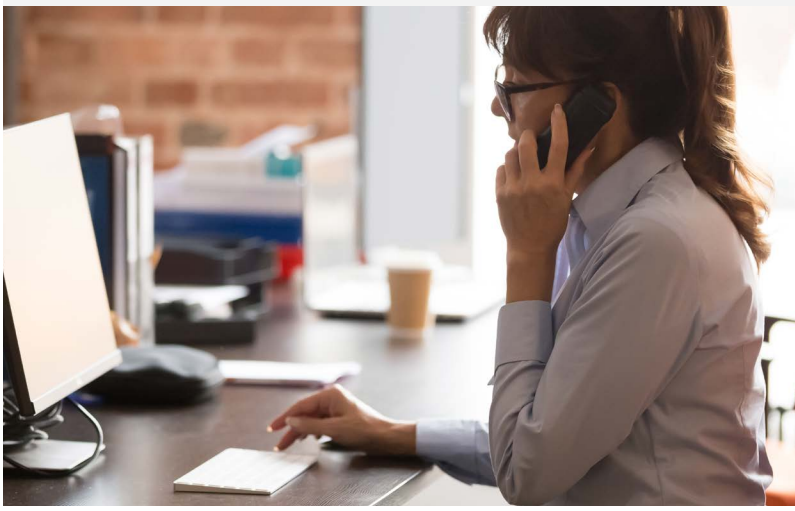
Free Resources

- Stock Tickers
- Financial Filings
- Google News Alerts
- Crunchbase
- Glassdoor
- LinkedIn

- **ProcessUnity Targeted Risk Intelligence: Vendor Intelligence Suite**
  - Vendor Identity Intelligence
  - Vendor Screening Intelligence
  - Vendor Cyber Intelligence
  - Vendor Financial Intelligence
  - Vendor ESG Intelligence

  VIS enhances Third-Party Risk processes with targeted risk intelligence for a more accurate and informed onboarding process and deeper due diligence in specific risk domains with contextually embedded ratings. With automated ongoing monitoring, issue identification and creation, and streamlined reporting capabilities, ProcessUnity VIS provides organizations with a comprehensive view of the health of their vendor ecosystem.

  Using VIS, vendor managers can augment their onboarding processes, vendor assessments, and ongoing monitoring with domain-specific content to accelerate and improve their risk-based decisions.



NEXT-LEVEL STRATEGIES

Once you've completed the basic foundation for streamlined due diligence, it's time to implement more advanced strategies to refine your strategy and bring it to the next level with the following tactics.

1. Establish Enterprise Controls

The first step toward improving due diligence is to consolidate enterprise controls. The leading way to do this is to utilize a control metaframework that eliminates duplicative controls across your regulations, standards, and business data. At the end of the process, you should have complete control coverage that can be tested a single time internally and externally. It also allows you to more swiftly adapt when these regulations inevitably change.

2. Scope Questionnaires Based on Controls

Automatically scope questions based on controls and vendor characteristics. First, align questions to the regulations and standards included in your control library, like NIST CSF, SOC II, PCI, GDPR, CCPA. Next, scope 'access to data' questions. If the third party has no access to sensitive data, they will receive a lighter set appropriate to the risk level they present to decrease the risk of vendor fatigue.

After that, scope business-specific regulation questions that haven't been scoped out with your controls. Finally, scope additional domain questions, so if a third-party service is hosted in the cloud, they remain compliant with ABAC and ESG regulations at a minimum.

3. Relate Third-Party Responses to Your Controls

The federal government uses the GOV-01 – Security & Privacy Governance Program standard to control access to its secure information. Although you won't be held accountable for this (unless you have a federal government contract), it still contains valuable information to follow and a great rating system to implement for your third-party responses, **like the following question:**

Does the organization staff a function to centrally-govern cybersecurity and privacy controls?

5 – Continuously Improving

4 – Quantitatively Controlled

3 – Well-Defined

2 – Planned & Tracked

1 – No

Asking your third parties questions like this can help you quantify how well your controls are enforced externally. You can compare the third party's response to your organization's preferred rating for the control.

EFFICIENCIES OF AUTOMATED CONTROL-BASED SCOPING:

Automating your control-based scoping is the most efficient way to conduct due diligence. With a platform like ProcessUnity Vendor Risk Management, you can configure your questionnaires to show or hide questions in-flight based on vendor responses and your control priorities. Organizations that use these systems report consistently report three major benefits:

1. Align Internal and External Controls

Building a questionnaire based on controls that are important to your organization — and nothing more — allows for purpose-based questions that truly determine if the level of risk a vendor poses is appropriate for your business. This process enables dynamic questionnaires and **lets you evaluate the effectiveness of your internal controls and see how vendors rate with their version of those controls.** When the company's controls are tied to the vendors, you can see them as a complete ecosystem.

2. Faster, Cost-Effective, Low-Error Response Analysis

With automated processes, you'll increase the likelihood of a faster assessment response time from vendors, allowing your organization to appropriately determine their risk level and the appropriate level of ongoing monitoring to conduct post-contract. Removing the human labor and other costly stages of assessment creates a more efficient, low-to-no error assessment that requires minimal repetition for correction. T**his allows the company to scale and accommodate even more vendors with less manual effort.**

3. Controls In Compliance Reporting

Automated due diligence improves compliance by helping you to quickly pinpoint coverage gaps in your third parties. Controls-based scoping means you take on your vendor controls and have better visibility into the risk they bring, setting your company up for more proactive risk mitigation. But it also exposes any holes that need to be patched in your internal controls. **ProcessUnity VRM can identify trends on a program-level view of every control, along with compliance of each third party.** No matter how widespread, large, and complicated your organization may be, the system will adapt to your exact specifications to keep you ahead of emerging regulations.

KEY TAKEAWAYS:

Conducting proper due diligence is vital when onboarding a vendor. You are ultimately responsible for all regulatory compliance regarding the safety and security of your customers' sensitive data and you will be held accountable for engaging with a third-party that uses illicit practices. Further, you must ensure that critical counterparties are able to satisfy your business requirements. Without a comprehensive understanding of the internal controls a potential vendor has, you could potentially onboard a vendor outside your risk tolerance, inadvertently jeopardizing the security of your organization.

It's imperative to properly scope your vendor's risk and execute a streamlined process to efficiently ensure your third-party vendors are compliant with the same regulations and security controls your organization is held accountable for. In reading this guide, you learned how to scope vendor risk assessments while keeping them accurate and objective across the board.

You now know how to use regulatory frameworks as a starting point to adapt questionnaires to your specific business needs, and resources to perform deep due diligence on every aspect of a potential vendor's business. **While conducting due diligence, keep these six important takeaways in mind:**

1. **Remember the Goal:** Keep Risk Out of Your Business
2. **Not all Vendors are the Same,** as some bring either Inherent Risk or require Service-Based Scoping.
3. **Adequately Define** Risk Domains
4. **Consider External** Expert Content
5. **Don't Overdo** it with Policies & Procedures
6. **Scope Based** on Your Control Framework

An important aspect of automated due diligence that cannot be understated is the ease of use for both vendors and your organization. Vendors often have to fill out lengthy questionnaires that do not equip organizations to adequately assess their risk level, fatiguing both the vendor and assessor while potentially missing relevant threats. With ProcessUnity templates, the ability to customize every element, and in-flight scoping, ProcessUnity will make sure that your organization is protected from risk.

Request a demo to learn how the ProcessUnity Assessment Engine improves efficiency in your pre-and post-contract due diligence process with auto-scoping.

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

Next steps

Request a demo to learn how the ProcessUnity Assessment Engine improves efficiency in your pre-and post-contract due diligence process with auto-scoping.

REQUEST A DEMO NOW