

GUIDE FOR COLLECTING VENDOR DUE DILIGENCE

Due diligence is a time-consuming, complex and cumbersome task.

As a best practice, it's an approach to assessing vendors that should be risk-based, scaled appropriately and conducted both prior to contract signing as well as throughout the term of engagement. Let's go through the game of what it actually takes to collect vendor due diligence and to do it well.



SET THE PLAYING FIELD FOR DUE DILIGENCE

Due diligence is a big job, but you have to start somewhere. Before you do, it's good to have a "big picture" idea of how it should operate.

Here's how the general flow usually works:

1

Gather Information

Have your business owner provide or validate details about the vendor. This is often done by way of an internal questionnaire to determine the vendor's inherent risk.

2

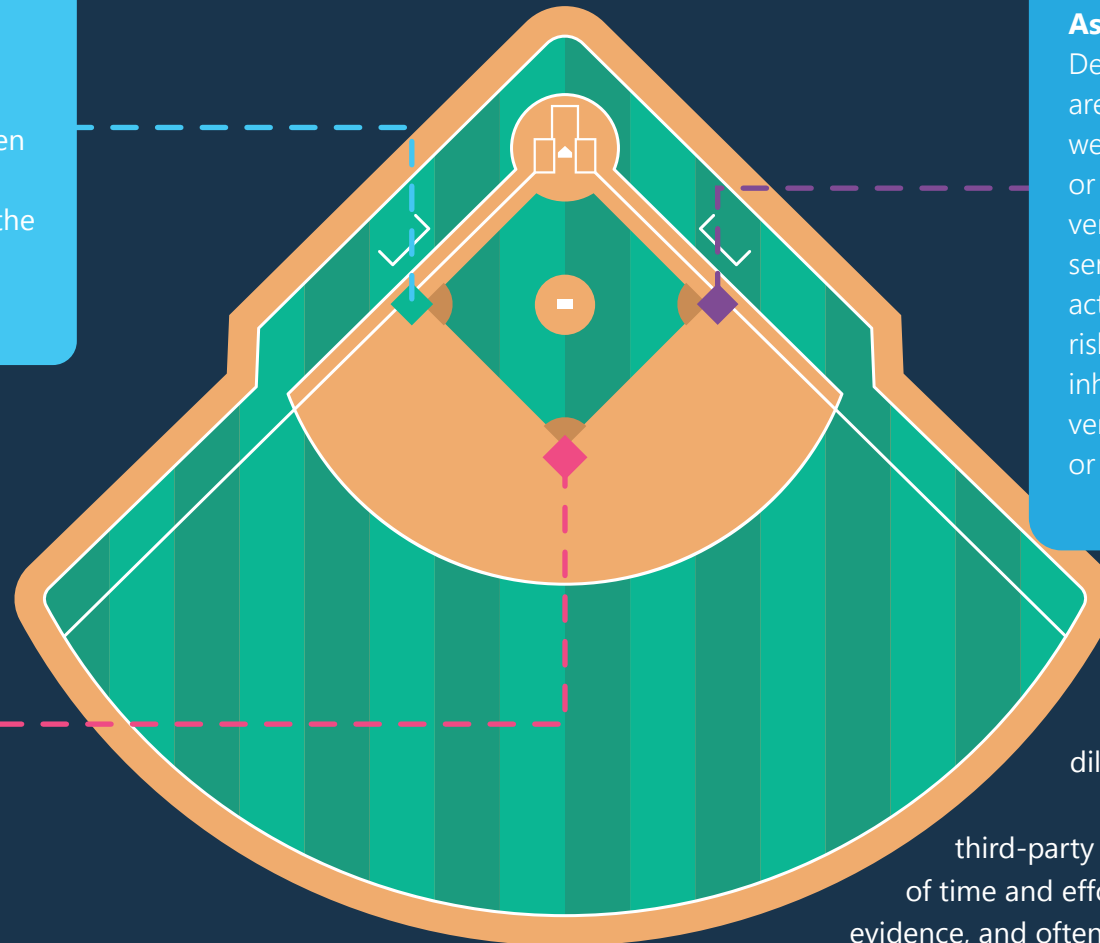
Reach out

Get in touch with the vendor and request they answer a list of questions and provide various documents. Keep tabs on this request and review the information they provide.

3

Assess controls and risk

Determine whether or not there are any issues or control weaknesses that need follow up or remediation. Work with the vendor, business owner and/or senior leadership until the actual residual risk – remaining risk after mitigating as much inherent risk as you can – of a vendor is adequate, accepted or remediated.



The standards your organization sets for due diligence must be attainable with the resources dedicated to third-party risk management. It takes a lot of time and effort to assess large quantities of evidence, and often, specific areas of expertise. It's not practical to have a standard for collection that can't be adequately managed and analyzed, as that'll lead to inundation and inefficiencies.

LET THE DUE DILIGENCE GAMES BEGIN

Phase 1: The Windup

You must understand the vendor engagement before you can determine the appropriate due diligence.

Scale due diligence based on risk and criticality. When you ask too much of low-risk vendors, too little of high-risk or critical vendors, or simply ask for things that don't make sense, it takes a lot of time to re-adjust the approach and settle confusion.



Before reaching out for due diligence, another good trick to have in the bag is understanding the contract terms as they pertain to your request.

In a perfect world, all of our contracts would come with a clause which automatically requires compliance with our due diligence requests, but that certainly isn't always the case. It's good to know how much support you do and don't have in the contract before asking your vendor to cooperate with your request.

Keep business owners informed of the overall status of their vendors' assessments.

Be communicative as they may have some important information to consider as part of your review.



Phase 2: The Pitch

Send a formal, polite and well-organized due diligence request to the vendor which includes the following:

- An introduction (your title, your organization name, etc.)
- The reason for your request
- Details around your request
- Specific turnaround time
- Ongoing expectations

While templates are important to have, be wary of relying on them too much, as a carelessly unrevised template can weaken your credibility.

Stay on top of follow ups.

Set reminders in your calendar to follow up close to your requested turnaround time.



Phase 3: “Field” their deliverables appropriately

As you receive due diligence, do the following:

Be sure to conduct a timely analysis.

Very often, documentation and questionnaire responses come back in fragments. Even the best thought-out due diligence packages have their gaps. Provide timely follow-up if you need any additional items.

Determine if the vendor meets your expectations.

If they don't, follow your process for remediation. Follow the same steps for requesting information, changes, recommendations, etc.

Phase 4: Bring It Home

Finally, be sure to let all parties know when the review is completed and report the results

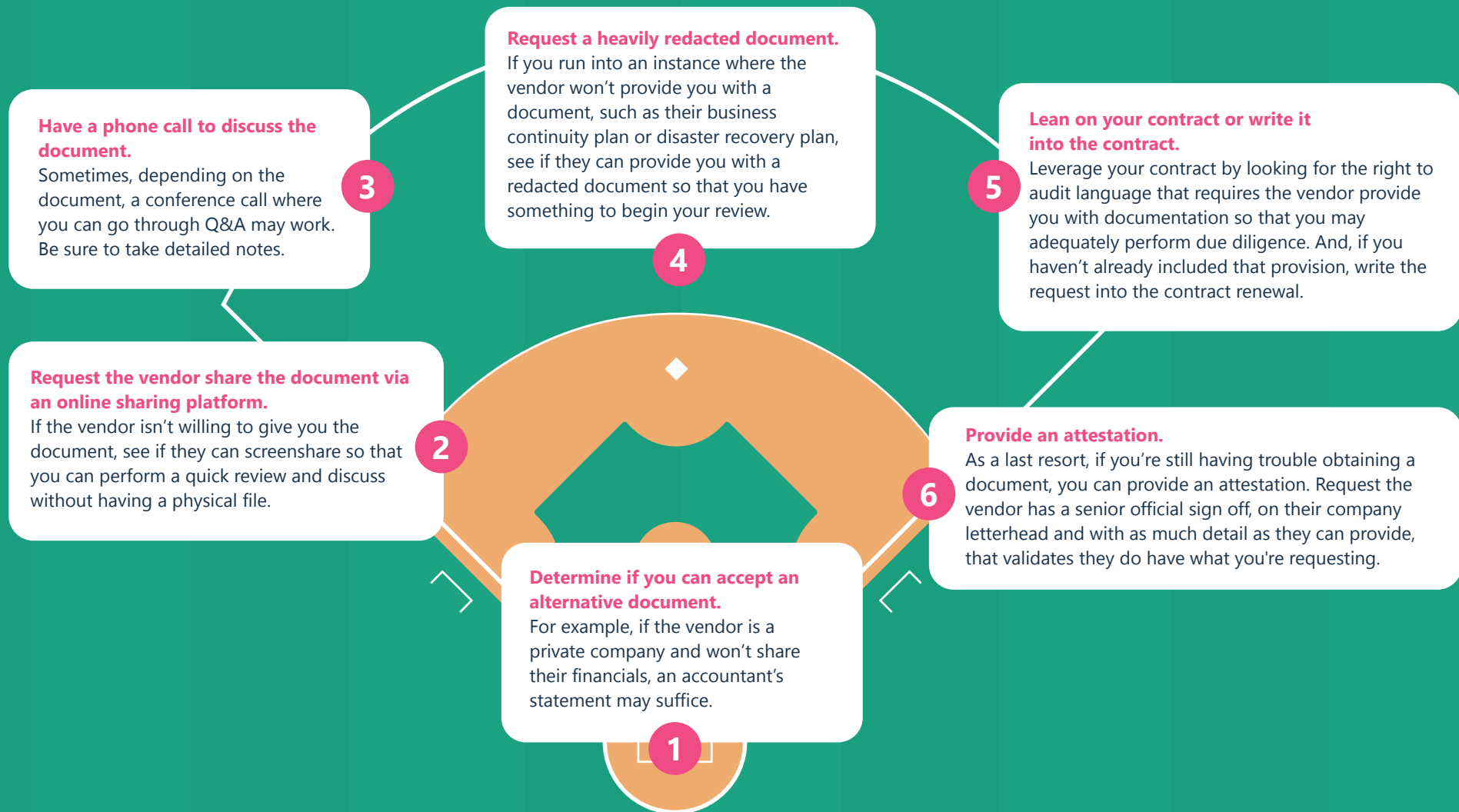
in accordance with your organizations prescribed parameters for third-party risk management reporting.



6 CREATIVE TACTICS WHEN THE VENDOR WON'T PROVIDE DOCUMENTATION

Sometimes, it can be difficult to get the vendor to provide what you're asking for.

Whatever the reason may be, here are some creative ways to help work around the situation:



3 DUE DILIGENCE TIPS AND TRICKS



1 Understand where you might have wiggleroom in documentation requests and provide it to your vendors when able.


While it helps your process to standardize due diligence requests, it's important to remember that there are many different ways to gain adequate control assurance for any given vendor. Work with your vendors, and they'll work with you.

2 Documentation is key.

The more information you capture, track and document about your assessment process, the better. Good tracking can assist with issue resolution, escalations, required metrics reporting, litigation, trend analysis and more.


3 Collect data in controlled and filterable fields.

A tool with these capabilities will greatly assist with reporting and trend analysis. Try to avoid putting all your information in one text box. For example, make sure you can sort by review start and end date, inherent risk, residual risk, critical/noncritical, etc.



While collecting and managing due diligence is a time-consuming task, it's one of the most important elements of a strong third-party risk management program.

We'll leave you with a secret play:
When collecting due diligence, it's always easier to catch a fly with honey than with vinegar.





Download free sample assessments of vendor controls and see how Venminder can help you reduce your third-party risk management workload.

DOWNLOAD NOW



Manage Vendors. Mitigate Risk. **Reduce Workload.**

(270) 506-5140 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online library. The assessments enable clients to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance and more.