INFO~TECH
RESEARCH GROUP

The Duty of Due Diligence:

Examining your vendors could prevent disaster

Summer 2023

By Frank Sewell

Introduction

It should go without saying that most of us would never buy a home without some level of due diligence. We want to know what sort of neighborhood it is in, the flood zone potential, how much the average utilities were for the last year, whether it is under termite contract, and we'd want to get an inspection done (many of these qualifications are required before a bank will fund a mortgage or an insurance company will set a replacement value). We innately understand that our investment in such a large enterprise could be a potential disaster (both financially and personally) if we do not look at our options. Still, we often take shortcuts for expedience when it comes to business.

Organizations buying software, hiring professionals, or entering a relationship with another party face many kinds of potential disasters when picking the wrong partner. *I am using "partner" here liberally. You should evaluate the effectiveness of each relationship separately.* These potential disasters can be anything from a reputation hit to losing data, money, or the ability to operate effectively.

Is Your Vendor Really Your Partner?
— Info-Tech Research Group

Due diligence grants us a glimpse into the potential risks that might be involved when entering each vendor relationship. More importantly, the process allows us to continually reassess the nature of the relationship, the risks, and how we can potentially mitigate those disasters from happening.

What Due Diligence is NOT

A way to avoid formal risk assessments.

Due diligence is part of the process of exploring a relationship with a vendor and informs your organization in the risk assessment process. The information gathered through due diligence determines further questions to quantify the inherent risk associated with using the vendor for the required services so that you can target potential mitigation efforts.

> ***Inherent risk:*** *The risk to your organization from a vendor before any mitigating actions are taken to lower the impact.*
>
> ***Residual risk****: The risk remaining after mitigations are in place.*
>
> *— Wikipedia*

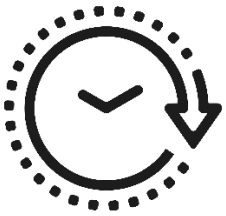
A one-time activity

ONGOING MONITORING CADENCE

- *Annually*
- *Major Updates*
- *Renewals*
- *When Security Changes*

Due diligence needs re-performing periodically to ensure that new factors have not caused a shift in your understanding of the relationship. Vendors often change their security posture or data hosting locations; they reduce employees or move to alternate geopolitical locations to maximize profits or overcome a shortcoming. They rarely inform their customers of such measures, and you may not discover the change occurred until an incident happens. Establishing a cadence of ongoing monitoring enables your organization to revisit the vendor's posture so that you can either hold them accountable for redressing the issue or have an option to terminate the relationship.

Adding language to your agreements can secure your right to audit the vendor's compliance and sever the relationship if the vendor breaches. If your organization has a mature risk management group, you can set risk thresholds as triggers for breach. Include factors such as denigration of security, financial health, and other criteria. See the examples below for additional points to consider. Be sure to add language stating that the vendor must notify you directly of changes they intend to make, not just via a posting on their portal or website.



What Due Diligence IS

> ***Due diligence**: The investigative process during which a third party is reviewed to determine its suitability for a given task.*
> *-- Shared Assessments*

Due diligence starts with proper vendor management. In order to know the important criteria you want to review on the vendor, you need to understand a few things about the services they are to perform and how those services are delivered. These questions center around identifying different risks the vendor could bring to your organization.

Are the services you need the vendor to perform critical to your operations?

Will the vendor have access to your sensitive data or your infrastructure?

Are there other vendors in the space who can step in if this vendor fails?

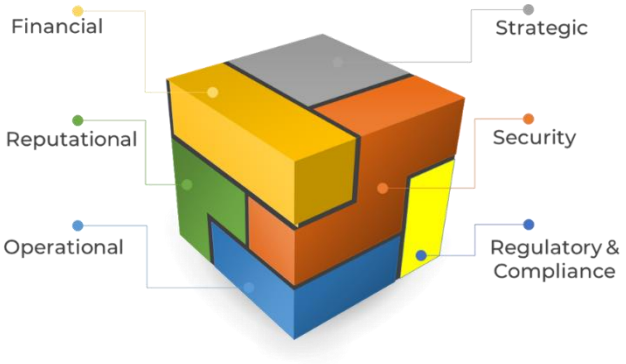
Classifying your vendors according to the criticality of their services to your operations will inform you of the levels of risk you are willing to tolerate. Organizations should understand their risk appetite and risk tolerance (usually given from the top of the organizational hierarchy) to determine the levels of risk acceptance they need to implement mitigating controls. Furthermore, understanding the escalation path for risk acceptance will help guide business decision makers on acceptable vendors.

For an in-depth look at the various components of vendor risk, please see the research;

Looking at Risk in a New Light: The Six Pillars of Vendor Risk Management

Once you understand the risks a vendor may pose, craft your due diligence questions to see if the vendor shows signs that a potential risk may be more likely.

An example checklist of items to include is at the end of this article.



Examples of Risks

I. Financial

You want to ensure the vendor can remain solvent and avoid potentially subjecting your organization to financial penalties. Review their current financials and those of the last few years, along with any investments that could offset their ability to continue serving you, their customer, in the manner you require. Ensure that the vendor has no significant plans to change their offerings, potentially forcing you to accept a similar service for a more expensive re-branded one or moving all their services to a more expensive cloud service.

a. Include: Obtain the vendor's income statements, balance sheets, and cash flow statements for the last three years. Obtain their financial audit report, paying particular attention to the auditors' opinions and all footnotes. If privately owned, ask their financial group for the relevant data points.
    i. Establish a cadence for when you will re-review these documents for established vendors – at least before the renewal of agreements – and if anything arises in the media that would cause an inquiry.

II. Strategic

Review the vendor's proposed multi-year plans to see if their product offerings align with your strategic goals. It is essential to have a regular cadence of ongoing business reviews with established strategic vendors to assess their relevance and value to your strategic plan.

a. Include: Review your strategic plan and ensure the vendor's services align with your goals. Ask to review their multi-year plans to see if their offerings' directions align with your needs and expectations.
    i. Established vendors in this category should be checked annually, during renewal, and whenever your business strategies change. Best practice with strategically aligned vendors is establishing a formal business review cadence that includes this review.
        1. *Jump Start Your Vendor Management Initiative Phase 2 Tools and Templates Compendium*. Contains an example agenda for a business alignment meeting.

III. Reputational

There are a number of ways being in a relationship with a vendor could harm your brand. Consider their posts on social media, their response to regulatory requirements, and how they treat their customers and employees as significant review points. In addition, review any potential litigation and if they are positioning for an acquisition that could put you in a regulatory bind.

a. Include: Perform a media review for data and security breaches, mergers and acquisitions, loss of key staff, and legal proceedings.
    i. You should check on your established vendors periodically to determine if anything changes in this area.

IV. Security

Possibly the most apparent due diligence is the security risk assessment. Don't be afraid to ask for the vendor's documented security program and third-party risk management program – it is vital that you know how they will be managing their vendors. Make sure to check for any security or data breaches in their past and how they handled them. Be sure to understand

where the vendor will host your data and how they intend to secure and manage it throughout all points of transfer and storage.

a. Include: You must understand the framework you want to hold the vendor accountable and include the appropriate Security Addendum. The vendor should provide a SOC 1 or SOC2 (or equivalent) for the security review. For cloud and SaaS services, review any documentation the provider may have and look for articles on data breaches and security in the media.
    i. Established vendors should have this review done at least annually, at each renewal period, and on any significant upgrade that affects their security posture.
    ii. *Why You Need a Security Addendum: Managing Vendor Expectations*

V. Operational Performance

Review the staff that the vendor has available. Understanding the average tenure by role at their organization will give you insight into potential staff turnover during a project. Also, ask for staff locations so that you can grasp any geopolitical issues that could cause a work stoppage and interrupt your plans.

a. Include: Inquire about the longevity of their staff and their credentials. Ensure the vendor will have enough resources to sustain your operations with competent professionals as long as they are needed. Check their geo-location for any potential issues that might cause an interruption of services that could affect your business operations.
    i. Review the established performance metrics for vendors already in place, and inquire with the business units on how the vendor is perceptively performing so you can adjust as needed.
        1. If the vendor's service is critical to business operations, have a transition plan in place if the vendor ceases operations.
        2. The vendor's security addendum should include their business continuity and disaster recovery plans for your review so you can ensure they meet your expectations.

VI. Regulatory & Compliance

Part of due diligence is working internally to discover which laws and regulations are required for your organization to maintain compliance. Knowing these will allow you to determine if you can hold the vendor accountable in the future and will enable you to review any non-compliance on their part in the past. If you have an industry sanctions list, remember also to check that.

a. Include: Check with your compliance, risk management, and legal teams to ensure that the vendor is not on any sanctions list and that they can accommodate your regulatory needs.

i. For established vendors, re-check the sanctions lists and research to ensure they have not had any regulatory penalties applied.

Once you have the above information from the vendor, you should compile it into a due diligence report so that the appropriate people at your organization can perform their reviews. The report evaluations will guide further activities in the risk assessment process.

How to use Due Diligence Reports and who should review them

One of the core tenets of vendor management is coordinating processes needed to ensure organizations are protected and achieve the highest value from their vendors. Aligning with that tenet, vendor managers can aid in both the capture of documentation and the review of the due diligence report.

A number of people in your organization should review due diligence reports. The business units need to check them to see if the identified issues have merit in light of the proposed services. Your risk managers and compliance personnel should ensure that the vendor meets regulatory qualifications. Security and IT should check to see that the vendor meets the security frameworks necessary and is compatible with your existing infrastructure, standards, policies, and guidelines. Executives and board members will want to know the inherent and residual risks identified so that they can ensure that proper controls and/or exceptions have been put in place to mitigate those risks.

Managing 4th-Nth Party Due Diligence

4th-Nth Party: The vendors your vendors use to support their business.

From SaaS vendors needing cloud storage to implementation partners using supplemental staffing subcontractors, more than ever, vendors rely on outsourcing services to achieve their clients' goals. These relationships are your 4th-Nth party vendors, and you need to know who they are.

It can be seen as daunting to map out the relationships throughout the supply chain, but this is a necessary step in ensuring your organization is protected. In your security addendum, ensure that your vendors have a robust third-party risk management (TPRM) program to hold them accountable for downstream liability.

THE VENDORS' TPRM PROGRAM SHOULD INCLUDE:

- THEIR **VENDOR INVENTORY** SO YOU KNOW WHO THEY WORK WITH.
- A **RISK REGISTER** SO YOU UNDERSTAND THE ASSOCIATED LEVELS OF RISK THEY HAVE ACCEPTED

An important part of your due diligence is ensuring that the requirement of a TPRM program is a component of the vendor's security program. Obtain and review their program to ensure it aligns with your expectations. The main agreement and addendum should require the vendor to have and enforce this program so that you can hold them accountable to the agreed-upon standards.

Summation

The world is becoming more complicated every year, and the potential risks associated with your organization are no exception. To understand the potential impacts that any new vendor relationship can have on your organization, you need to put in the effort and maintain due diligence throughout the lifecycle of those relationships.

Understanding the risks a vendor may pose today is one step in the due diligence process. To ensure your organization's safety, you need to monitor the relationship with ongoing due diligence set at a proper cadence. Consider the resources required to ensure process compliance and validate the information gathered. Allow your vendor managers to aid in collecting and coordinating reviews to ensure that your checklist is complete and accurate.

Due Diligence Checklist

Vendor Legal Name: _____

Vendor DBAs: _____

Vendor Contact: _____

Contact Phone & Email: _____

Vendor Address: _____

Vendor URL: _____

Please obtain/answer the following items from/about the vendor for review.

- ☐ Vendor's articles of incorporation and bylaws or operating agreement
- ☐ Vendor's organization chart
- ☐ Vendor's comprehensive list of operating locations
- ☐ Vendor's number of employees (by region) and average tenure (by role)
- ☐ Vendor's financial statements for the last three (3) years
  - Income statements
  - Balance sheets
  - Cash flow statements
  - Tax returns and filings
- ☐ Vendor's performance forecast for the next three (3) years
- ☐ Vendor's known mergers & acquisitions for the last three (3) years
- ☐ Vendor's tax ID, credit report, D&B report
- ☐ A list of pending, threatened, and active litigation for the last five (5) years.
- ☐ Vendor's relevant policies and code of ethics
  - HR, background checks, AUP, privacy, security, standards of conduct, etc.
- ☐ Vendor's complaint history for the last three (3) years
  - BBB, FTC, Glassdoor, CFPB (consumer complaint database), etc.
- ☐ Review vendor's social media and website activity
- ☐ Vendor's security program (identify relevant framework)
  - Include vendor's third-party risk management (TPRM) program
  - Obtain assurance documentation (Soc I & II, SSAE-18, etc.)
  - Identify where the vendor stores data and how it is protected/managed
  - Include the vendor's business continuity (BC)/disaster recovery (DR) program information
- ☐ Vendor's history of security & data breaches for the last three (3) years
- ☐ Vendor's insurance coverage information (including certificates)
- ☐ Is the vendor on any sanction list currently or was it in the last five (5) years
  - If yes, explain: _____

References

- *Looking at Risk In a New Light: The Six Pillars of Vendor Risk Management*
- *Jump Start Your Vendor Management Initiative*
- *Why You Need a Security Addendum: Managing vendor expectations*
- *Build a Vendor Security Assessment Service*
- *Checklist for Third-Party Providers*
- *Vendor Contract & Cost Optimization*