THE **COMPLETE** BREAKDOWN

HOW TO DO Vendor Due Diligence Reviews

venminder

HOW TO DO Vendor Due Diligence Reviews

THE **COMPLETE** BREAKDOWN

If you're like most of us, collecting due diligence on vendors can feel like one of the most challenging tasks that you have. You feel like you're constantly calling, emailing, and chasing your vendors to obtain the report you've needed for weeks now. Then, once you've received the report, you realize the battle is only half over.

Then, you, or a subject matter expert (SME), must fully analyze the report and write a thorough assessment with your findings. Remember, you should never have a check-the-box mentality when it comes to due diligence. Simply checking the box without doing a thorough assessment can lead to unwanted consequences.

Analyzing the documentation can become overwhelming. Sometimes it's difficult to determine where to begin, what to review, and how to interpret what it all means. We're here to breakdown how to review and analyze **six** of the most common due diligence documents we see every day.

SOC REPORT

Overview:

SOC stands for system and organization controls. It's an independent audit report performed by a certified public accountant (CPA) that shares additional details about the vendor's controls. It's an attestation that your vendor has the controls in place to safeguard your data and whether the controls can effectively mitigate part of the vendor's inherent risk.

Steps to Review a SOC Report:

1. **Take a look at the reporting period.** Confirm it's the most current report available. If the report is older than the reporting period length plus three months, then a newer report should be available. A Gap Letter, or Bridge Letter, can be issued by the vendor's management to cover the gap between the last SOC reporting period end date and the date of the letter.

2. **Review Section 3 of the report.** Management's description of its system and controls will give you a great deal of information about the vendor such as how they're set up, who is responsible for what, the management structure, and governance processes.

3. **Confirm the products and services** listed within the SOC report are the ones that your organization is utilizing. You'll often find that many vendors have multiple reports covering different products and services; therefore, it's very important that you verify you're reviewing the correct one.

4. **Understand the data and how it is used.** Know what type of data the vendor processes and how it's protected. Within the SOC report, your vendor should provide details on how they secure servers, networks, and computer systems.

5. **Understand the data center information.** Review the infrastructure's environmental, monitoring, and access controls. You want to ensure the vendor is managing their data center properly and keeping their infrastructure resilient. This is crucial to protecting data.

6. **Thoroughly analyze the control objectives and activities.** The audit firm will test the controls in place and note if they're operating effectively.

7. **Review audit findings.** See how management responded to the findings. This will help you determine if the vendor is reliable and can provide you with the contracted service as promised.

8. **Have a qualified SME write up the assessment.** This should be an experienced risk or security professional or someone with a related credential.

9. Once you have your assessment in hand, **reach out to the vendor to discuss any findings and next steps.**

BUSINESS CONTINUITY PLAN (BCP)

Overview:

Business continuity planning assists vendors (or any business) in ensuring that their significant operations and products/services continue to be delivered in a full, or at a predetermined and accepted, level of availability. The expected level of availability is typically outlined in the Service Level Agreement (SLA) that your organization has with the vendors.

Steps to Review a BCP:

1. **Verify the vendor has a formal BCP.** Ensure it meets your organization's needs and covers critical components that are needed to ensure operations continue. If the vendor becomes unavailable, will your services operate normally?

2. **Review the vendor's strategy for addressing personnel loss –** aka their succession plan. Look for cross-training, job rotation, staffing agencies, etc. as mitigations. Social unrest may occur.

3. **Determine if the BCP contains plans for pandemic contingencies or mass absenteeism** following Center for Disease Control guidelines.

4. **Check their relocation plans.** Confirm they're acceptable and verify whether the vendor has a secondary office facility or remote work capabilities. This includes things like assets, equipment, building relocations, remote access strategy, contract third-party office space, and more.

5. **Review their breach/disruption notification policy** to verify a clear communication plan is in place. It should be adequate and align with the information security language that's in the contract between your organization and the vendor.

6. **Understand the vendor's testing procedures.** Ensure the testing is at least annual and ask to see the actual or redacted test results. Any test results that show room for improvement should be followed up on.

7. **Review the vendor's Business Continuity Impact Analysis (BIA) within the BCP and ensure that it matches your expectations.** This includes the following:

   Recovery Time Objective (RTO): RTO helps identify the targeted duration of time in which the vendor states they will restore a business process, post-disruption.

   Recovery Point Objective (RPO): RPO helps identify how much data may be lost if data needs to be recovered. Typically, this matches with your backup or replication frequency. It really becomes important if a computer, system, or network goes down.

   Maximum Tolerable Downtime (MTD): MTD specifies the maximum period of time that the vendor can be down before their survival is at risk.

   How much data may be lost and how long will normal operations be impacted? This is what you're learning when reviewing RTO and RPO. Some vendors will have different objectives for different services and client tiers. How does this relate to your contracted service level agreement (SLA)?

8. **Analyze the frequency of ongoing maintenance of the plan.** The plan should be reviewed regularly as part of the vendor's routine policy maintenance, but should also be updated when a significant change occurs in the vendor's organization.

9. **Have a qualified SME write up the assessment.** This should be an experienced risk professional or someone with a related credential.

10. Once you have your assessment in hand, **reach out to the vendor to discuss any findings and next steps.**

DISASTER RECOVERY PLAN (DRP)

Overview:

Disaster recovery is a subset of business continuity. A disaster recovery plan involves processes and procedures for an organization to follow immediately, as soon as a business impacting incident occurs, until normal operations are resumed.

Steps to Review a DRP:

1. **Verify the vendor has a disaster recovery plan in place that is readily available to staff in the event of a disaster and addresses data loss and system availability.** How much data may be lost and how quickly availability is restored should be represented by RTO and RPO.

2. **Check whether criteria is defined and in place for declaring a disaster.** Without defined internal communication and an incident management program, employees may not know when to formally declare a disaster, attempting to fix the business impacting event instead of communicating the issue to key stakeholders.

3. **Verify the plans cover availability and potential loss of equipment, data, and the data center/ server room.** Look at how data is stored as well as the location and status of the recovery information system.

4. **Check if a secondary data center is readily available** in the event of a disaster and ensure it's sufficiently geographically separated so that a regional impacting event won't affect the vendor's production and recovery sites simultaneously.

5. **Review the configuration of the vendor's data center recovery locations** to assess the adequacy of recovery capacity to meet your business needs.

6. **Ensure that a clear communication plan is in place and verify their client notification process meets your requirements.** Communication can save a relationship. Verify that the vendor's notification timeline meets any requirements you have, including regulatory requirements.

7. **Review critical IT functions outsourced to a third party** and ensure communication plans exist with subcontractors (aka your fourth parties).

8. **Understand the vendor's testing procedures.** Ensure the testing is at least annual and ask to see the actual or redacted test results. Any testing results showing room for growth should be followed up on.

9. **Analyze the frequency of ongoing maintenance of the plans.** Plans should be reviewed annually and after any significant organization changes as part of the vendor's routine policy maintenance.

10. **Have a qualified SME write up the assessment.** This should be an experienced risk professional or someone with a related credential.

11. Once you have your assessment in hand, **reach out to the vendor to discuss any findings and next steps.**

CYBERSECURITY PROGRAM

Overview:

A cybersecurity program helps protect your organization and the vendor from potential vulnerabilities like a data breach. Evaluating your vendor's cybersecurity posture will help you identify potential weaknesses. From there, you can effectively communicate with the vendor about those weaknesses and develop strategies to strengthen controls before a breach occurs.

Steps to Review a Cybersecurity Program:

1. **Focus on the 4 critical elements** – security testing, sensitive data security, employee, contractor, and vendor management, and incident detection and response.

2. **Review the vendor's security testing.**
The vendor should be performing these tests annually:

   Scanning/Testing:
   This test will identify any security vulnerabilities in the infrastructure (e.g., application, server, or network).

   Penetration Testing:
   This testing validates vulnerabilities identified in scanning that could be exploited by an attacker. This testing is performed by experienced professionals and is done in addition to scanning.

   Social Engineering:
   This type of testing will focus on human error within the organization, meaning testing employee vulnerability to common tactics (e.g., phishing emails).

3. **After reviewing the security testing, note any issues found.** You'll want to mention things like critical and high-risk vulnerabilities, how vulnerabilities have been addressed and corrected – or mention if they haven't been – and the vendor's plan to prevent future vulnerabilities like the ones identified.

4. **Review the vendor's sensitive data security.**
Sensitive data security is important as it's information that should be protected, at all times, against unintended disclosure. Make sure the data is encrypted and protected from destructive forces and unwanted actions of unauthorized users.

5. **Request the vendor's data retention and destruction policies as well as data classification and privacy policies.** These go hand-in-hand with sensitive data security. If they don't have these policies, that's a huge red flag.

6. **Verify the vendor has trained their employees, contractors, and vendor management team to protect data.** Look for things like confidentiality agreements, employee background checks, annual security training with documented completion, management of vendors, and access management policies to confirm they've all been properly trained.

7. **Review the vendor's incident response plan.**
Request that it's tested annually and ask to review the results of the most recent test. It's crucial the vendor has one in place to address any issues that may arise. This will help minimize the impact. Confirm they're acceptable and meet your organization's expectations.

8. **Have a qualified SME write up the assessment.**
This should be an experienced risk or security professional or someone with a related credential.

9. Once you have your assessment in hand, **reach out to the vendor to discuss any findings and next steps.**

FINANCIAL STATEMENT

Overview:

At a minimum, financial information should be reviewed on an annual basis for key vendors. This review will help ensure that the vendor has adequate financial health to provide uninterrupted, safe, and high-quality solutions and services to your organization, and reduce any risk that may be introduced from a vendor's poor financial health signals.

Steps to Consider to Review a Financial Statement:

1. **Evaluate a vendor from both a quantitative and qualitative point of view.** This includes a thorough assessment of key line items in financial statements and ratios, as well as notes and commentary that speaks to changes in the vendor's operations and ownership structure, management structure, legal environment, and other risk factors.

2. **Determine if the company is public or private.**

   Public Company – If the company is public, the statement is usually a Form 10-K. Thoroughly review the form and watch for the following:

   - **The risk factors –** These are shared within the financial documentation, with notes related to any regulatory actions that may have occurred.
   - **Active legal proceedings or lawsuits –** Be aware of any pending legal proceedings or lawsuits, as well as what the settlement charges will likely be.
   - **The auditor's opinion on financial statements –** Look at the auditor's opinion on the vendor's financial statements, including the auditor's view on the vendor's ability to operate as a going concern and whether the vendor has any noted weaknesses or deficiencies.
   - **The auditor's opinion on internal controls –** See whether the auditor has deemed the controls adequate.

   Private Company – If a vendor is private, availability of data may vary, but the key financial information and qualitative information should be no different. You should start with the 'gold standard,' which would be annual audited financial statements from vendors. However, your organization can utilize other data for vendor financial health reviews, such as internally prepared, unaudited financials, IRS forms (such as a Form 1120), management/financial letters on performance, or publicly sourced credit reports.

3. As you review the financial statement, look at the following to **compare year-over-year numbers for a minimum of the last 2-3 years:**

   Balance Sheet – To understand the company's financial position, such as its current cash balance, assets balance, debt obligations, and other liabilities.

   Income Statement – To understand their scale, trended performance, revenue profile, gross profit profile, operating expense profile, and operating profit profile.

   Cash Flow Statement – To understand the company's sources and uses of cash from operations, financing, and investing activities.

   Ratios – To understand certain metrics, such as current ratio, which conveys a company's ability to generate liquidity and cover short-term obligations with its current assets.

4. **As you perform your vendor financial health reviews and dive deep into the provided information,** consider the following questions on the vendor's financial health:
   - *Is the vendor making money?*
   - *Do they have sufficient capital, or access to capital, to support their ongoing operations?*
   - *What is the vendor's debt-to-worth?*
   - *What is their tangible net worth?*
   - *Can the vendor continue operations at the current cash level?*

5. Have a qualified SME, such as a CPA, **write up the assessment and report executive summary comments.**

6. Once you have your assessment in hand, **reach out to the vendor to discuss any findings and next steps.**

CONTRACTS

Overview:

A contract is an agreement between two parties creating a legal obligation for your organization and vendor to perform specific activities. Each of the parties to the contract are legally bound to perform the specified duties outlined within the contract. Having a well-written contract is important because it sets the expectations and formal agreement between the two parties.

Steps to Review a Contract (Before Entering the Relationship):

1. **First, remember that negotiation is vital.** Don't accept the first contract that you see. It's common and often necessary for both parties to make changes and special requests in the contracts.

2. **Review the scope of services.** You want to verify there are provisions such as the following:

   - *The products/services the vendor will provide*
   - *Rights and responsibilities*
   - *Language around any timeframes promised or custom services requested*
   - *Rights to modify*
   - *Any guidelines around contract re-negotiation*
   - *Right to audit*

3. **Locate the performance standards and make sure they're adequate.** This is where you should find the SLA requirements, remedies, and any penalties if the SLAs aren't met.

4. **Confirm the duration of the contract is correct.** Verify that the term, renewal term, non-renewal, termination notice periods, and anything else related to timeframes are accurate.

5. **Make sure your contract spells out the conditions for contract termination.**

6. **Consider costs and price increase language.** In the fee description, you're looking for information pertaining to cost overview, increase limitations, support for merger/acquisition activity and costs, payment terms, late fee language, deconversion fees, and, if applicable, who's responsible for cost to maintain software or hardware.

7. **Always look for security and confidentiality provisions.** This should include information on how the vendor plans to safeguard your data, prevent exposure to breaches, how they'll notify you of a breach, and how they plan to maintain a log of incidents. You also want to confirm how the vendor will return or destroy your data or assets if the relationship terminates. If the service is cloud based, be sure there are geographical limits on where your information can be stored and that it will be segregated from your vendor's other clients.

8. **Look at the audit requirements.** Verify there's a description of audit reports your organization is entitled to receive – like a SOC 1, SOC 2, and SSAE 18 – and that they're accurate.

9. **Understand what reports will be made available to you and if there will be any fees for customizations** (e.g., financial statements, performance reports, PCI compliance certification).

CONTRACTS (continuation)

10 **Verify that business resumption and contingency plan language is included within the contract.** You're seeking provisions around disaster recovery, business continuity, and back-up record protection.

11 **Be sure the vendor outlines their policies around subcontracting.** Your vendor should provide any required due diligence documents related to any subcontracted vendors (your fourth parties).

12 **Ownership and license information should be included in the contract.** There should be a description of ownership, rights, and allowable use of your organization's data, system documentation, and other intellectual property rights, such as protection by the vendor in the event of a patent/copyright infringement claim. It's important to make sure there are protection rights for your organization outlined within.

13 **Confirm the contract includes a clause pertaining to indemnification** so that the vendor will hold your organization harmless from liability due to a negligent vendor.

14 **Review the limitation of liability to verify it equates** to the amount of loss your organization might experience as a result of the vendor's failure to perform.

15 **Provisions around dispute resolution** should always be included too.

16 **Include standards around complaints management, where needed.** Who will resolve complaints and perform the root-cause analysis?

17 **And, to bring it all home, review the general provisions.** You're looking for provisions such as the following:

- Survival
- Governing law
- Contract conflict – order of precedence
- Severability
- Failure to exercise/waiver
- And more, depending on the vendor relationship in review, as the provisions necessary aren't limited to these 5

18 Have a qualified SME, such as a paralegal, **write up the assessment.**

19 Once you have your assessment in hand, **reach out to the vendor to discuss any terms that may be missing and next steps to negotiate them into the contract.**

As a reminder, don't forget that there are many other foundational documents that you should always be collecting on a vendor. These often include:

- Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- Basic Information (i.e., full legal name, address, all physical locations, website URL)
- Ownership structure and affiliated companies
- Tax ID
- State of Incorporation
- Articles of Incorporation
- Secretary of State Check
- Business License
- Certificate of Good Standing
- Credit Report
- OFAC/PEP Checks
- Any "doing business as" or "also previously known as" (d/b/a, aka, pka)
- Dun & Bradstreet (D&B) Report
- Vendor complaints research findings
- Vendor negative news search findings
- List of subcontractors / fourth parties
- Picture or Google map view of facility (if required)
- Conduct check of CFPB Complaint Database and/or Better Business Bureau rating

Due diligence is a fundamental component of any vendor risk program.

When done correctly, it tremendously helps prevent risk to an organization and the customers.

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

Download Now

venminder

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

+1 (888) 836-6463 | 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 exchange library. The assessments enable customers 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.