Unacceptable
Vendor Due Diligence

venminder

Unacceptable
Vendor Due Diligence

Performing vendor due diligence is a regulatory requirement and sound business practice. It helps keep your vendor management program in compliance. If you're performing due diligence adequately throughout the year, you're reaching out to your vendors to request updated documentation and will perform an analysis. If all goes well, you'll simply conduct your analysis and keep it on record until it's time to readdress the document.

At some point, however, one of your vendors is going to send back a due diligence document that doesn't suffice. It's inevitable. The catch is, will this deficiency slip through the cracks or will you notice the issue within the documentation right away?

Here are five major due diligence reports often received and some of the signs to watch for that indicate vendor due diligence that's unacceptable. Some may seem obvious, but you'd be surprised how easy it is to overlook these issues.

SOC Report

What It Is

SOC stands for System and Organization Controls. It's an independent audit report performed by a certified public accountant (CPA) that shares additional details around the vendor's controls in place. It's an attestation that your vendor has controls in place to safeguard your data, and if the safeguards are operational, they would effectively mitigate part of the risk inherited by using the vendor.

5 Signs of an Unacceptable SOC Report:

1. **The report is outdated.** Review the reporting period. If it's not the most current report available, then you won't be able to properly assess controls.

2. **There are reporting variations.** This includes inadequate testing, report modifications, removing pages, etc. All are potential signs of an underlying issue.

3. **There are exceptions or no response to exceptions.** Do you see multiple exceptions? Are some of these repeated exceptions from the last reporting period? If you do, and especially if management hasn't responded to the repeat occurrences, then that's a warning sign.

4. **You notice words like "inadequate" or "misrepresentation".** Be on the lookout for these words in the Service Auditors Report section.

5. **The service auditor provided a qualified opinion.** This means that the auditor may have some concerns that you should review further.

Business Continuity and Disaster Recovery Plan

What It Is

Business continuity and disaster recovery 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.

5 Signs of an Unacceptable Business Continuity and/or Disaster Recovery Plan:

1. **Business continuity and disaster recovery aren't individually defined and addressed.** Some vendors don't differentiate between business continuity planning and disaster recovery planning. As a best practice, and to properly safeguard your organization, they should. The information may all be found in one report or policy but should be separately called out and addressed.

2. **The plan hasn't been updated within the last 12 months.** Or, it hasn't been updated within the time range defined by the vendor in their plans.

3. **The plan doesn't cover the products or services that are applicable to what your organization is using.** Verify it's the right plan as vendors often have multiple plans for different products/services.

4. **You don't see defined recovery point objectives (RPOs) or recovery time objectives (RTOs).** And, if they're defined but don't align with what your organization deems an acceptable timeframe, then that's a sign of an unacceptable plan.

5. **The plan isn't tested annually.** These plans should be reviewed and tested on an annual basis to ensure the procedures outlined are effective and that all involved with execution are adequately trained and prepared.

Financial Statement

What It Is

Financial statements should be reviewed to identify the financial health of any vendor you outsource a product or service to. This helps you determine if the vendor can continue to provide secure, safe and quality products or services that meet your organization's expectations. With financial statements, review at least the last three years of financial statements to get a good sense of how the vendor is trending. This is known as horizontal analysis.

5 Signs of an Unacceptable Financial Statement:

1. **The vendor only provides the income statement and a balance sheet.** This happens often as many organizations only request those two documents from the vendor; however, there are potentially two reports in addition to the income statement and balance sheet that you should obtain to get a good idea of the financial health of any vendor. These are the cash flow statement and, if the vendor is publicly held, request the statement of shareholder equity.

2. **There's declining equity within the balance sheet.** The balance sheet is a listing of everything you own or owe. Make sure the value of the business is growing over time by looking at the equity. Declining equity can signal bad things are happening. If you compare the current assets to the current liabilities and you find liabilities are greater than a one-to-one ratio, the business may have a problem.
The equation to follow is current assets/current liabilities = current ratio.

3. **As you review the income statement, net income isn't consistent with sales.** Sales trends are the key here as sales should be trending up over time. If the vendor's sales are trending up, examine the net income. Net Income should parallel sales. If net income isn't trending with sales, that can indicate a host of problems with the vendor.

4

A negative net cash flow. The statement of cashflows has three parts. They are operating activities, investing activities and financing activities. You want to scrutinize the net cash flows from operating activities and you're hoping that number is positive. A negative number here indicates problems either with current financing or finance problems to come down the road. The higher the net cash flow from operations the more likely the business is to be successful.

5

You notice unusually high dividends and the vendor has issued capital stock. The point of analyzing a statement of shareholder equity is to determine where the business is investing their profits. Are they reinvesting in the business by increasing retained earnings or are they investing in themselves by paying dividends to shareholders? Of course, there are two parts to this problem. Capital stock and retained earnings. You need to determine where the total shareholder equity comes from and how the business is distributing the profits. If the dividends are unusually high and the vendor has issued capital stock, that's a problem. Repurchase of shares by the vendor is also an issue. Often a business that's repurchasing shares is attempting to increase their share price artificially.

Cybersecurity Program

What It Is

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 prior to a breach happening.

6 Signs of an Unacceptable Cybersecurity Program:

1. **There's inadequate testing.** If you don't see testing on vendors that are medium risk, high risk, critical or that process, store or transmit your data then that's a concern. Also, ensure testing includes vulnerability, penetration and social engineering.

2. **A lack of security policies in place.** Policies should be documented well and updated frequently. Examples of security policies include data retention and destruction policies, data classification and privacy policies, data encryption standards, network security policies, access management policies and incident detection and response plans.

3. **Sensitive data has been exposed in the past.** Has the vendor experienced a data breach? That's a massive red flag!

4. **Policies and procedures of the vendor's employees, contractors or vendor management are nonexistent.** The vendor should make sure their employees, contractors and their own vendors are properly trained and on the same page regarding cybersecurity measures and the precautions that should be taken.

5. **Lack of strong protocols around shared accounts and password strength.** Weak password requirements and shared accounts can cause cybersecurity issues.

6. **There are open firewalls and/or unpatched operating systems.** These can lead to vulnerabilities.

Sufficient due diligence is a critical component of a successful third-party risk management program.

Download free due diligence samples and see how Venminder can help you reduce your workload.

Download Now

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

(270) 506-5140 | venminder.com

About Venminder
Venminder is a leading third-party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.