Rules to Receive CPE Credit

BY ATTENDING TODAY'S SESSION, YOU ARE ELIGIBLE TO RECEIVE 1 CPE CREDIT PER THE FOLLOWING GUIDELINES:

In order to receive this credit, the following items MUST be completed:

- Each person wishing to receive CPE Credit must log into the session individually with their credentials
- You MUST answer ALL of the polling questions throughout the presentation
- You MUST be in attendance for the entire live session
- You MUST complete the follow-up survey regarding the session

venminder

Creating an Effective Vendor Document Collection Process

June 27, 2023

PRESENTED BY

Hilary Jewhurst

Head of Third-Party Risk Education & Advocacy
Venminder

venminder

Session Agenda

1. Where vendor document collection fits into the due diligence process
2. Strategies for effective document collection
3. Workarounds and tips for common document collection challenges
4. Key takeaways

venminder

What Vendor Due Diligence Is

- **Due diligence is one of the most important activities** in third-party risk management
- It's conducted for new engagements and periodically for existing engagements
- Collect, review, and assess applicable vendor information and controls
- Helps determine residual risk of your vendor

Why Is Due Diligence Necessary

LET'S START WITH THAT IT'S A REGULATORY EXPECTATION.

Along with risk assessment, ongoing monitoring, contract management, and reporting, due diligence is a fundamental requirement of regulatory guidance. Below is not a full global inventory:

- The Board of Governors, FDIC, and OCC interagency guidance on managing third-party relationships - **Interagency Guidance on Third-Party Relationships: Risk Management.**

- NIST, ISO, ITIL, HITRUST
- DOJ Evaluation of Compliance Programs
- UK Serious Fraud Office Bribery Act
- ISO 19600 & 37001
- GDPR, CCPA, and other state's privacy laws
- HIPAA
- 12 CFR Appendix B to Part 30
- FINRA RN 21-29
- NFA Compliance Rules 2-9 and 2-36
- 23 NYCRR 500

venminder

Why Is Due Diligence Necessary

IT'S GOOD BUSINESS

- When considering a vendor, it's easy to be swayed by first impressions. But it's crucial to dig deeper and evaluate their reputation, qualifications, risk management practices, and controls to determine if partnering with them will be beneficial or pose potential risks.
- Having vendors who are unqualified, non-compliant, or substandard can result in significant costs for the organization in terms of time, money, and resources.
- Vendor issues that aren't addressed properly can lead to operational disruptions, financial losses, higher expenses, and potential legal consequences.

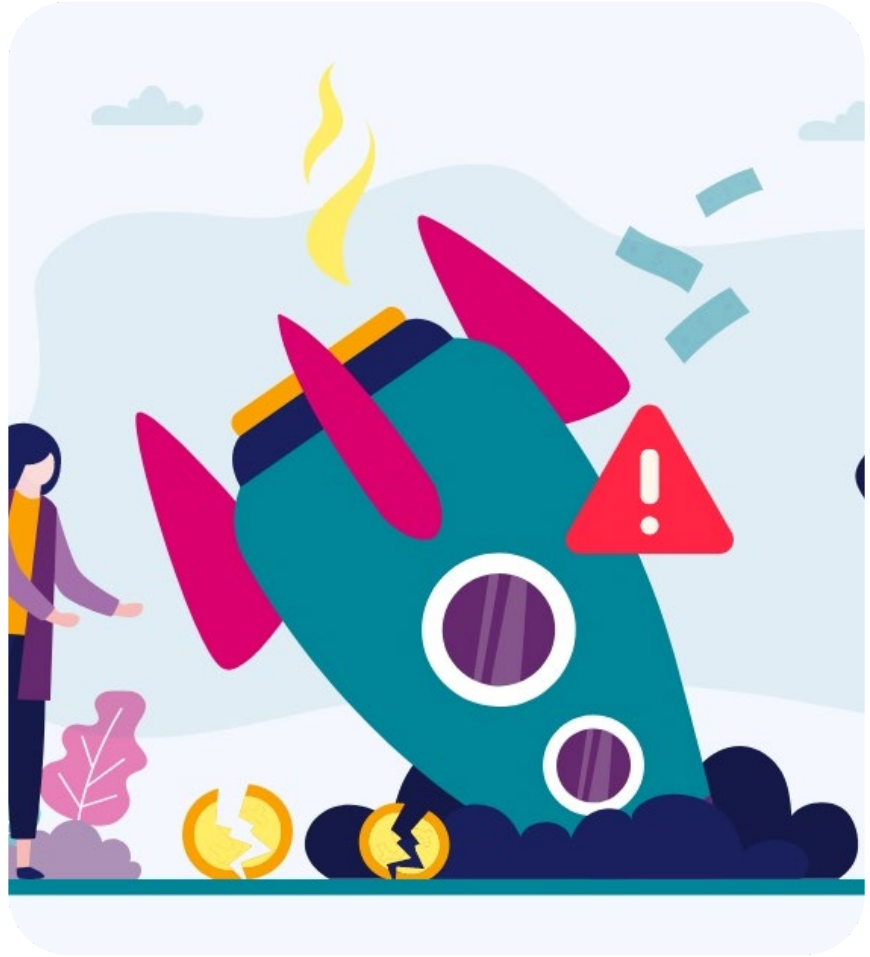
Why Is Due Diligence Necessary

PROTECTS YOUR CUSTOMERS AND YOUR BRAND

- Your customers have a reasonable expectation that the products and services offered by your organization, and its vendors, will not cause harm to them.
- Performing due diligence is an essential task to identify and eliminate vendors who do not adhere to legal and regulatory requirements, neglect to safeguard data, or exhibit inadequate quality and safety standards.
- It's important to remember that customers and the public view your organization and its vendors as one entity.
- Whenever you interact with a vendor, you're placing your reputation and brand in their hands.

Hazards of NOT Doing Vendor Due Diligence

- It can be challenging to ascertain the legitimacy of the business you are engaging with.
- You have no visibility of fundamental issues in the relationship.
- There is insufficient data to help your organization proactively anticipate future problems (e.g., data breach, “bad actors,” financial, or business continuity issues).
- You risk regulatory non-compliance, resulting in fines or enforcement actions.
- Your organization and customers may be exposed to avoidable and potentially devastating risks.
- The application of standards is inconsistent.



venminder

Understanding the Due Diligence Process

Due Diligence is a process with multiple components and activities

1. **Collecting Basic Vendor Details**

   Company address, ownership, background, locations, business license, etc.

2. **Vendor Risk Questionnaire**

   Completed by the vendor, this questionnaire asks questions about the product or service and the vendor's risk management practices and controls for applicable risk domains (cybersecurity, compliance, business continuity, financial health, etc.).

3. **Due Diligence Documentation**

   Documented evidence of a vendor's risk practices and controls, including policies and procedures, financial documentation, business continuity plans and testing, cybersecurity controls, compliance, customer complaint logs, etc.

4. **SME Vendor Risk Review**

   Information is reviewed by a qualified subject matter expert (SME) by risk domain. SME assesses if risk practices and controls are sufficient to mitigate known risks.

5. **Issue Remediation**

   Issues that need to be addressed before the contract is signed are fixed, a SME reviews and approves evidence of the resolution. Issues that can be remediated after contract execution are written into the contract.

venminder

The Importance of Due Diligence Documentation

1. **Documents serve as evidence.** While it may be tempting, it's always advisable to avoid relying solely on the vendor's claims or the answers provided in a questionnaire. It's better to adopt a 'trust but verify' approach.

2. **Documentation provides visibility to history through revision tables** (e.g., is this a new business continuity program or one that has been in place for several years?).

3. **Proves that vendor governance is in place.** Policies require internal compliance and a level of oversight.

4. **Provides insight into vendor's controls maturity** and changes over time.

venminder

What You Need to Know Before Collecting Vendor Due Diligence Documentation

- Performing due diligence involves assessing the risk level, which determines the extent of evidence required. Higher-risk levels require more thorough due diligence, meaning that more evidence needs to be gathered.
- When it comes to managing vendor risks, due diligence documents play a crucial role in demonstrating both the vendor's risk management practices and your organization's adherence to regulatory requirements and industry standards.
- It’s important to keep the information well-organized and easily accessible for potential audits or examinations.

venminder

What You Need to Know Before Collecting Vendor Due Diligence Documentation *CONTINUED*

- **Document collection strategies must ensure that the documented evidence collected is:**
  - **Professional:** Information provided should meet basic business documentation standards and be concise, clear, and accurate. Additionally, it should be written in a professional manner and free of any errors.
  - **Relevant:** When requesting documents, ensure that they are relevant to risk management practices and controls for identified risks. Avoid asking for unnecessary information as it can be a waste of time for both you and the vendor.
  - **Comprehensive:** It should provide enough information to make a decision or take necessary action.
  - **Timely:** Documentation should reflect the current state and be well within any expiration dates.

venminder

How often do you perform due diligence on third parties?

a. Only prior to the contract being signed
b. Annually
c. Periodically, based on risk
d. Periodically, based on workload
e. Do not perform due diligence
f. Not sure

Vendor Document Collection Strategies

1. Include due diligence in the contract
2. Establish a standardized list of required documentation per risk domain and product/ service type
3. Use a risk-based approach for determining required documentation
4. Make vendor documentation requests clear and concise
5. Make sure to review what you receive promptly
6. Keep following up

venminder

Vendor Document Collection Strategies

1 INCLUDE DUE DILIGENCE IN THE VENDOR CONTRACT

- It’s important to ensure that every vendor contract includes your organization's right to collect information and documentation for the purpose of periodic due diligence.
- A “right to audit” clause should also be included and can be leveraged to collect the information you require to assess the security, safety, and stability of the vendor, at any time.
- Contracts that don’t include these important provisions should be flagged for updates during renegotiation or renewal.
- A binding Non-Disclosure Agreement (NDA) should help alleviate vendor concerns about sharing sensitive data.

venminder

Vendor Document Collection Strategies

2 ESTABLISH A STANDARDIZED LIST OF REQUIRED DOCUMENTATION PER RISK DOMAIN

- What are the minimum document requirements for each risk domain?
- What additional documentation is required based on the product or service type (customer complaint logs, penetration testing, employee background checks, etc.)?
- Which document types may be used by multiple risk domains (i.e., SOC or ISO reports)?
- How old is too old for a document to be considered valid?
- Which documents have expiration dates? (SOC reports, insurance certificates, licenses, etc.)?
- Are there acceptable document alternatives or formats?

venminder

Due Diligence Documents Standards – Example

Compliance – Required Minimum Documentation

Document Type	Maximum doc age	Expiring docs	Alternative
Compliance policy including: • Compliance oversight structure • Governance routines	< 2 years		If older than 2 years, provide the following: 1. Policy update schedule 2. Next policy review date
Employee compliance training • Required courses • Evidence of successful completion	1 year		
Compliance audit or exam results	< 2 years		An audit or exam summary report is acceptable. If there has been no audit or exam within two years, provide the following: 1. Compliance audit schedule 2. Next compliance audit date
State licensing documents		Within 90 days of expiration	
SOC 2 Type II	1 year	Bridge letter no more 30 days old	Expired SOC must have an accompanying bridge letter detailing the issue date of renewed SOC report

Due Diligence Documents Standards By Product or Service – Example

Additional Required Compliance Documentation for Collections Vendors

Product or Service Type	Document Type	Maximum doc age	Expiring docs	Alternative
Collections	**Customer complaint logs** • Issue resolution rate • Issue remediation planning	Require 2 years of reporting		
Collections	**Employee compliance training** • FDCPA • TILA • UDAAP • Privacy	1 year		
Collections	**Policies** • FDCPA • TILA • UDAAP • Privacy • Do not call • Robo dialers • Can-spam	< 2 years		If older than 2 years, provide the following: 1. Policy update schedule 2. Next policy review date

venminder

The Benefits of Standardizing Required Due Diligence Documentation

- Provides clear information for the vendor and describes what they need to provide by risk domain
- Reduces due diligence process cycle time
- Improves document organization
- Saves time for the third-party risk management team and subject matter experts
- Ensures consistency in your due diligence process

venminder

Vendor Document Collection Strategies

3 USE A RISK-BASED APPROACH FOR DETERMINING THE REQUIRED DOCUMENTATION

- Take time to understand the business engagement before determining the types and amounts of due diligence necessary.
- Scale document requests based on risk and criticality and remember that one size does not fit all.
- When dealing with vendors that are considered high risk or critical, it is necessary to conduct more in-depth document collection and assessments.

PRO TIP: *If this is an existing vendor, understand the contract terms as they pertain to your request. It's helpful to know how legal leverage you do or don't have before asking the vendor to cooperate with your request.*

venminder

Vendor Document Collection Strategies

4 MAKE VENDOR DOCUMENTATION REQUESTS CLEAR AND CONCISE.

Send a formalized due diligence request that is well-structured and courteous. Make sure you retain the request with the vendor record.

- Offer an introduction (your title, your organization, etc.)
- Include the reason for your request
- Details and expectations for the request, including your required document types, content, acceptable document age, and any acceptable substitutions
- Specific turnaround time (due by date)
- Explain how exceptions are handled (e.g., for missing, incomplete, or unclear responses)
- Let the vendor know whom to contact with questions

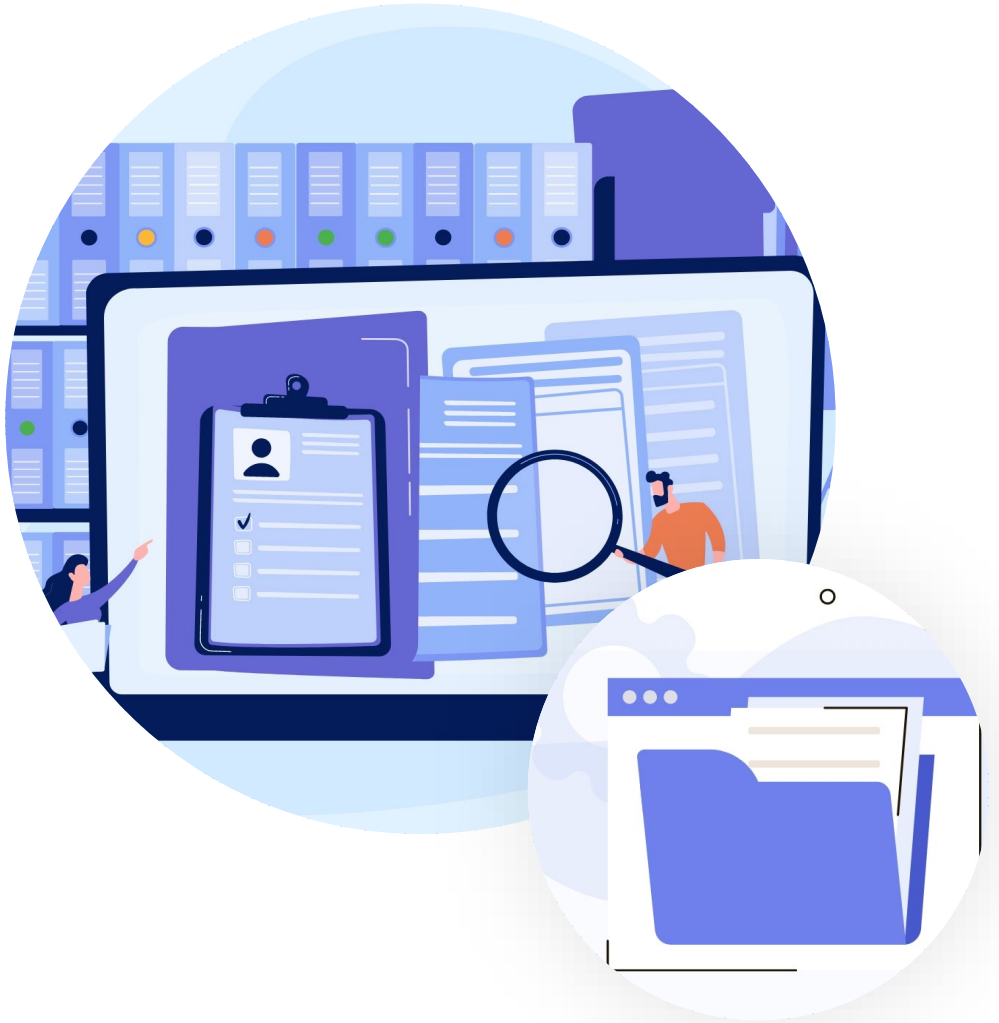
PRO TIP: Copy the vendor owner on the request.

venminder

Vendor Due Diligence Requests - Considerations

When asking for documents, it's typical to contact a sales representative or client manager. However, they may not be acquainted with the exact data and files you need.

- **It’s reasonable to expect that your primary point of contact can assign tasks to other staff members within their organization, including those in compliance, finance, or infosec.** However, you must ensure that the primary vendor contact is responsible for collecting and submitting the necessary documents.
- **It’s important to ensure that your vendor owner is responsible for communicating directly with the vendor contact** to follow up on any missing documents or additional requests.



venminder

Vendor Document Collection Strategies

5 MAKE SURE TO REVIEW WHAT YOU RECEIVE PROMPTLY.

- Your business may need this service ASAP, so consider internal stakeholders/customer needs.
- Often, questionnaires and due diligence responses can lack completeness or coherence.
- It's best not to wait until you have the documentation for all risk domains to start reviewing, as different risk domains are usually managed by multiple SMEs.
- It’s important to promptly review any received information to ensure that follow-up requests for additional details can be made if necessary.

Vendor Document Collection Strategies

6 KEEP FOLLOWING UP

- Make sure you know who is reviewing what and keep track of those assignments.
- Set up calendar reminders or reports for vendors, vendor owners, and SMEs.
- If the information has not been received, follow up before your requested turnaround time (both internally and externally).
- It's better for someone to get a reminder for something they are already working on before it's due than after it's already late.

Does your organization have a standardized list of required due diligence documents by risk domain?

a. Yes
b. Some
c. No
d. Not sure

Baseline Document Collection Items to Collect

- Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- Basic information (full legal name, address, all physical locations, website URL)
- State of Incorporation
- Articles of Incorporation
- Business License
- Secretary of State Check
- OFAC/PEP checks
- Certificate of Good Standing
- Any specialized certifications or licenses (e.g., PCI certification, ISO certification, proof of admission to the bar for state practices)
- Tax ID
- Credit Report
- Dun & Bradstreet (D&B) Report
- Ownership structure and affiliated companies
- Vendor complaints research findings
- Vendor negative news search findings
- List of subcontractors/fourth parties
- Picture or Google Map view of facility (if required)
- Reputation risk check (Better Business Bureau and CFPB consumer complaint database)

Common Document Collection Items to Collect

Low-Risk Vendors – All items of Baseline Document Collection

Moderate-Risk Vendors – All items for Low-Risk Vendors, **plus:**

- 3 years audited financials
  (if can't obtain, then a credit report or annual report can help)
- Insurance certificates
- Any applicable compliance policies
- Vendor's third-party management practices
- SOC report (with bridge letter, if needed)

- Reports of internal and external audits
- AML policies (if applicable)
- Information security policy
- Record retention/data destruction policy
- Background check policy
- Hiring practices

Common Document Collection Items to Collect

High-Risk Vendors – All items for Low and Moderate-Risk Vendors, **plus:**

- Policies and procedures
- Biographies of key senior management and owners of the organization
- Logical access management policy
- Data classification and handling policy
- Incident management policy
- Business continuity/disaster recovery plans, protocols, and results

- Penetration testing results
- Vulnerability testing
- Network diagram
- Data flow diagram, including third-party/fourth party
- Record of outages and SLA violations (usually a contractual obligation)
- Potential on-site visit

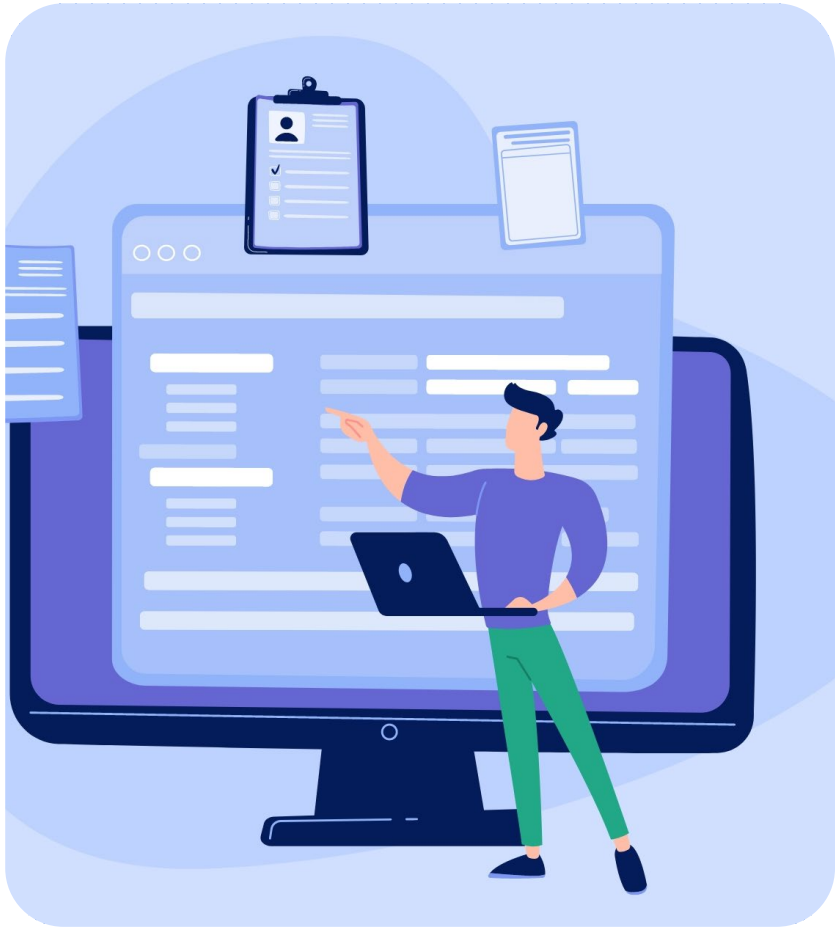
venminder

Additional Document Collection Items You May Need to Collect

Depending on the type of product or service provided, you may need to do some additional document collection.

Examples include:

- If they'll be storing or processing credit card information, you need to be sure they're PCI compliant.
- If they'll be performing collection services, it's important to ensure that they possess the necessary licenses and certifications in the required jurisdictions.
- If they'll be storing, processing, or transmitting personal health information (PHI), you need to be sure they're Health Insurance Portability and Accountability Act (HIPAA) compliant.



venminder

Documentation Requirements for Fourth Parties

Don’t forget about fourth parties (your third party’s vendor with whom you don’t have a direct contract), especially those of your critical third parties or who are high risk and have access to your data.

Here are a few fourth-party vendor due diligence documentation considerations.

- Leverage your third parties. Work closely with them to obtain fourth-party information (SSAE 18 requires their disclosure).
- Require disclosure of critical fourth parties – your third party should provide a list, including the product or service type.
- Require evidence of fourth-party risk assessments, due diligence, and monitoring, especially for critical fourth parties.
- Require your third party to provide their vendor risk management policy and vendor issues management procedures.
- Make sure that your third-party contract includes obligations related to fourth-party involvement, such as requiring their inclusion in audits.

venminder

Issues and Challenges for Document Collection

The following are common document collection and issues challenges:

- Vendor won’t provide documents
- Chasing vendors for documents can be a hassle, especially if they're unresponsive and need multiple follow-ups
- Only doing document collection on the vendor level instead of on the product/service level
- Lack of centralized repository
- No available internal SME to review complex vendor evidence

venminder

A Large Vendor Won't Respond to Your Due Diligence Requests

It's not uncommon for very large vendors to ignore all requests for due diligence requests. Reasons for this include:

- There are simply too many customers for them to respond effectively
- The information can be obtained on their website or through a customer portal
- They aren't legally obligated to provide the data – this is especially true when the vendor issues you non-negotiable terms of service agreement

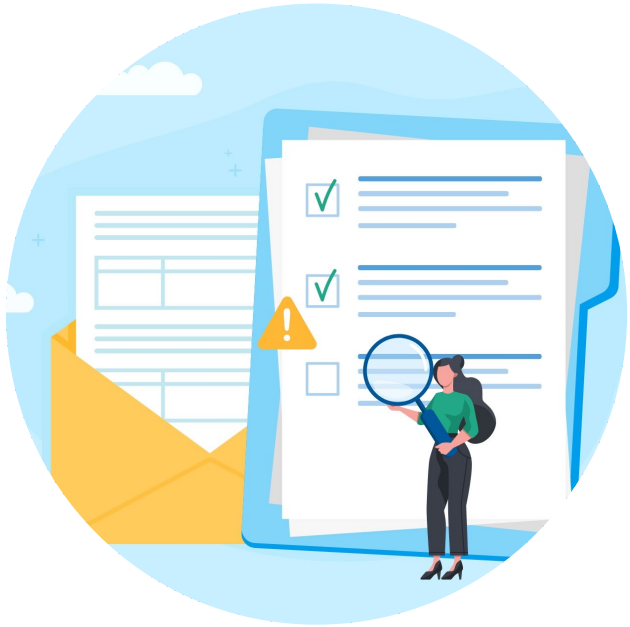
No response from the vendor doesn't alleviate your organization's responsibility to conduct due diligence.

Auditors and examiners will anticipate that a reasonable level of effort was exerted in assessing the safety and stability of your third-party vendors – including the major ones. **Something is always better than nothing.**

Your senior management and board should be aware of exceptions to due diligence requirements for any critical or high-risk vendor.

Tips and Tricks for Collecting Due Diligence Information on Large Vendors

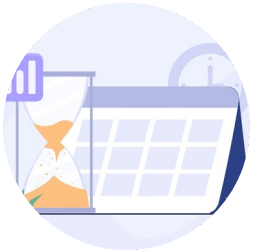
- Make the request anyway and document your efforts
- Try working directly with the sales rep or account manager – ask if there is a customer portal or other way to obtain the information
- Look on their website or do an internet search for terms such as:
  - "(company name) SOC 2 or SOC 3 reports"
  - "(company name) privacy policy"
  - "(company name) privacy and security"
  - "(company name) risk management and security framework"
- Public companies must disclose audited financials and conditions in 10-K reports
- Consider using a vendor risk alert or monitoring service that can provide a qualified risk profile or other data to contribute to your due diligence efforts



venminder

The Vendor Can’t or Won’t Provide Requested Documentation

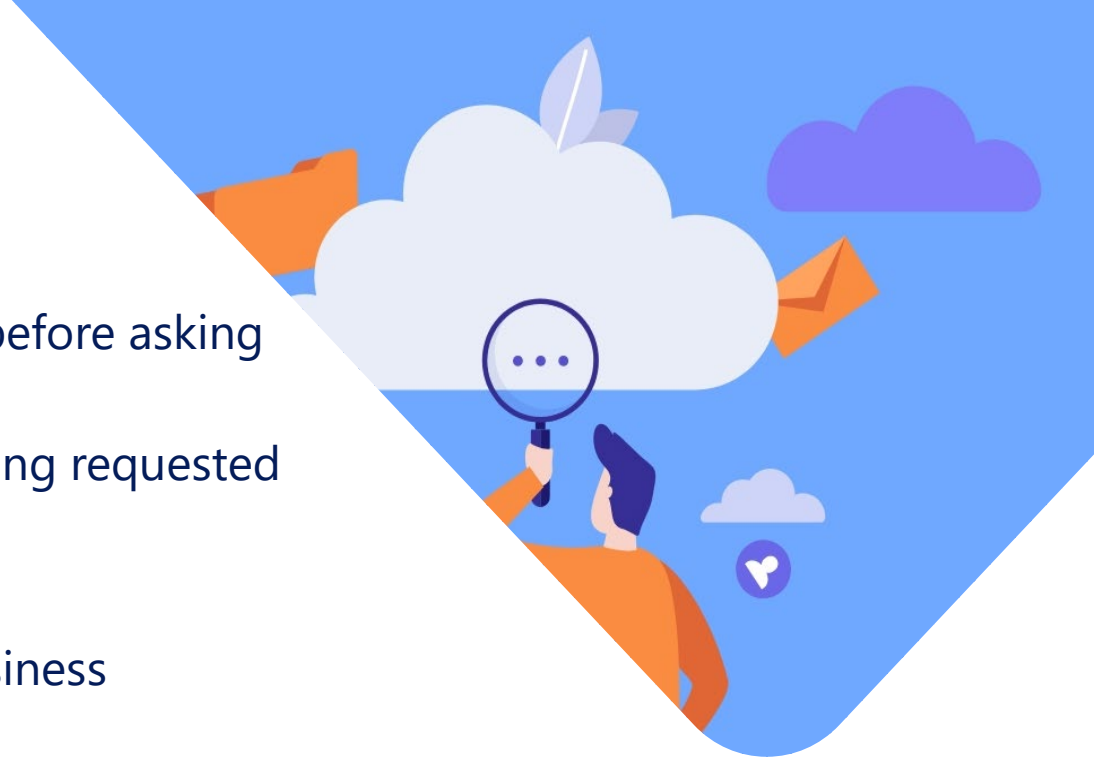
If a vendor is unable or unwilling to provide certain documentation, it’s advisable to take the following steps:



- Document the situation including the vendor’s rationale for not providing the document
- Determine if you can accept an alternative document
- Request a heavily redacted document
- Request the vendor share the document via an online sharing platform
- Review the document during an on-site visit
- Schedule a phone call for an SME to review controls verbally with the vendor’s senior management or internal expert
- Ask the vendor for a written attestation of suitable controls (per your documented requirements)
- If necessary, seek approval from senior management through a formal risk acceptance process for any exceptions

venminder

Additional Considerations for Missing Due Diligence

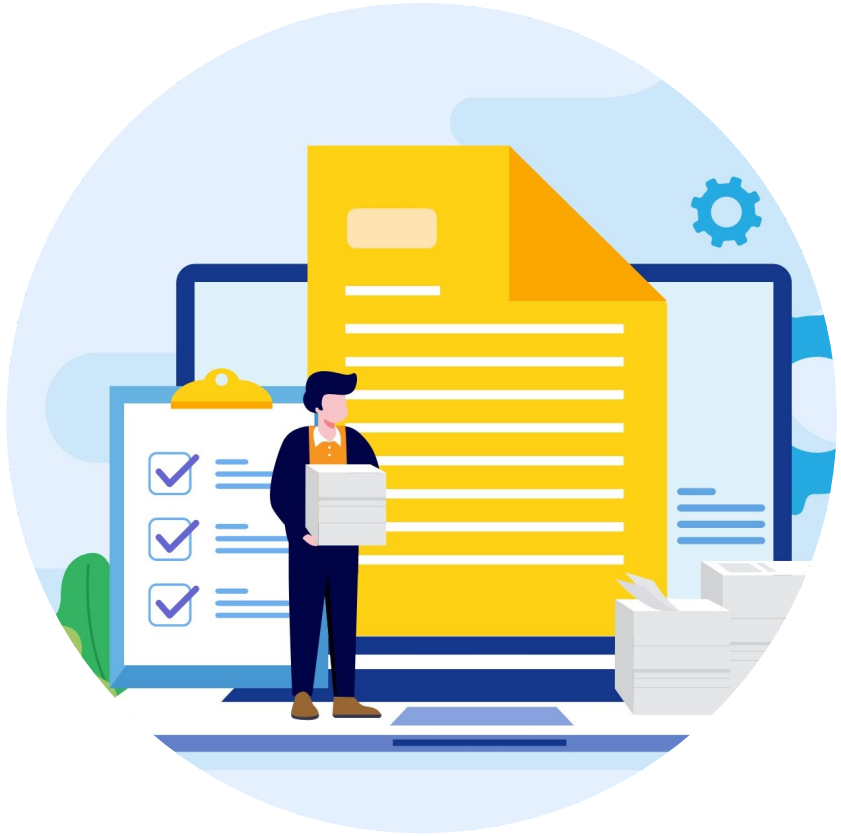


- Make sure there is a binding non-disclosure (NDA) agreement before asking the vendor to provide sensitive data.
- Ask the vendor to formally document their reasons for not sharing requested data and consider:
  - Do their reasons make sense?
  - Are they providing a vague reason such as, “it’s not our business practice?”
  - Do they claim that their “other customers do not require due diligence?”
  - Are other vendors offering the same product and service able to provide the requested information?
  - Does the vendor truly understand the purpose and value of due diligence not only as a best practice but also as a regulatory requirement?
  - Does it seem like the vendor is potentially hiding something?

If a vendor declines to share data without a valid justification or neglects the importance of due diligence, it’s a warning sign that should be treated with seriousness. In the case there is no satisfactory explanation for withholding the data, it’s a cause for concern.

venminder

Once You've Gathered the Documentation… Then What?



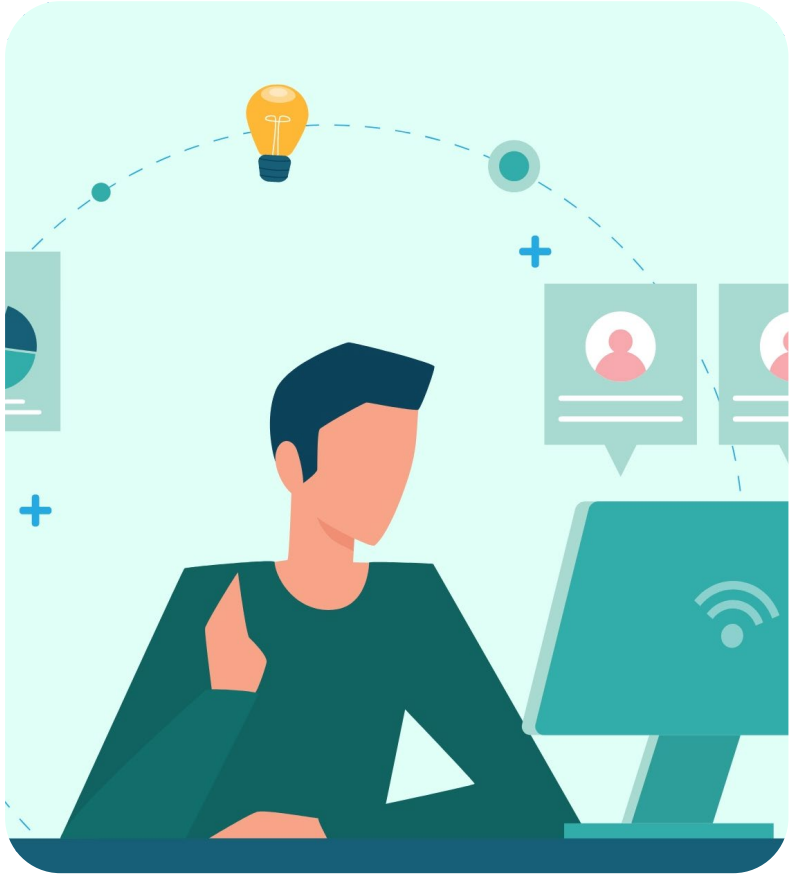
What are the next steps you should take after gathering the documentation?

- Take note of and record the expiration dates of the documentation, such as independent third-party audit reports, insurance certificates, licenses, business continuity plans, certifications, etc.
- Make sure you have the documents organized and easily accessible for your subject matter experts in a single document repository.
- Make sure you have processes to manage document version control.
- Coordinate the necessary subject matter expert reviews and timing.
- Communicate review schedules to stakeholders and keep on top of them. Delays (including the reason for the delay) should be communicated to the stakeholders. Standardized reporting can make this process easier.

venminder

Due Diligence Issue Remediation and Management

- Document and track open issues and required remediations.
- Work with a SME to determine if the remediation must take place before the contract execution (a deal breaker) or if post-contract remediation is acceptable.
  - Ensure all post-contract remediation is written into the contract.
- Notify the vendor and the vendor owner of issues or findings discovered during due diligence that require remediation. Remember to establish clear deadlines for addressing and resolving any issues that arise.
- Ensure that remediation actions and evidence are reviewed by the SME before closing any issues.



venminder

Other Ways to Make Your Document Collection Easier and More Efficient

1. Ensure your vendor owners understand the due diligence process and can explain it to their vendors – they should be the vendor's first point of contact for questions or concerns.

2. Standardize your document types by risk domain and product/service type.

3. Don't ask for documentation you don't need.

4. Provide a list of FAQs (frequently asked questions) to your vendors with due diligence document requests.

Using Third-Party Risk Management Software and Services

- Manual processes are time-consuming and extremely error-prone.
- Juggling several emails containing scattered information can be difficult to manage and organize effectively.
- Constantly updating spreadsheets, schedules, and vendor files, as well as sending out numerous emails can be quite inefficient.
- When due diligence is delayed, your organization misses out on the timely benefits of a new vendor relationship. This can result in lost time, cost savings, and revenue.

Incorporating third-party risk management software and services can enhance your organization's productivity and efficiency, enabling you to achieve more with less and within shorter timeframes.

venminder

TPRM Software and Due Diligence

TPRM software is typically designed to help your organization:

- Send, receive, and retain vendor communications all in one place
- Send and collect vendor risk questionnaire data
- Automate requests for documentation
- Better manage vendor documentation as it's uploaded directly to the system by the vendor
- Keep track of due diligence requests and submissions
- Create a shared workspace for all stakeholders
- Collect and retain subject matter expert reviews and findings
- Generate due diligence schedules and reports
- Track documentation with expiration dates
- Track and manage issues requiring remediation

venminder

TPRM Software and Due Diligence

If your organization lacks the necessary resources to tackle due diligence effectively, professional third-party services companies can assist your organization by:

- Providing qualified and credentialed subject matter experts to conduct vendor risk reviews
- Managing the due diligence collection and organization process
- Following up with vendors missing documentation or requiring remediation
- Providing other administrative support (due diligence or other) for TPRM process or programs

venminder

Does your organization include a standard right to audit clause in vendor contracts?

a. Yes
b. No
c. Not sure

Key Takeaways

- **Due diligence is necessary** – it's a best practice and regulatory expectation.
- **When engaging with vendors, it's important to conduct due diligence based on the level of associated risks.** The higher the risks, the more comprehensive the due diligence process should be.
- Documentation for due diligence serves as evidence not only of the vendor's controls but also of your organization's compliance.
- Make sure due diligence and right-to-audit clauses are included in your vendor contracts.
- Standardize your documentation requests by risk domain, level, and product or service types.

venminder

Key Takeaways *CONTINUED*

- Don’t ask for documents you don’t need.
- Make vendor documentation requests clear and concise.
- Make sure to review what you receive promptly.
- Keep following up.
- Ensure your vendor owners understand the due diligence process and can explain it to their vendors.
- Track and manage issues discovered in due diligence.
- Consider using TPRM software and services.

venminder

THANK YOU

ALSO JOIN US AT

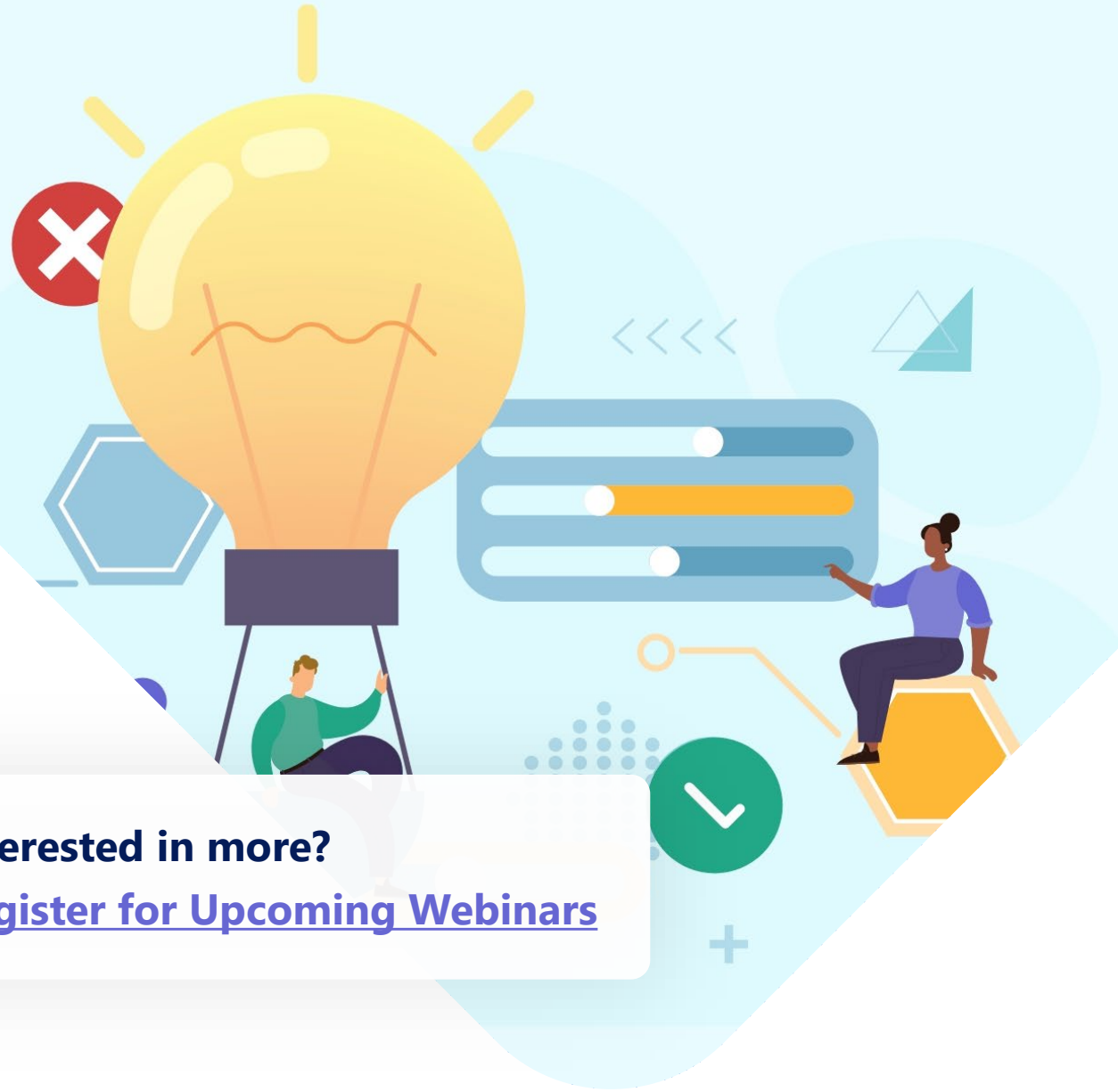
Our Upcoming Webinars:

JULY 11, 2023

How to Classify Who Is a Critical Vendor

JULY 25, 2023

Vendor Exit Strategies and Plans: Managing the Offboarding Process Safely and Effectively



Interested in more?

[Register for Upcoming Webinars]

venminder

Post a Question:

POST A QUESTION:
www.thirdpartythinktank.com

THIRD PARTY thinktank
A Community for Risk Professionals

EMAIL US:
resources@venminder.com

FOLLOW US:
@venminder

venminder