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

Vendor Due Diligence and Contract Management Best Practices

PRESENTED BY

Nicole O'Brien

Kelly Vick

Third-Party Risk Officer
Venminder
nicole.obrien@venminder.com

President
Venminder
kelly.vick@venminder.com

October 20, 2020

Session Agenda

1

Initial Vendor Due
Diligence – Importance,
Themes, Examples and
Traps to Avoid

2

An Understanding of Contract
Management

3

Overview of Ongoing
Monitoring and Hazards of
Falling Asleep at the Wheel

venminder

The Importance of Vendor Due Diligence

- Look before you leap!

- Regulatory requirement

- Sound business practice

- Helps you make informed decisions on what is

  best for your organization

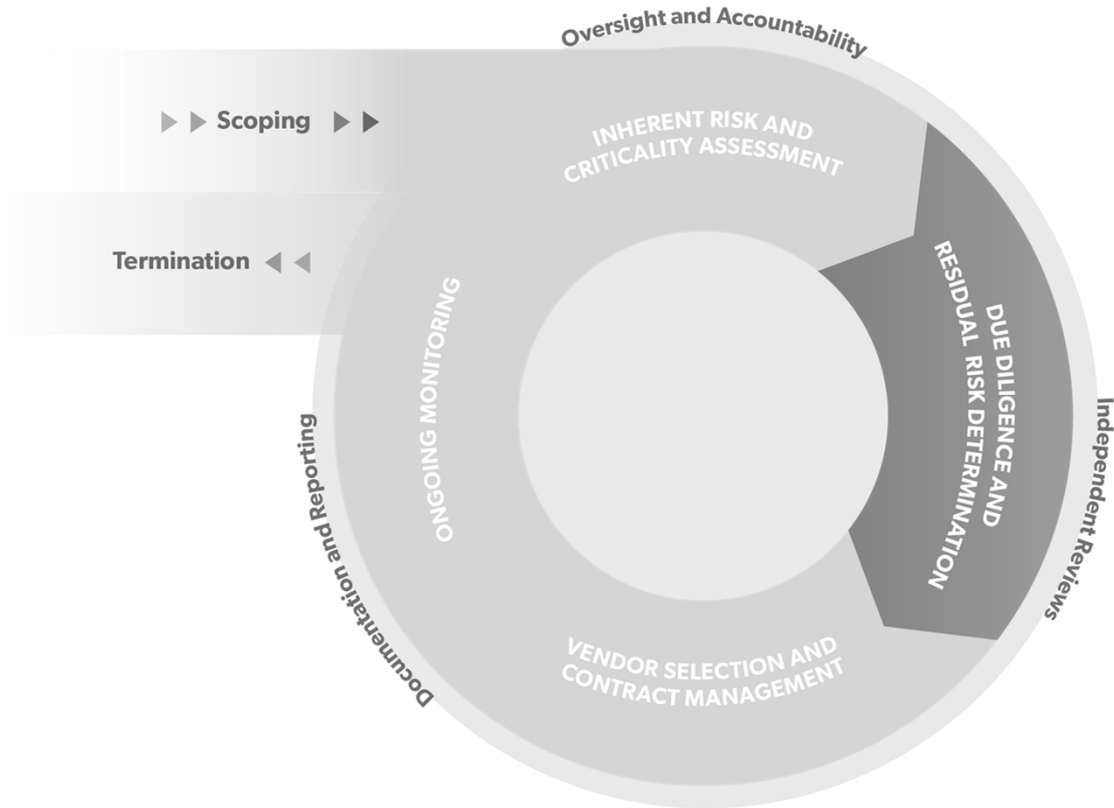- Provides insight into the future relationship

venminder

Poll Question

When does your organization do due diligence?

a. Initial due diligence
b. Periodically after boarding a new vendor
c. Both at initial due diligence and periodically afterwards
d. Never
e. Not sure

venminder

Where Initial Due Diligence Fits into the Third-Party Risk Management Lifecycle

Scoping

Termination

Oversight and Accountability

INHERENT RISK AND CRITICALITY ASSESSMENT

DUE DILIGENCE AND RESIDUAL RISK DETERMINATION

Independent Reviews

ONGOING MONITORING

Documentation and Reporting

VENDOR SELECTION AND CONTRACT MANAGEMENT

venminder

Key Themes in Vendor Due Diligence

- Pre-Contract

- Risk-based and tailored to the product or service

- Document everything
    - Attempts to gather information
    - Results of document reviews
    - How it impacts the overall (residual) risk rating

venminder

Risk-Based Due Diligence Examples

Direct Interaction with Customers	Stores Sensitive Data	Unescorted Access to Facilities	Provides Critical Service
• Reputation assessment • Background investigations and HR policies • Compliance and performance training and monitoring • Third-party risk management	• Information Security Policies • Penetration testing and vulnerability scanning • SOC assessment • Third-party risk management • Insurance	• Background investigations and HR policies • Compliance and performance training and monitoring • Insurance	• Financial assessment • Business continuity & disaster recovery planning and testing • Third-party risk management • Reputation assessment • Insurance

venminder

Traps to Avoid

- **"We've never been asked that before"**

- **One-size-fits-all questionnaires**

- **Dusty due diligence documents**
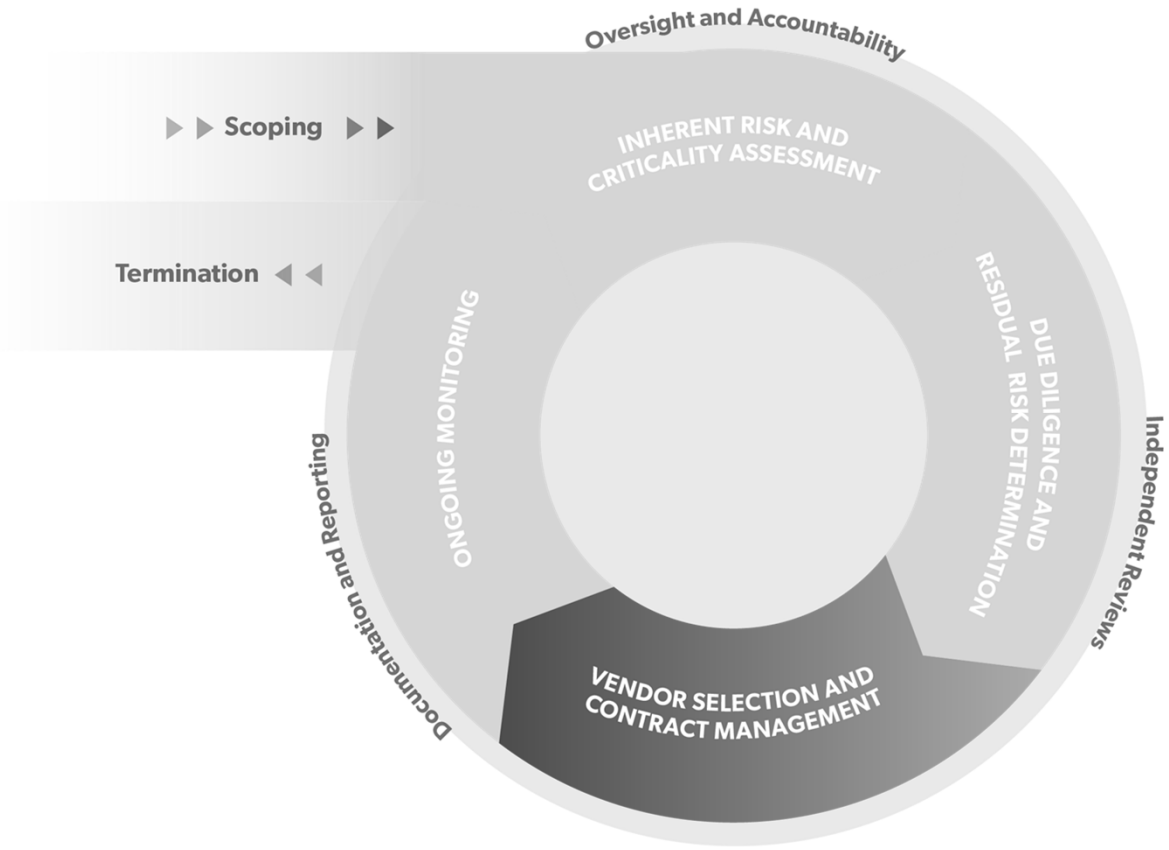
- **The never-ending assessment**

venminder

Let's now dive into effective vendor contract management...

venminder

Poll Question

Do you currently vet your vendors before signing a contract?

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

venminder

Where Contract Management Fits into the Third-Party Risk Management Lifecycle

Oversight and Accountability

Scoping

Termination

INHERENT RISK AND CRITICALITY ASSESSMENT

ONGOING MONITORING

DUE DILIGENCE AND RESIDUAL RISK DETERMINATION

Independent Reviews

Documentation and Reporting

VENDOR SELECTION AND CONTRACT MANAGEMENT

venminder

What Is Contract Management?

Vendor contract management is the oversight of written agreements with vendors that provide an organization with products or services. It entails:

- Negotiating contract terms

- Incorporating essential controls

- Having a process in place for review, negotiation, approval and execution of contracts

- Managing and tracking contract inventory

  - Service level agreements (SLAs)

  - Terminations and renewal dates

venminder

Why Is Contract Management Important?

- Save money, time, expense and avoid unnecessary headaches

- Establish expectations to assure your organization is protected from all areas of vendor risk

- Avoid missing significant contract dates

venminder

Who Is Generally Involved

- Legal

- Vendor Management

- Lines of Business

- Information Technology

- Information Security

- Business Continuity Management

- Compliance

- Operations

- Risk

- Finance

- Procurement

venminder

Major Elements That Should Be Included

- Business terms

- Term, notice and automatic renewals

- Identify and mitigate risks

- Confidentiality provisions

- Disposition of data throughout the relationship (post-termination)

- Harmless and indemnification provisions

- Events of default

- Remedies

- Cause for termination

- Termination assistance

- Dates and deadlines

- Warranties and representations

- Dispute resolution

venminder

Poll Question

Do your contracts identify what will happen to your data upon termination?

a. Yes
b. No
c. Not sure

venminder

Additional Provisions for Critical or High-Risk Vendor Contracts

- Defined SLAs

- Adequate security and confidentiality provisions

- Subcontractor notification requirements

- Ongoing right to audit

- Business continuity and disaster recovery planning

- Data protection agreement

- Insurance requirements

venminder

Common Contract Mistakes to Avoid

Regulators and auditors are looking for well-developed and organized programs. They'll likely find contract management issues with any of the following:

- No senior management/board approval

- Lack of contract repository

- Lack of proper contract tracking

- Contract execution without documented vendor vetting
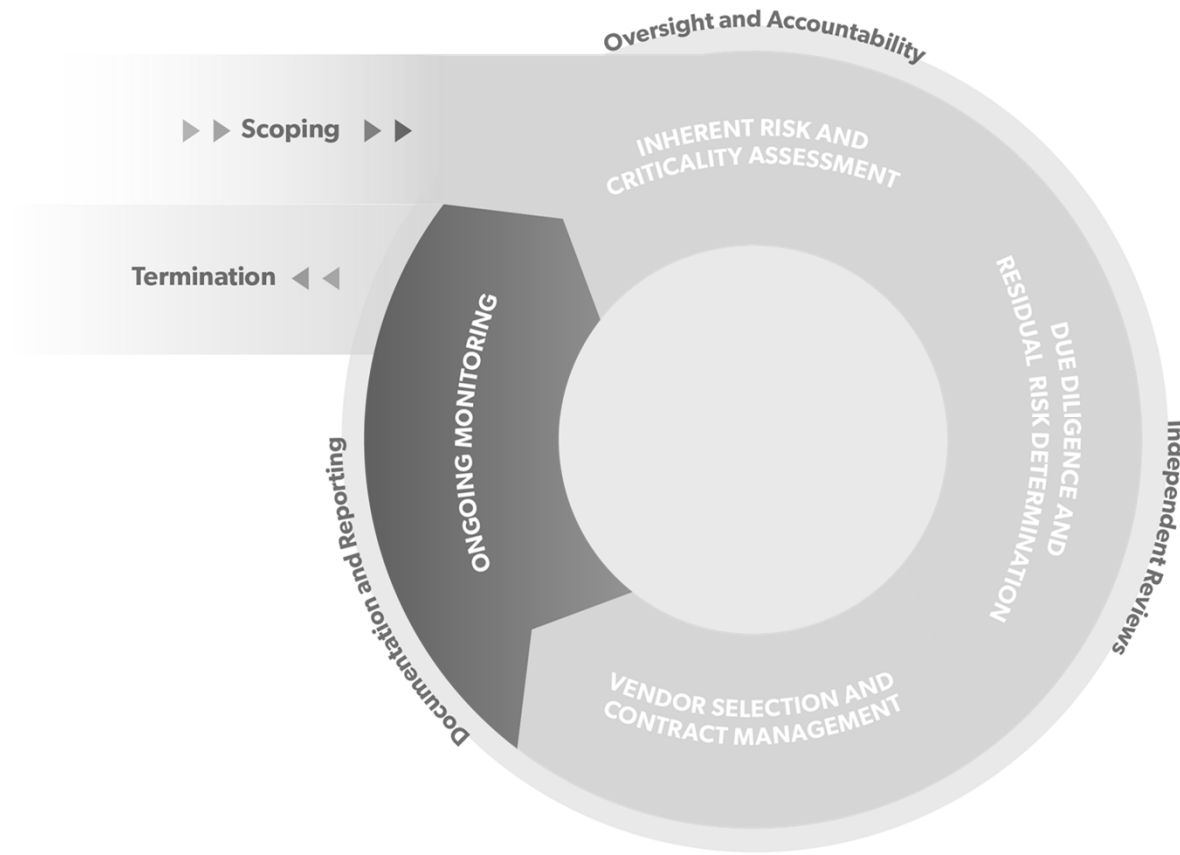
- Roles and responsibilities are not clearly identified

venminder
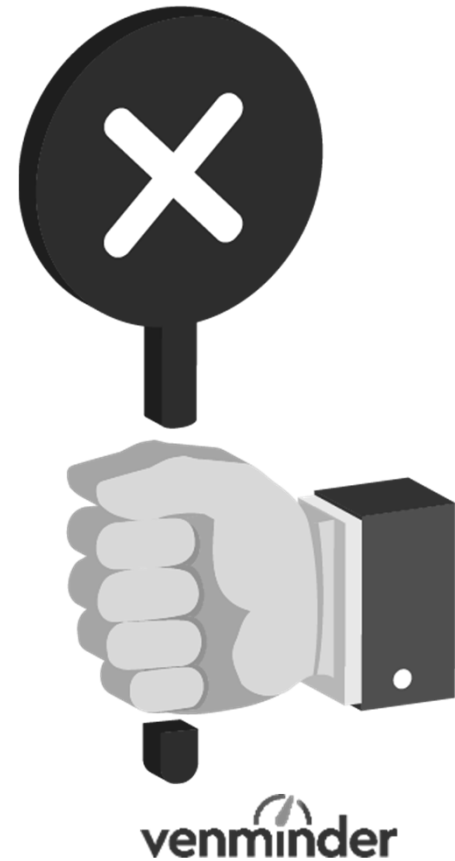
Now that services are up and running, we continue ongoing monitoring.

venminder

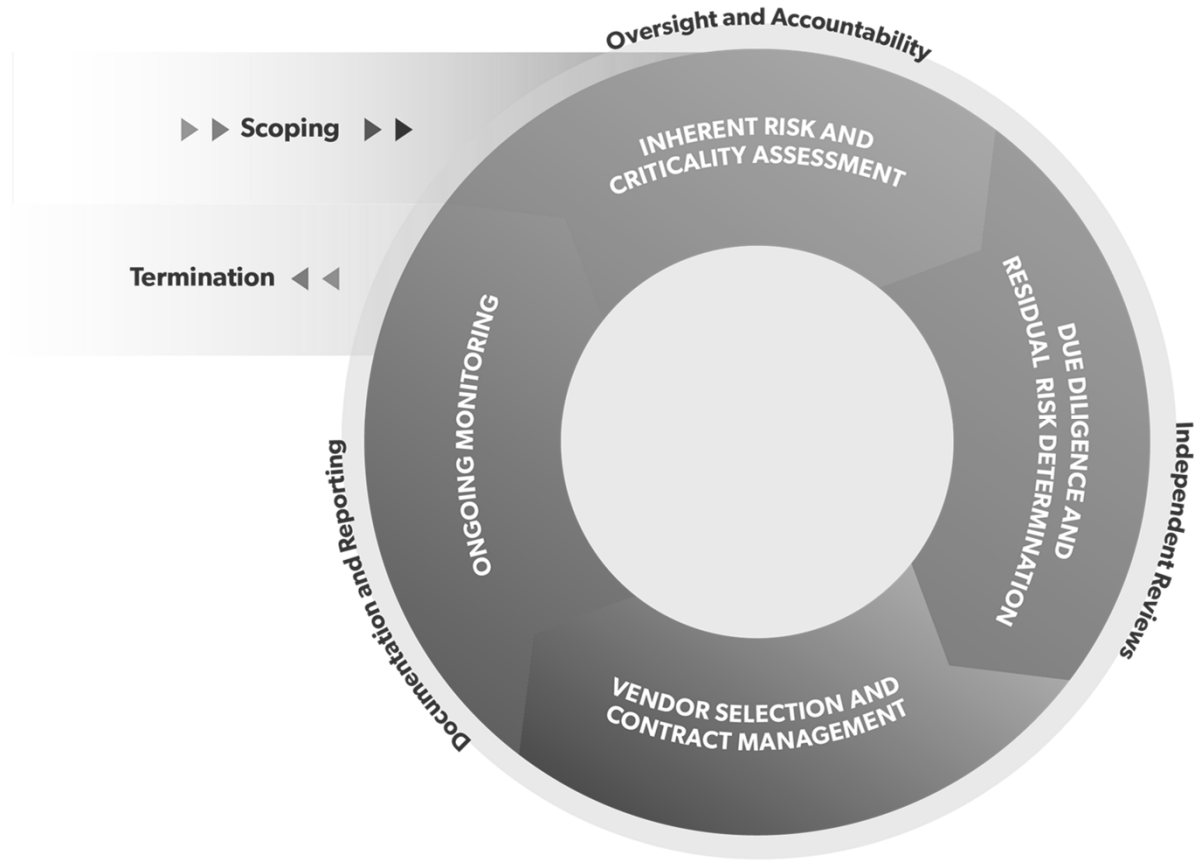# Contract Management & Due Diligence Do Not End When the Contract Is Signed

- Ongoing oversight is required by most regulatory guidance

- Includes periodic reviews of vendor due diligence, frequent monitoring of contract SLAs and addressing outstanding risks and/or deficiencies
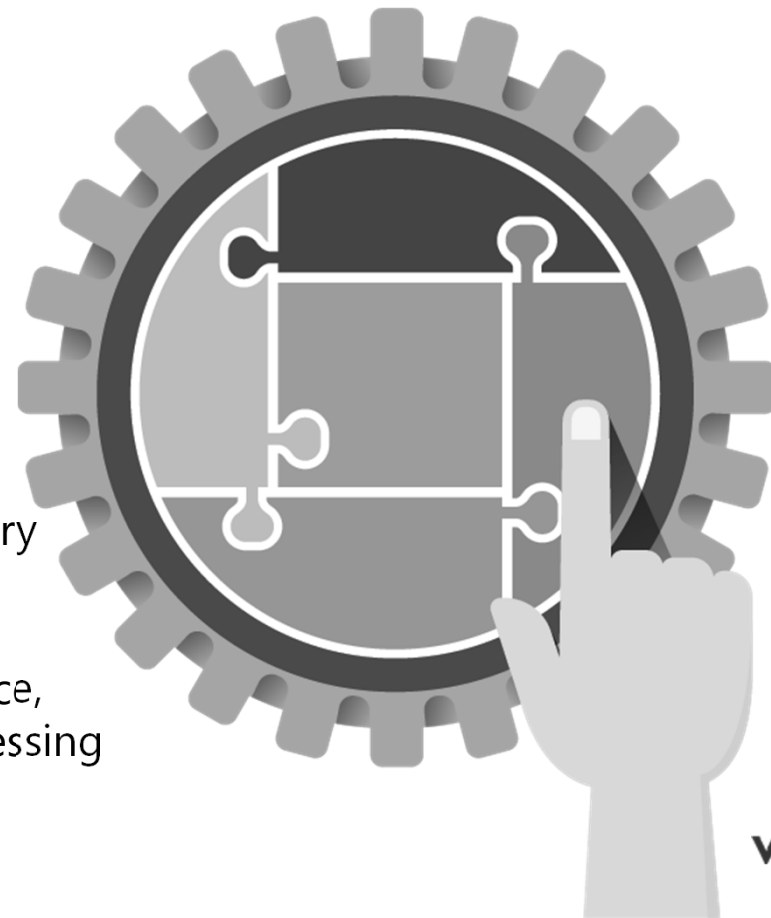
venminder

Where Ongoing Monitoring Fits into the Third-Party Risk Management Lifecycle

venminder

Where Ongoing Monitoring Fits into the Third-Party Risk Management Lifecycle

Oversight and Accountability

Scoping

Termination

INHERENT RISK AND CRITICALITY ASSESSMENT

DUE DILIGENCE AND RESIDUAL RISK DETERMINATION

Independent Reviews

ONGOING MONITORING

Documentation and Reporting

VENDOR SELECTION AND CONTRACT MANAGEMENT

venminder

Continuing Due Diligence

Verify vendors still meet expectations and identify areas of concern, such as:
- Faulty security controls or customer complaints
- Negative changes regarding the vendor

Set a schedule for ongoing due diligence assessments that is appropriate for the relationship:
- Critical and inherently high risk, Annually
- Moderate risk, 18-24 months
- Low risk, 2-3 years

venminder

Ongoing Contract Management

- Managing the vendor relationship is essential for monitoring the service delivery

- Track renewal dates

- Schedule ongoing meetings to address service delivery

- Assure SLAs are monitored on a routine basis
    - Track receipt of deliverables laid out in contract requirements

- Seeing through the transaction

- Discover contract gaps, poor vendor trends and declining service levels

- Make individuals accountable

venminder

# Hazards of Falling Asleep at the Wheel

- Third party stops reporting

- Problems are not discovered until it is too late

- Customers complain but no one is listening

- Regulators notice issues before your organization

- Inadequate oversight can lead to enforcement actions

venminder

Best Practices

- Fluid communication between associated teams

- Shared databases and repositories

- Win-win mentality

- Policy is not just for show

- Good note taking and documentation

- Understand your industry's regulations and best practices

- The lifecycle is a 'wheel' for a reason
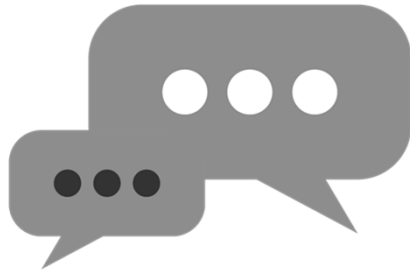
venminder

Questions & Answers

Post a Question:

www.thirdpartythinktank.com

THIRD PARTY
thinktank

Email Us:

nicole.obrien@venminder.com

kelly.vick@venminder.com

Follow Us:

@venminder

venminder

Also Join Us At
Our Upcoming Webinars:

OCTOBER 29, 2020
Virtual Vendor Due Diligence Site Visits

NOVEMBER 10, 2020
Understanding and Analyzing Vendor SOC Reports

Click here to view our Webinars Page.

venminder

Thank You