# 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 Management 101

January 10, 2023


**PRESENTED BY**

**Hilary Jewhurst**

Head of Third-Party Risk Education & Advocacy
*Venminder*


venminder

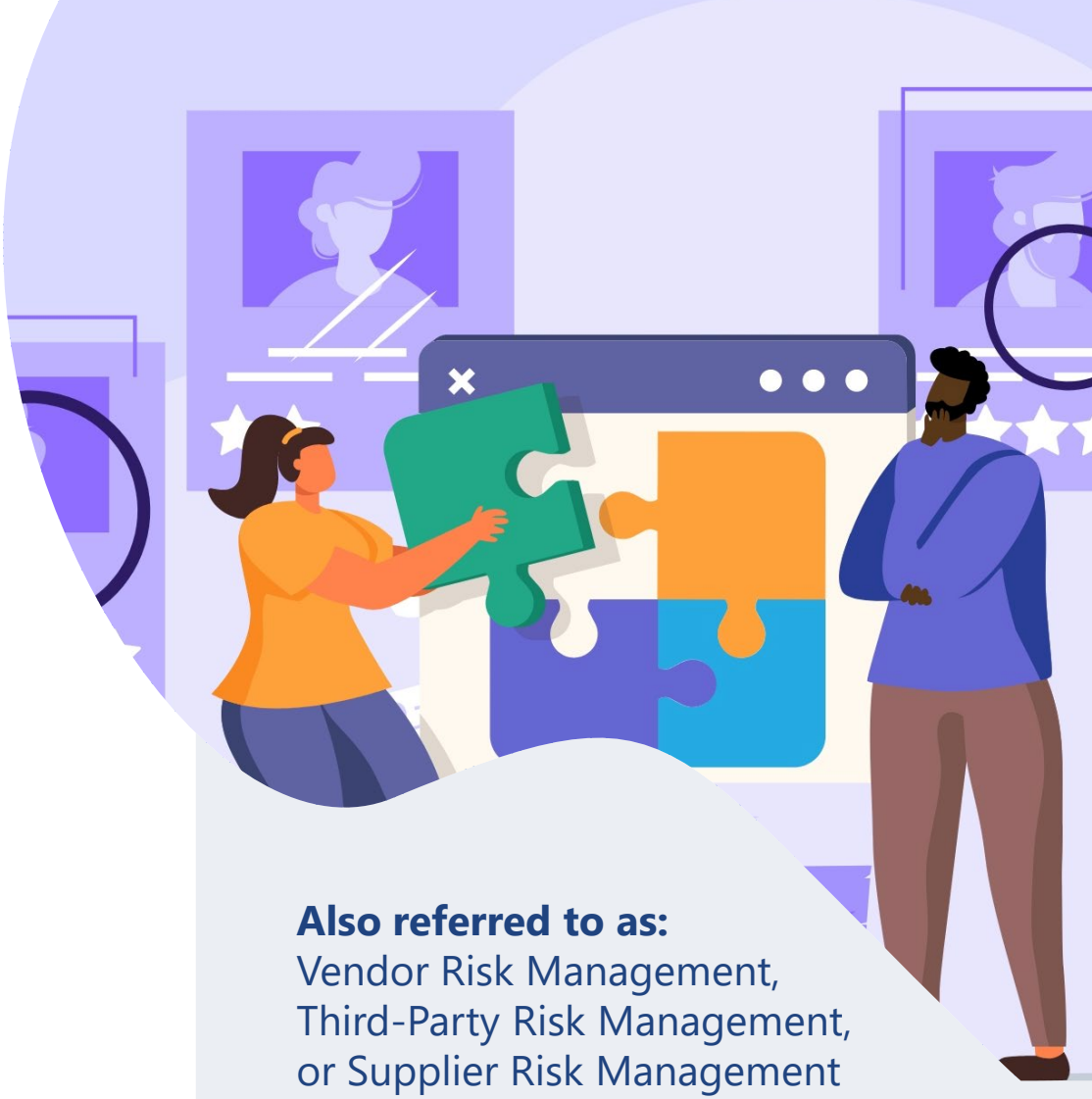
# Session Agenda

1. **Vendor management:** The who, what, why, when, and how
2. The **types of vendor risk** to identify and manage
3. **The vendor risk management lifecycle:** what it is and how to apply it
4. **Key Takeaways**

# What Is Vendor Management?

The process of fully identifying all of the significant companies that aide in the delivery of a product or service to an organization or to an organization's customers on behalf of the organization.

**It involves controlling costs, driving service excellence, and mitigating risk to gain increased value throughout the vendor relationship.**



**Also referred to as:**
Vendor Risk Management,
Third-Party Risk Management,
or Supplier Risk Management

venminder

## MANAGING RISKS INCLUDES PERFORMING DUE DILIGENCE TO ENSURE:

- The vendor has sufficient risk controls that they meet the terms of the contract
- Provides the intended value of the relationship
- Has acceptable performance
- Can continue to service your organization during outages and business interrupting events, if necessary

venminder

# Why Vendor Management Is Important Today

- It's a best practice and strategic advantage
- Vendor management has a positive ROI
- It protects your organization:
  - Enables better vendor selections
  - Improves your organization's cybersecurity profile
  - Drives improved service and innovation
  - Confirms your vendors are performing as agreed
  - Reduces the potential for supply chain disruption
  - **Is a regulatory requirement for many industries**

venminder

# Why Vendor Management Is Necessary

- The third-party risk landscape has expanded due to the pandemic
- Cybersecurity threats are prevalent and growing – ransomware is proliferating
- Business operations have completely changed for many organizations – moving to partially remote or permanent remote work for their employees
- Economic pressure resulting from the pandemic is constant and financial health of many third parties is decreasing
- Business resiliency has been severely tested due to constant supply chain interruptions
- Organizations are losing staff in record numbers
- Some industries have an active regulatory environment*

** Full list of regulations is available for download in the Related Content widget.*

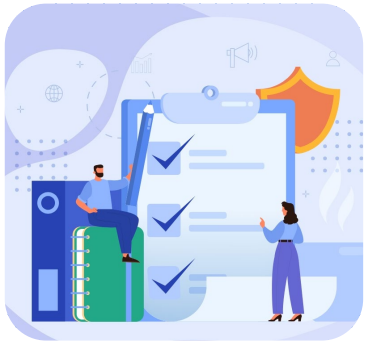
venminder

# Who Is Responsible for Vendor Management?

*Lines of Vendor Management*

THE FIRST LINE – Those that own and manage vendor risks. Often referred to as the vendor/product owner

THE SECOND LINE – Those that oversee and monitor vendor risks such as the vendor risk team, enterprise risk team, compliance, legal, finance, information security, or even sourcing and procurement



THE THIRD LINE – Those functions that provide independent assurance over vendor risks and monitor the effectiveness of vendor management activities (i.e., internal audit)

venminder

# First Line Roles and Responsibilities

## VENDOR OWNER/PRODUCT OWNER

**These individuals are usually responsible for:**

- Products or services provided by the vendor
- Identifying and managing risk associated with the product or service and the vendor relationship
- Setting appropriate service level agreements and key performance indicators with the vendor
- Managing and reporting vendor performance and addressing declining performance, if necessary
- Establishing and managing a vendor exit strategy

venminder

# Second Line Roles and Responsibilities

## DEDICATED VENDOR MANAGEMENT TEAM, ENTERPRISE RISK, COMPLIANCE, ETC.

The second line provides the policies, frameworks, tools, techniques, and support to enable vendor risk and compliance in the first line. They're typically responsible for:

- Ownership of the vendor management governance documents, tools, etc.
- Monitoring first-line vendor risk deliverables for accuracy, timeliness, and quality
- Facilitating the vendor management lifecycle activities
- Acting as the liaison between subject matter experts and vendor owners during initial due diligence and subsequent risk reviews
- Creating and distributing vendor management reporting for committees, senior leadership, and the board
- Responding to an internal or external audit or regulatory requests and issues

venminder

# Second Line Roles and Responsibilities *CONTINUED*

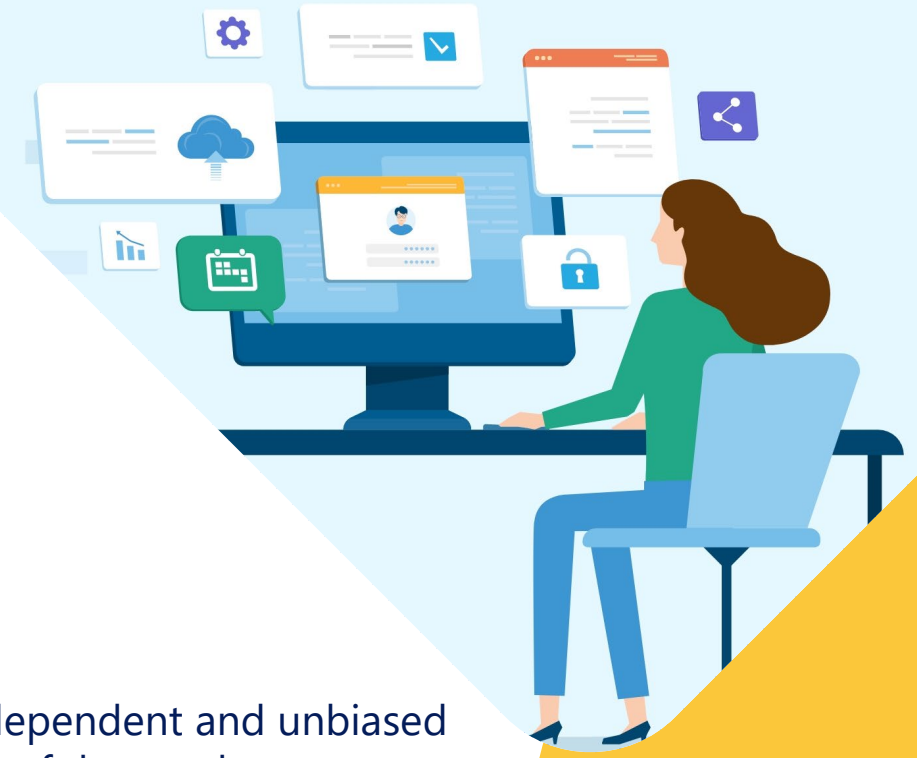
## SUBJECT MATTER EXPERTS (SMEs)

SMEs can be internal or external. These are the individuals or organizations tasked with reviewing and assessing vendor-provided evidence of controls for the purposes of vendor due diligence and periodic risk reviews. Their responsibilities include:

- Reviewing documents provided by the vendor and other materials to validate a substantial control environment
- Identifying any controls gaps or weaknesses
- Providing a documented assessment and recommendations related to the sufficiency of required vendor controls
- Consulting with the first and second lines regarding the seriousness of any control deficiency
- If remediation is possible, they'll review additional documentation or evidence provided and deliver a second assessment to validate if the issue has been remediated

venminder

# Third Line Roles and Responsibilities



## INTERNAL AUDIT

The third line's primary role is to ensure that the first two lines operate effectively and in compliance with all laws and regulations. The third line is responsible for:

- Conducting regular audits on the vendor management program and on individual processes and controls within the program
- Identifying and documenting deficiencies within the vendor management program and monitoring the closure of the issues per the stated requirements
- Responding to regulatory or legal inquiries as appropriate
- Provide independent and unbiased evaluations of the vendor management policy, program, processes, and work product
- Confirming to the executive leadership team and the board that identified gaps or weaknesses are remediated

venminder

# Why does your organization do vendor management?

a. It's a regulatory requirement
b. It improves our bottom line, operations, reputation, etc.
c. All the above
d. We don't currently do vendor management
e. Not sure

# Internal Oversight and Governance

## SENIOR MANAGEMENT/THE EXECUTIVE TEAM

Responsible and accountable for all vendor management practices and processes at their organization

Ultimately accountable for ensuring those activities are appropriate for the level of risk, that effective controls are in place, and that corporate governance and oversight is effective

# Internal Oversight and Governance *CONTINUED*

## THE SENIOR MANAGEMENT/EXECUTIVE TEAM RESPONSIBILITIES INCLUDE:

- Setting the “tone-from-the-top," ensuring that the importance of vendor management is understood through the organization
- Integrating consideration of vendor risk and vendor management into strategy development and business decision-making throughout the organization
- Ensuring that enough resources are allocated to vendor management, including skilled and competent individuals, subject matter experts, technology, tools, etc.
- Reviewing/approving the vendor management policy
- Reviewing and understanding the types and level of risks present in the vendor portfolio
- Knowing which vendors are considered critical to the organization
- Addressing vendor risk issues or concerns escalated to them in an effective and timely manner

# Internal Oversight and Governance *CONTINUED*

## THE BOARD OF DIRECTORS

Along with the executive team, the board are ultimately accountable for the effectiveness of vendor management activities at the organization

# Internal Oversight and Governance *CONTINUED*

## THE BOARD OF DIRECTORS' RESPONSIBILITIES INCLUDE:

- Emphasizing, via their oversight role, the CEO and senior executives must prioritize vendor management
- Integrating consideration of vendor risk and vendor management into strategy development and business decision-making throughout the organization
- Identifying and reviewing ongoing monitoring results of critical activities and vendors
- Reviewing the results of periodic independent reviews (both internal and external) of the organization's vendor management process
- Ensuring senior management has allocated sufficient resources to ensure effective vendor management
- Approving risk-based policies that oversee the vendor management process

venminder

# External Oversight

## REGULATORS

- Regulators are the specific agencies appointed by the government to oversee and regulate specific domains or industries
- Some examples of federal regulatory include the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Securities and Exchange Commission (SEC), and the Consumer Financial Protection Bureau (CFPB)
- Other industry regulators include the Occupational Health and Safety Administration (OSHA) and Federal Trade Commission (FTC)
- There are also state and local regulators (e.g., insurance is regulated at the state level)

venminder

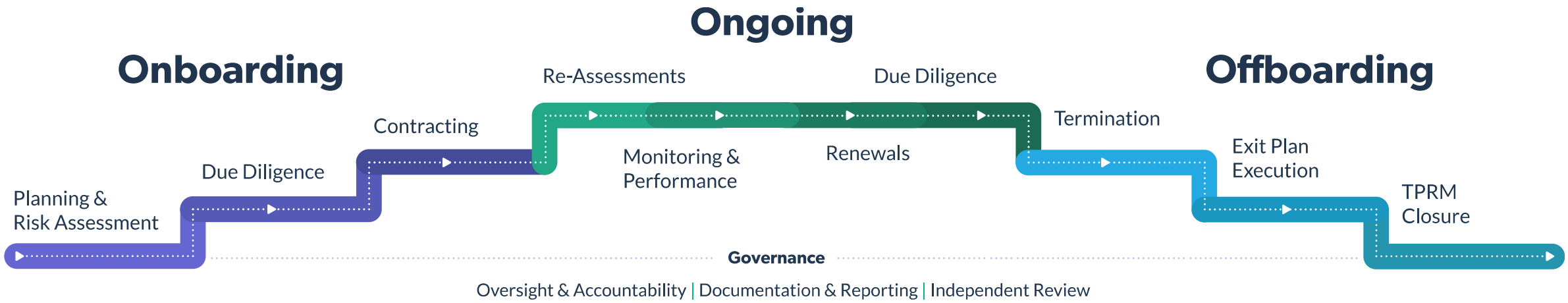
# External Oversight

*CONTINUED*

## A REGULATOR'S RESPONSIBILITIES INCLUDE:

- Compelling transparency of information and decision-making on the part of the regulated organization
- Monitoring the performance and compliance of the regulated company or organization and publishing the findings of its investigations or audits
- Carrying out enforcement actions, such as directing the company to comply through orders, imposing fines or other financial penalties, and/or revoking a license to operate

# The Third-Party Risk Management Lifecycle



# Oversight & Accountability, Documentation & Reporting, and Independent Review

## Oversight & Accountability

- Senior leadership and the Board
- Internal/External Audit
- Vendor Management Team
- Risk Committees

## Independent Reviews

- Internal/external audit review
- Regulatory exams
- SOC (and similar) reports

## Documentation

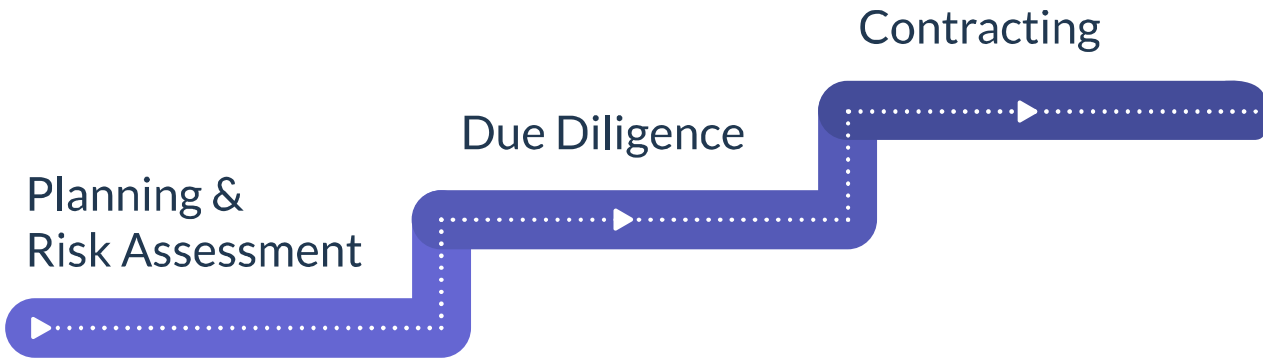
- Vendor management policy
- Vendor management program document
- Vendor management procedures

## Reporting

- Vendor management program reporting for senior executives and the board
- Due diligence and risk monitoring status reports
- Open issues reporting
- Performance management reporting

venminder

# Stage 1: Onboarding

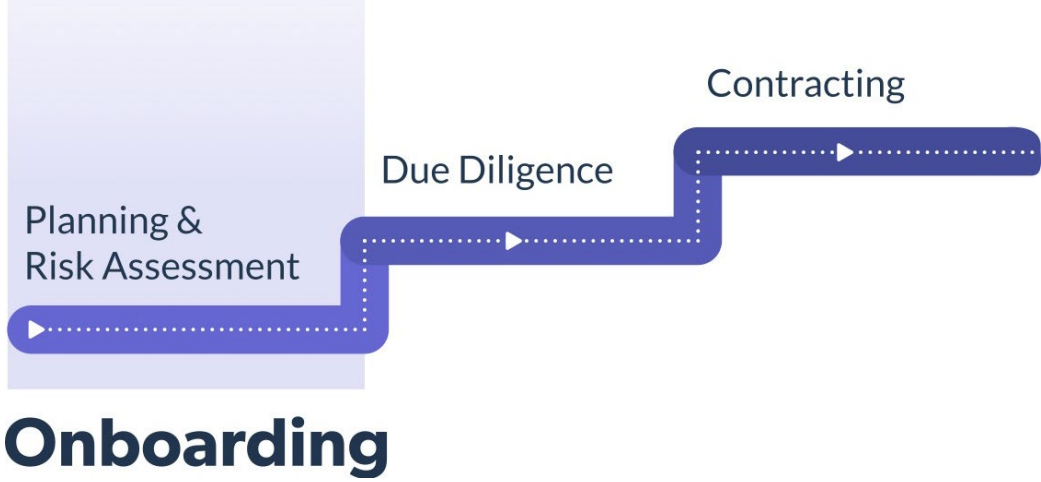



## Onboarding

- Bringing a new vendor into your organization requires careful planning and consideration to ensure that the engagement is built strong from the start.
- It's essential to fully understand the amount and types of risk that your organization will need to manage way before you get to the point of selecting a vendor and signing the contract.

venminder

# Planning & Risk Assessment




CREATE A REPEATABLE PROCESS TO DEFINE WHAT A VENDOR, SERVICE PROVIDER, OR THIRD PARTY IS TO YOUR ORGANIZATION.

Once you know that the third party is in scope for your third-party risk management process, you'll need to identify the inherent risk of the engagement and whether the product or service (and vendor) is considered critical to your organization's operations.

**INHERENT RISK** naturally exists as part of the product or service. This is assessed without considering any existing or future precautions or controls. Inherent risk is often rated by a tiered system on a scale of low, moderate, or high.

**CRITICALITY** reflects the business impact on your organization should the vendor fail or go out of business. Products and services necessary to sustain your core operations, interface with your customers or support your organization's ability to comply with regulatory requirements are all examples of critical vendor engagements. Every vendor should be rated as either critical or non-critical.

venminder

# What is your level of vendor management experience?

a. Brand new to vendor management
b. Some experience, but want to learn more
c. Moderate level of experience (2+ years)
d. Advanced (3-5 years)
e. Pro (5+ years)
f. Other

# Due Diligence

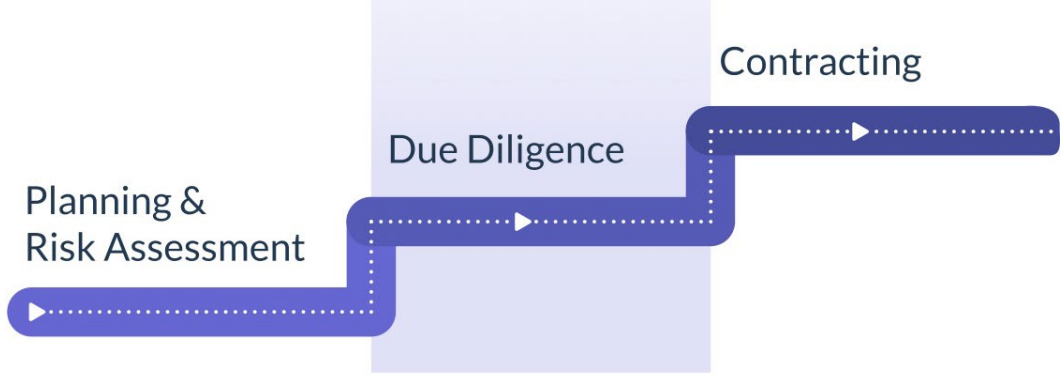
THIS IS THE STEP THAT HELPS YOU DETERMINE IF THE NECESSARY CONTROLS ARE IN PLACE TO MANAGE THE IDENTIFIED RISKS APPROPRIATELY.

**Considerations for all vendors:**

- Basic information (e.g., legal name, doing business as, professionally known as, address, locations, website, ownership structure, etc.)
- Articles of Incorporation or business license
- Tax ID #
- Liability insurance coverage/certificate of insurance


venminder

# Due Diligence *CONTINUED*

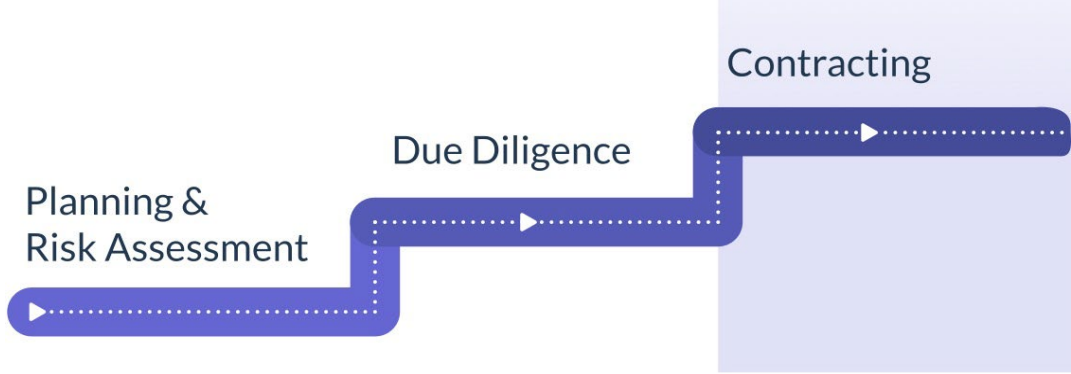



**Additional considerations for vendors who are critical or have high inherent risk:**

- Completion of a questionnaire for any additional information needed to understand risk exposure and mitigation
- Audited financial statements or the most recent financials, SOC 1, SOC 2, and SOC 3 audits, or any other information technology-related audit
- Business resumption, contingency plans, and testing summaries
- List of all subcontractors or other parties that may have access to data or information provided by your organization, or which are essential in providing services (i.e., your vendors' critical vendors)

venminder

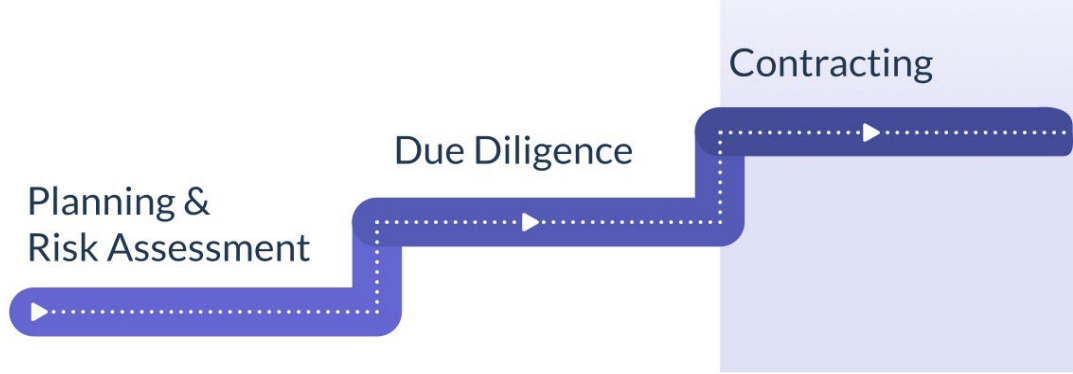
# Contracting




- Vendor contract management is the administration of written agreements with third parties that provide your organization with products or services
- For new engagements, you can go ahead and write your requirements into the new agreement
- You can use existing vendors' risk assessment and due diligence data to determine if any provisions should be made in the following contract review

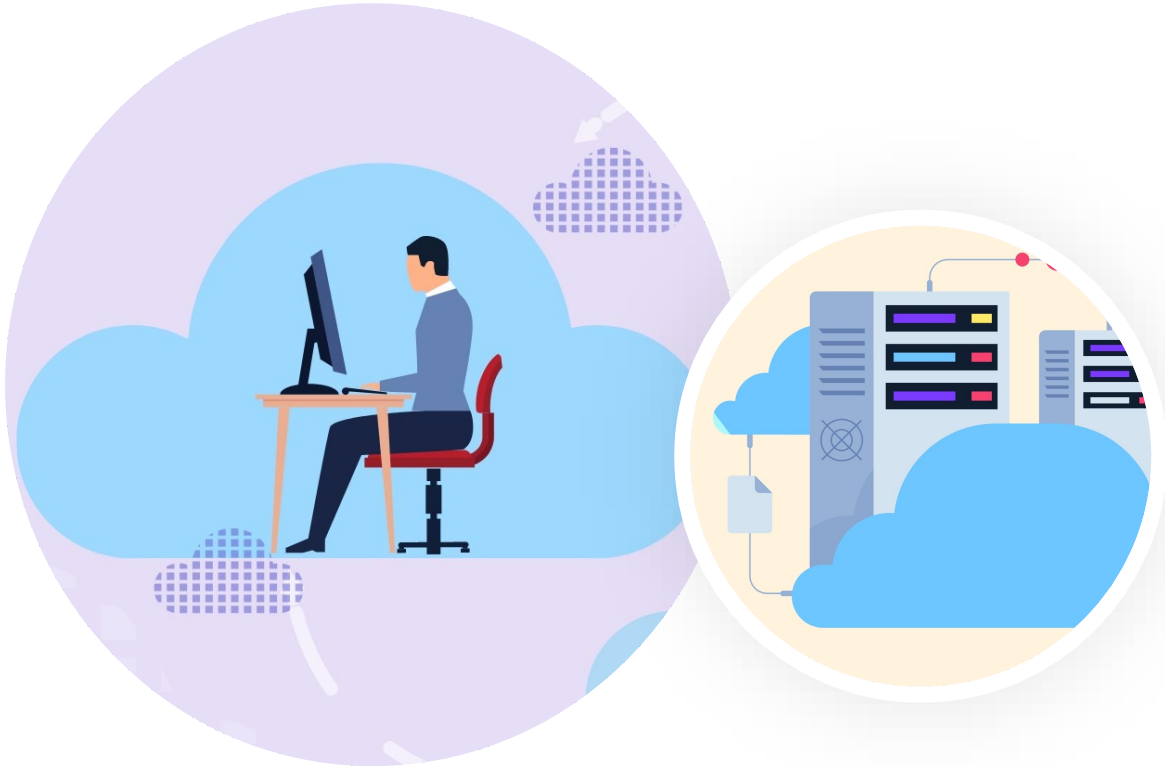
venminder

# Contracting *CONTINUED*



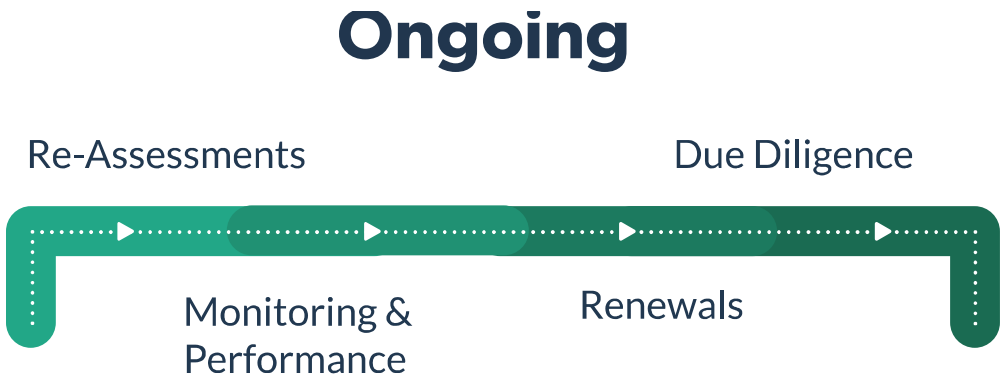

## CONTRACT MANAGEMENT ENTAILS:

- Having a process in place for internal planning, negotiating, creating/drafting, approving/executing, storing, and managing contracts
- Incorporating essential controls
- Creating service level agreements (SLAs)
- Managing key contractual dates



venminder

# Stage 2: Ongoing

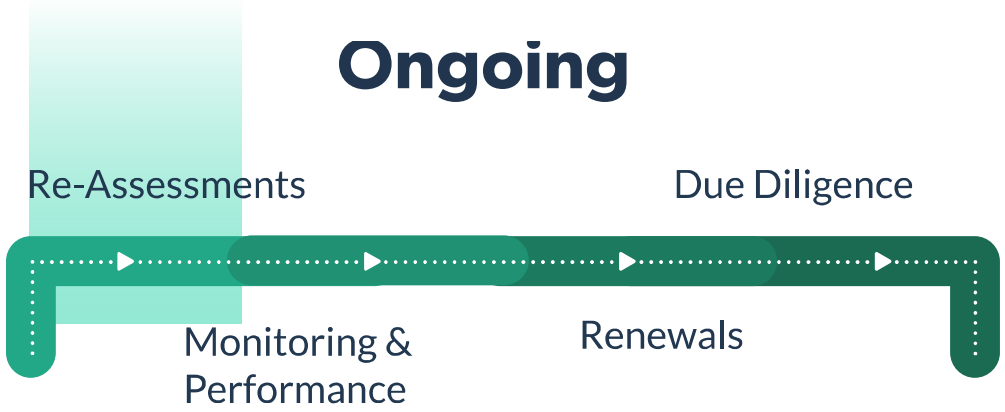



- Now that the planning & risk assessment, due diligence, and contract execution are complete, the ongoing stage begins
- After you sign the contract, ongoing monitoring of the vendor's risk and performance is extremely important

- This step allows you to remain aware of any new or emerging risks or performance issues
- Activities in this stage include re-assessments, monitoring, & performance, contract renewals, and due diligence

venminder

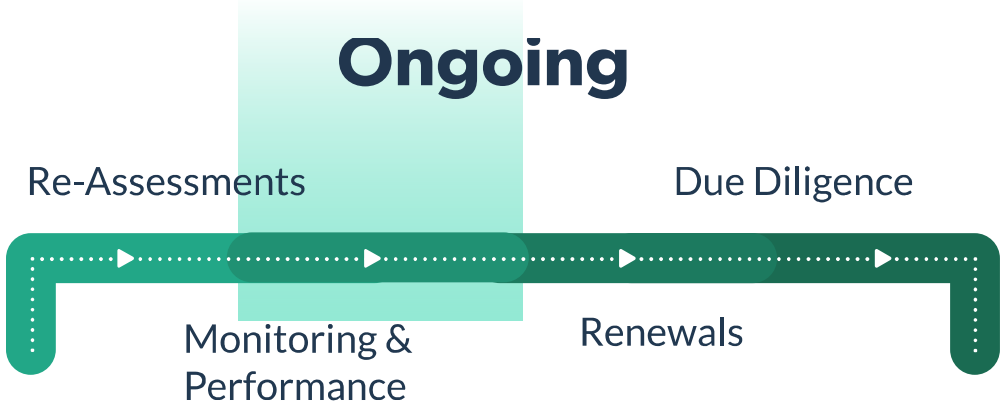
# Re-Assessments




- Start with your line of business or business owners confirm that nothing has changed with the relationship.
- This can be done by reviewing, and updating, if necessary, the inherent risk assessment.
- Once you've validated the inherent risk is the same, reach back out to the vendor to collect updated documents, assess the due diligence, and update your residual risk accordingly.
- A good standard is to re-assess critical and high-risk vendors at least annually, moderate-risk vendors every 18 months to two years, and low-risk vendors every two to three years.

venminder

# Monitoring & Performance




Ongoing monitoring of vendor risk and performance helps ensure that risk level and quality remain consistent throughout the relationship.

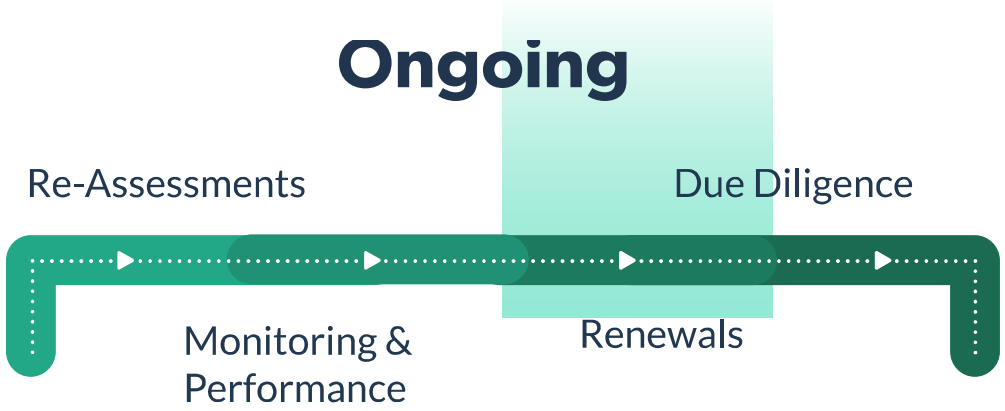
Monitoring should include the measure of performance of third parties in terms of profitability, benefit, and service delivery.

## THE KEY QUESTIONS BECOME:

- Are they living up to contractual obligations? (i.e., SLAs)
- Is the benefit of the vendor product or service worth the measured risks and cost?
- Has the cost/risk-to-benefit ratio changed enough to consider an exit?

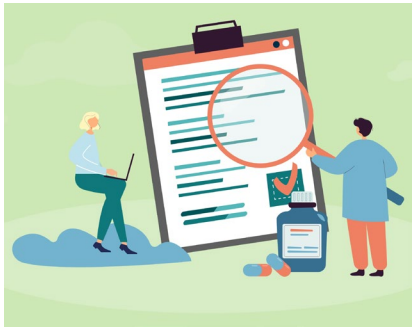
venminder

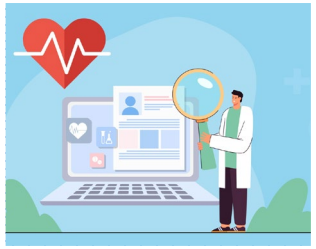
# Renewals




- Discussions should include service delivery, performance, meeting specific requirements, and addressing any service level gaps
- Don’t forget to track SLAs, enabling both parties to be accountable
- As a best practice, most regulators and auditors are looking to verify that your contract management process is well developed, organized, and maintained on an ongoing basis

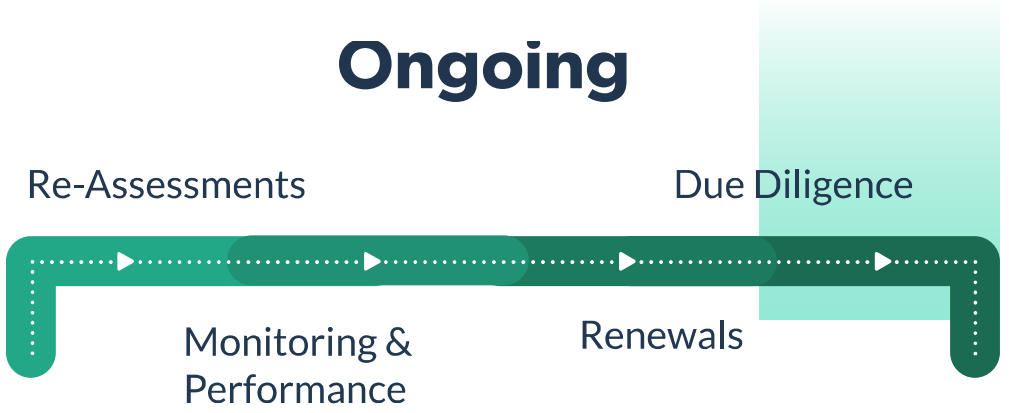
- Plan your contract renewals well in advance so you have sufficient time to negotiate any changes that may be needed
- Negotiations can be time-consuming, so it’s best not to wait to review the contract until just before the renewal period
- As part of ongoing contract management, you should be having a continuous and consistent dialogue with your vendor





venminder

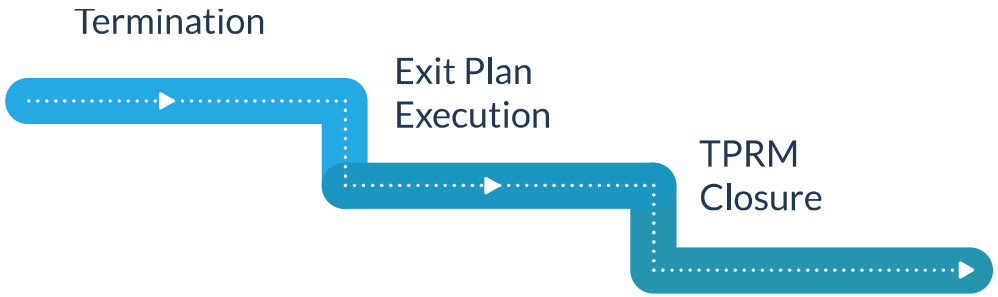
# Periodic Due Diligence




- Due diligence isn't meant to be a one-time activity done only at the beginning of a vendor relationship
- A vendor's risk as well as their underlying controls can evolve over time, so regularly collecting and reviewing due diligence is important
- Periodic due diligence reviews should be scheduled at least annually
- They can also be done before contract renewals, if there are performance issues or if there are new or updated regulatory requirements

venminder

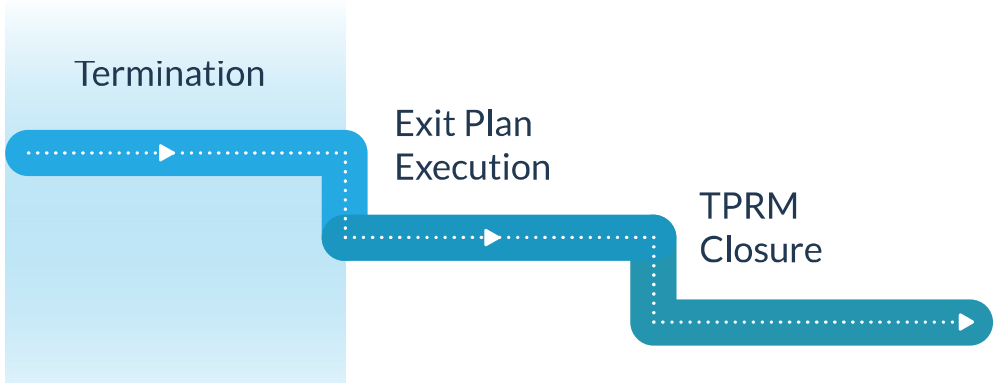
# Stage 3: Offboarding




- There comes a time when an engagement must come to an end, either proactively or reactively
- There should always be some consideration into how the termination processes may look for any particular vendor
- Once the contract term has ended, there isn't much to do besides closing the vendor out of your system and removing them from the vendor inventory
- You'll need to follow your exit strategy for more significant or critical vendors and make sure you're terminating the relationship per the contracted terms

venminder

# Termination




## Offboarding

This is the step in which you notify the vendor that the contract won't be renewed after it expires. Keep in mind that the vendor engagement won't be officially terminated until the date stated on the contract.

REASONS FOR EXITING A VENDOR RELATIONSHIP INCLUDE:

- Contract term is expiring
- A need to engage different or better resources
- Breach of contract
- Vendor is acquired
- Vendor business strategy is no longer compatible


venminder

# Exit Plan Execution

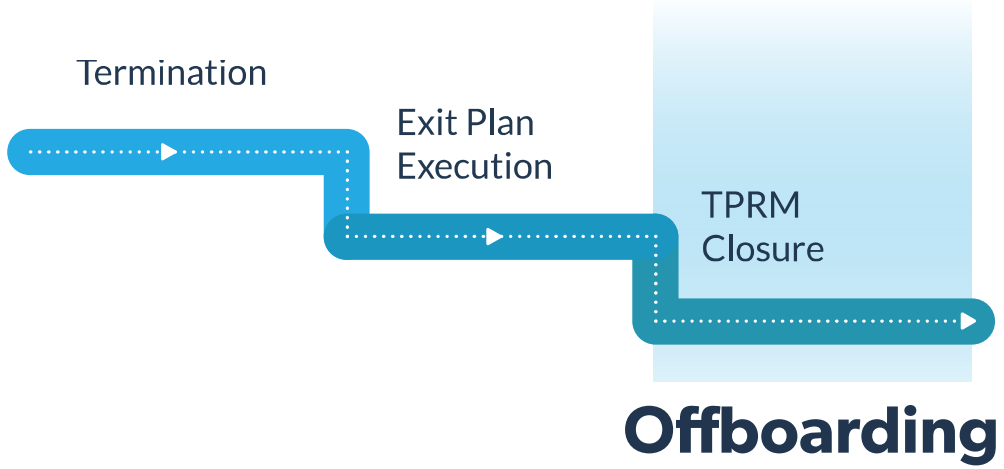

- Your exit plan should clearly define the duties and responsibilities of both parties when the contract ends
- The vendor must follow the proper return or destruction of sensitive data plan
- At the same time, your organization will perform its duties, which might include revoking all vendor access to your systems and facilities, transitioning to another vendor or bringing the activity in-house

**It's important to ensure that all vendor terminations and exits include the following:**

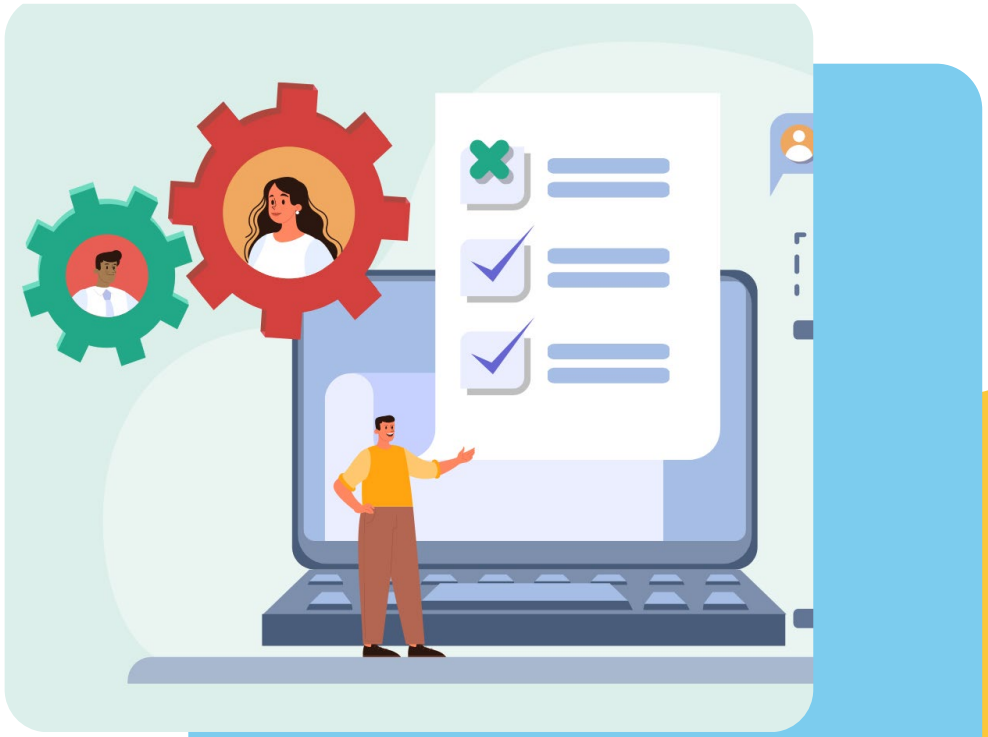
- A thorough review of the contract to understand required notice periods, rights of termination, any potential penalties, or liability as the result of the termination
- An exit strategy
- Requirements for return of assets, data, or destruction of data
- Required record keeping

venminder

# TPRM Closure




- Once the vendor exit plan is complete, you may still have a few final steps to close down the relationship formally
- This might include reviewing and paying any final invoices and working with accounts payable to prevent payment of any future invoices
- All relevant vendor information should be appropriately filed or archived should you need access to it later (perhaps for an audit)



venminder

# Does your organization currently follow the third-party risk management lifecycle?

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

# Key Takeaways

- ✓ **Oversight starts at the top.** The board and senior management must be engaged with TPRM.
- ✓ **Follow the third-party risk management lifecycle.**
- ✓ **Make sure roles and responsibilities are clear** and stakeholders know how to perform their roles.
- ✓ **Remember, critical is not a risk rating.** It's a way to identify the third parties who are most important to your operations.
- ✓ **Inherent risk is the naturally occurring risk** of a product or service, not taking any controls into consideration, and determines how third parties must be managed.

venminder

# Key Takeaways

*CONTINUED*

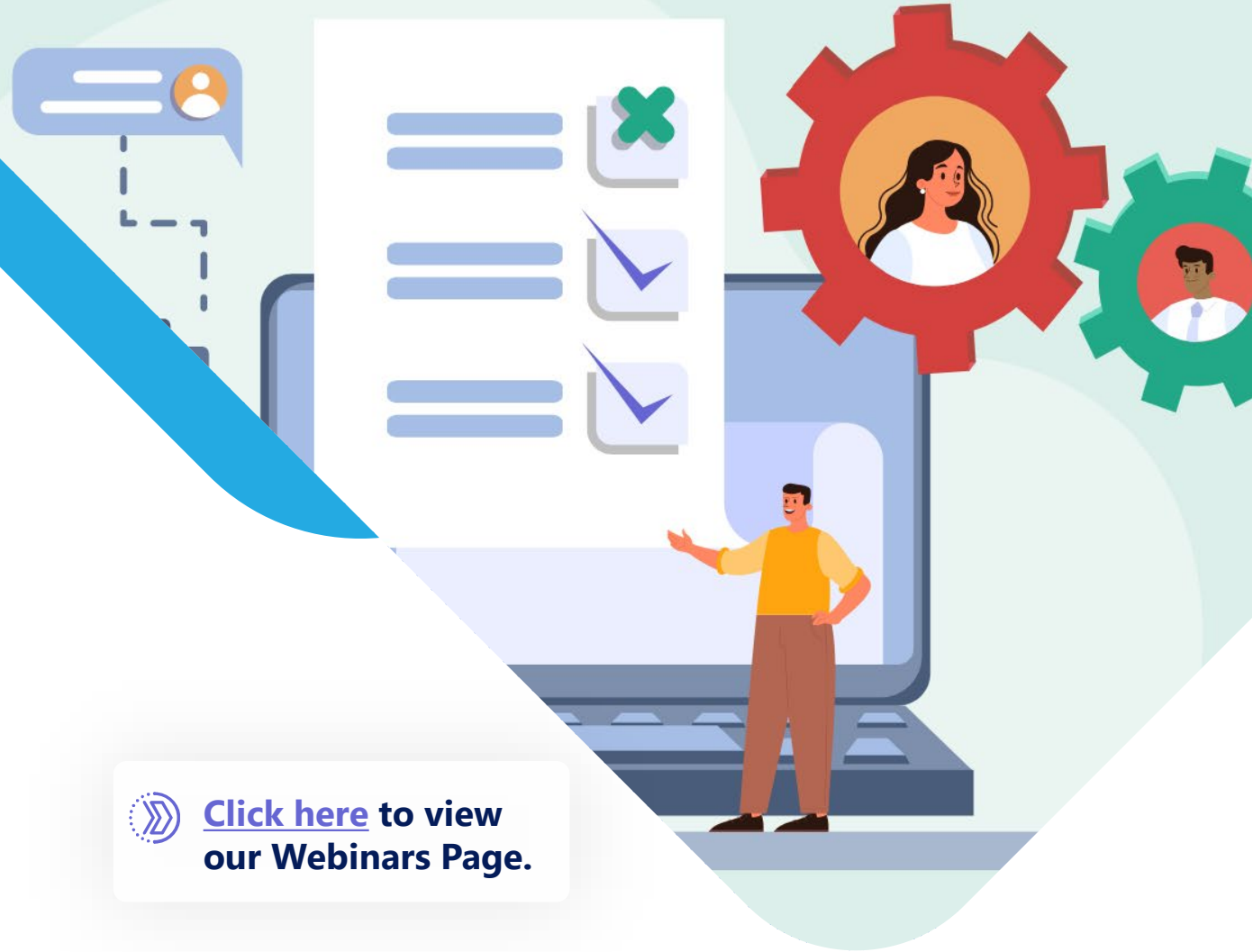
- ✓ **Residual risk is the remaining risk** after controls have been applied and is used to measure confidence in the controls (Important: It does NOT take the place of the inherent risk rating).
- ✓ **TPRM activities should be risk-based.** More risk = more intensive due diligence, enhanced contract terms and conditions, and frequent risk and performance monitoring.
- ✓ **Due diligence must be completed before contract execution.**
- ✓ **Risk re-assessments and due diligence should occur annually** for critical and high-risk vendors.
- ✓ **Risk and performance monitoring are essential** all the time.

venminder

# THANK YOU

ALSO JOIN US AT

# Our Upcoming Webinars:



**JANUARY 24, 2023**

Developing and Maintaining Effective Third-Party Risk Management Governance Documentation

**FEBRUARY 7, 2023**

State of Third-Party Risk Management 2023

**Click here to view our Webinars Page.**

venminder

# Questions & Answers

**POST A QUESTION:**
www.thirdpartythinktank.com

THIRD PARTY thinktank
A Community for Risk Professionals

**EMAIL US:**
resources@venminder.com

**FOLLOW US:**
@venminder

venminder