# 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

# Beyond the Basics: Strategies to Mature Your Vendor Risk Management Program

March 23, 2023


**PRESENTED BY**

**Hilary Jewhurst**

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


venminder

# Session Agenda

1. The attributes of a mature vendor risk management program
2. Steps and actions to drive program maturity
3. Correctly identifying the right issues for improvement and removing barriers
4. Using a program maturity roadmap
5. Measuring and reporting your success
6. Key takeaways

venminder

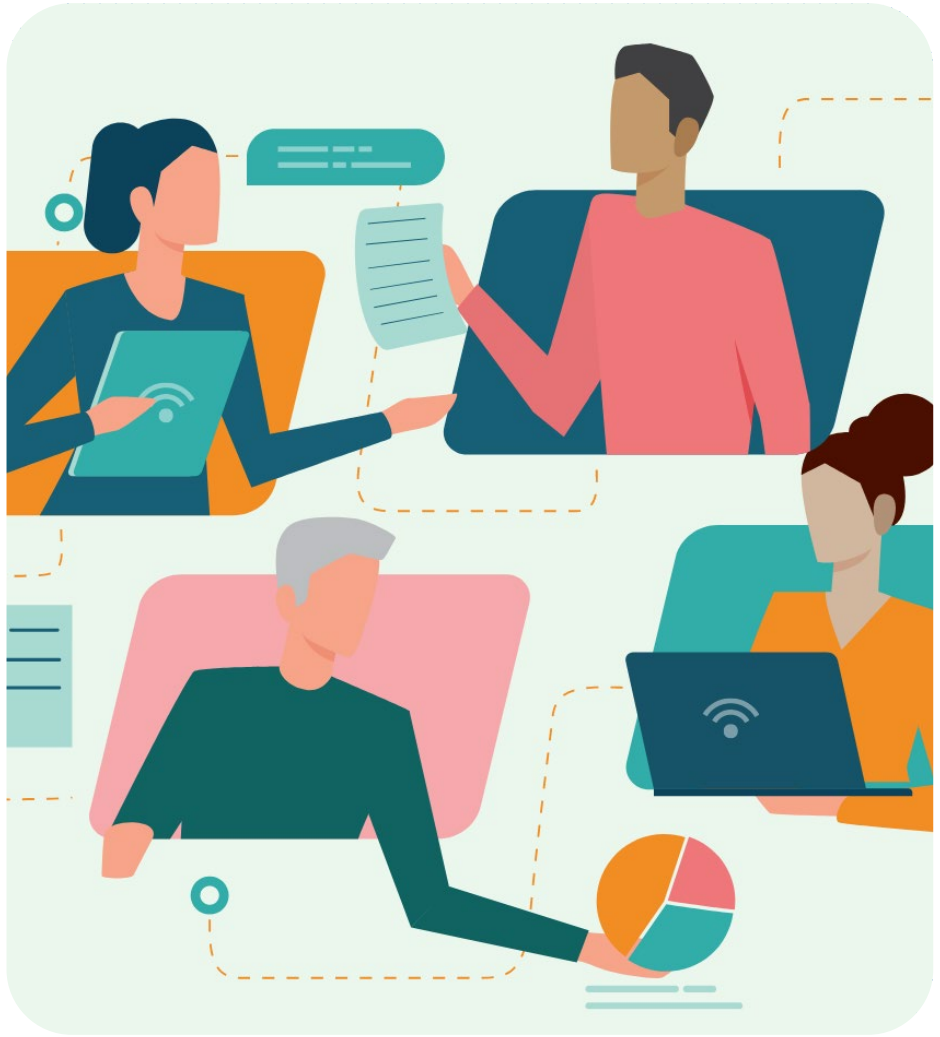
# What Is a “Mature” Vendor Risk/Third-Party Risk Management Program?

SO NOW THAT YOUR VENDOR RISK/THIRD-PARTY RISK MANAGEMENT (TPRM) PROGRAM IS IN PLACE, YOU MIGHT BE WONDERING HOW TO MAKE IT BETTER OR MORE “MATURE.”

**What makes a vendor risk management program “mature?”**

Research this topic online and you may find some interesting (if not aspirational) hallmarks of what a mature program looks like.

Let’s take a look…



venminder

# 8 Hallmarks of a Mature Program

1. The board isn't only aware, but is interested and engaged, too
2. Active engagement and oversight from senior management
3. TPRM is part of or has its own risk/governance committee
4. TPRM is fully integrated into corporate strategic planning and decision making
5. Established governance structure and documents
6. Trained professional staff in clearly-defined roles throughout the third-party risk management lifecycle
7. Integrated with other internal and external data sources to enhance insights
8. Established TPRM program metrics and reporting

venminder

# Why Worry About Program Maturity?

- Vendor risk/third-party risk is really extended enterprise risk, and outsourcing spending typically accounts for a significant portion of operational budgets
- Outsourcing is utilized to address issues or realize opportunities
- Vendor risk/third-party risk management programs should deliver value beyond regulatory compliance
- The vendor risk/third-party risk landscape constantly changes, and emerging threats are business as usual
- Regulatory changes and updates often result in more stringent requirements

venminder

# Vendor Risk/Third-Party Risk Management Program Maturity Considerations

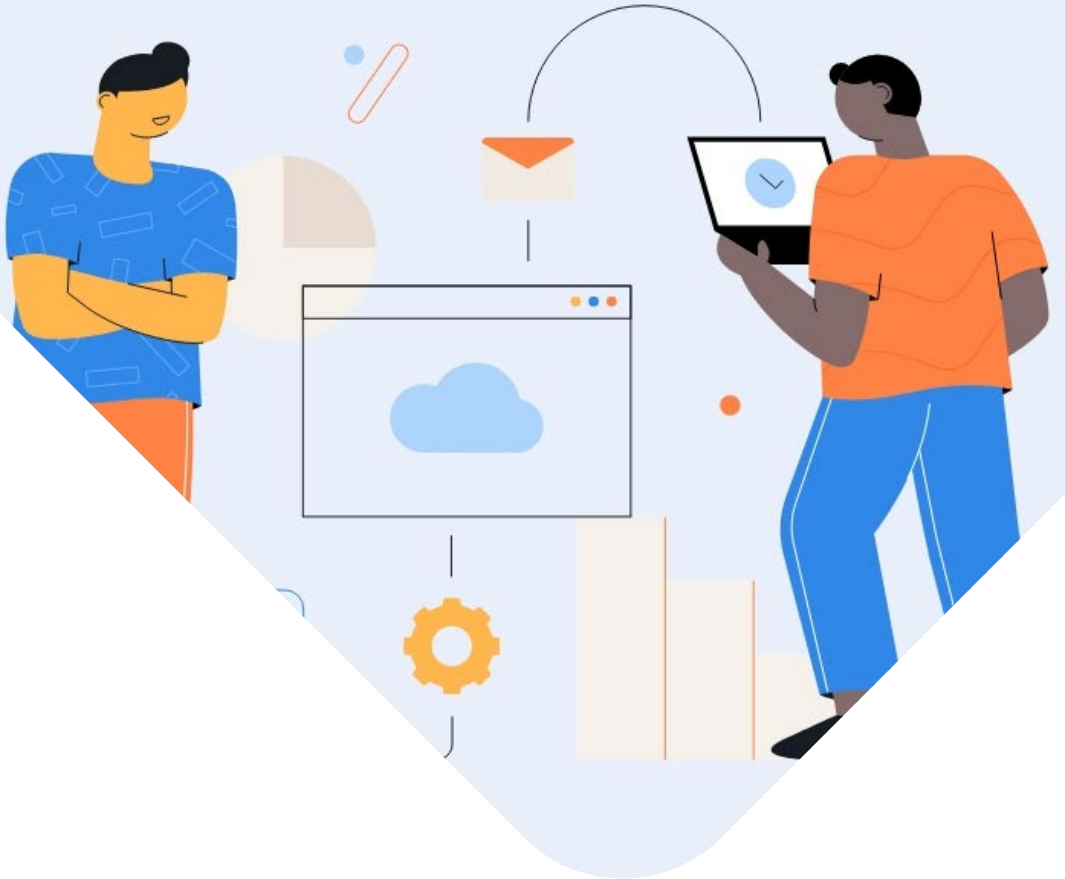
ALL VENDOR RISK/THIRD-PARTY RISK MANAGEMENT PROGRAMS AREN'T CREATED EQUAL, NOR SHOULD THEY BE.

**There are many variables to consider when determining what makes a program "mature":**

- Size of the organization
- Regulated industry
- Direct to consumer products and services
- Number of vendors utilized
- Products and services provided by the vendors
- Organizational risk appetite and culture
- Support of and collaboration with other functional teams such as InfoSec, Compliance, Sourcing, Legal, etc.

venminder

# Benefits of Continuous Improvement



- More objectivity regarding what is working and what isn't
- More flexibility to address new or emerging risks and regulatory changes
- Prioritizes risk management over "this is how we do it"
- Increases effectiveness and efficiencies

**No vendor risk/third-party risk management program is perfect. Strive for progress, not perfection.**

venminder

# Vendor Risk/Third-Party Risk Management Program Maturity Levels

| Initial | Developing | Implemented | Managed | Optimizing |
|---|---|---|---|---|
| ▪ Ad-hoc or nonrepeatable processes<br>▪ Processes aren't sufficiently defined and documented and aren't easily replicated<br>▪ No organizational awareness<br>▪ Roles and responsibilities aren't defined or inconsistent<br>▪ Minimal involvement from senior management | ▪ Foundational processes developed, but untested<br>▪ Rules and requirements are defined<br>▪ Low organizational awareness<br>▪ Some formal documentation<br>▪ Roles and responsibilities are emerging<br>▪ Some senior level sponsorship | ▪ Processes defined and are repeatable<br>▪ Rules and requirements are established<br>▪ Governance structure established<br>▪ Increasing organizational awareness<br>▪ Formal documentation<br>▪ Roles and responsibilities are defined<br>▪ Senior management ownership and accountability | ▪ Documented processes and procedures<br>▪ Engagement and oversight from senior management<br>▪ Strong organizational awareness<br>▪ Formal governance routines<br>▪ Stakeholders held accountable<br>▪ Program metrics defined and reported<br>▪ Compliance with regulatory requirements and best practices<br>▪ Strong process discipline | ▪ Processes evaluated for effectiveness and efficiency<br>▪ Process automation<br>▪ Vendor risk incorporated into corporate strategy<br>▪ Multi-source data integration<br>▪ Improvement strategies are documented, and progress is reported<br>▪ Review assessment and incorporation of new data sources and technology to support risk identification and management |

venminder

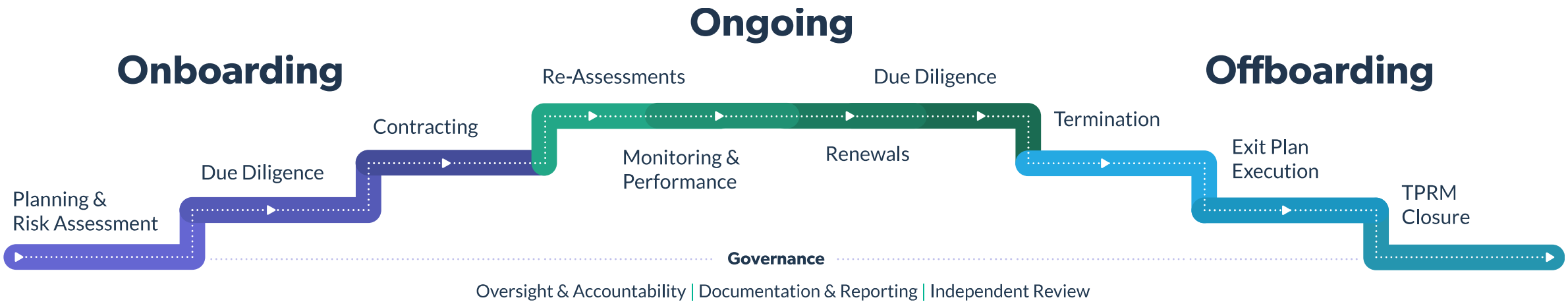
# Vendor Risk/Third-Party Risk Management Program Fundamentals

YOU MUST HAVE THE BASICS IN PLACE BEFORE YOU CAN TACKLE PROGRAM MATURITY:

- Support from senior leadership
- Governance documentation, such as a vendor risk management policy
- A complete vendor inventory
- Methodology to risk rate vendors
- Methodology to identify critical vendors
- Processes that are aligned to the third-party risk management lifecycle
- Defined roles and responsibilities
- Participation from the vendor owners (first line, business line)
- If in a regulated industry, know your regulator(s) and their requirements

venminder

# The Third-Party Risk Management Lifecycle



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

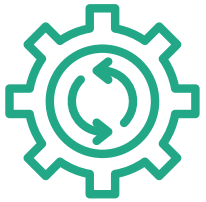
a. Yes, from end to end
b. Somewhat – not all stages and activities are included
c. No
d. Not sure

# Vendor Risk/Third-Party Risk Management Components

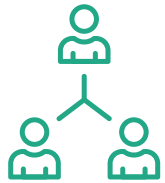
**TPRM Framework**

**Governance Documents**

**Processes**



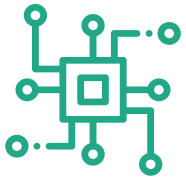
**Governance**



**People**

**Risk Appetite**

**Tools and Technology**



**Reporting**

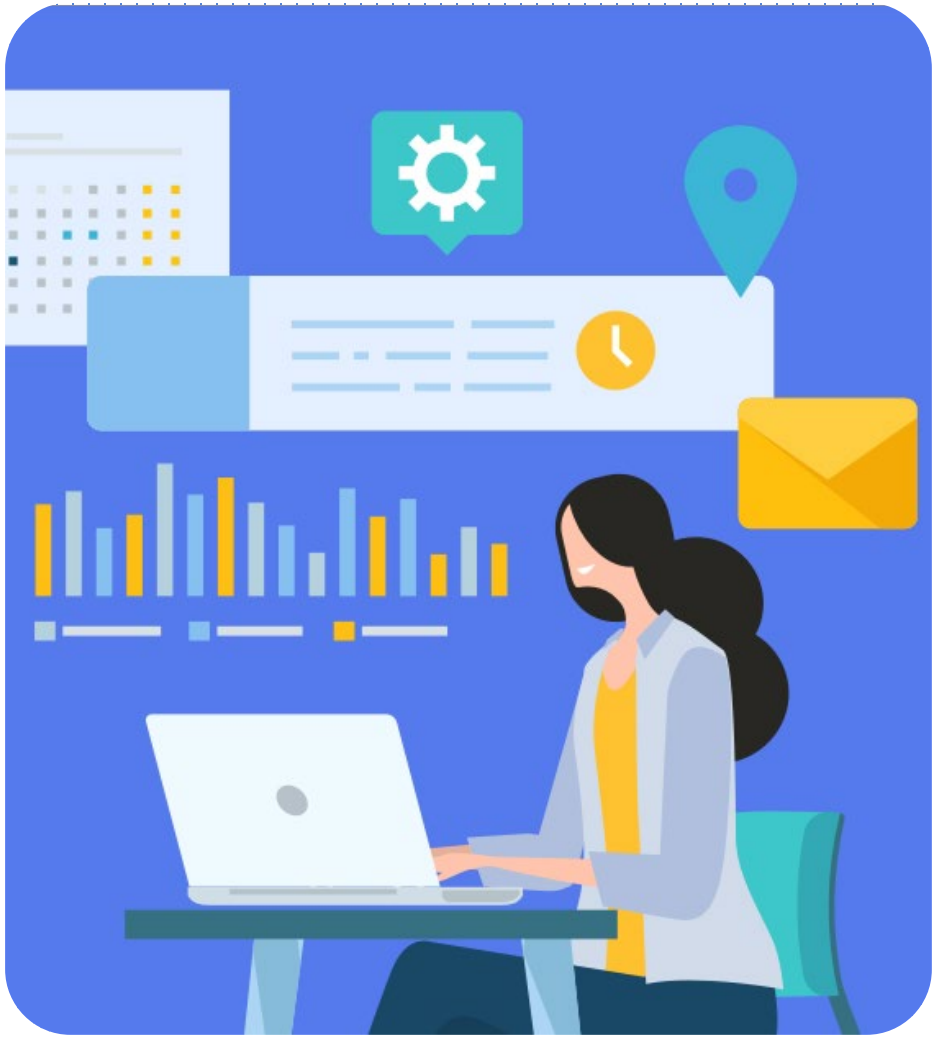
venminder

# TPRM Framework

Your framework is the all-encompassing collection of requirements, rules, tools, and processes that make vendor risk management possible at your organization.

**Attributes of Mature Frameworks:**

- Defined rules and requirements that are memorialized in governance documents
- Clear roles and responsibilities
- Documented and tested processes
- Established oversight and governance
- Defined risk appetite and tolerance levels
- Effective tools and technology
- Comprehensive reporting



venminder

# Governance Documents

Governance documentation consists of your Policy, Program, and Procedures. Governance documentation formalizes your rules and requirements (Policy), processes (Program), and procedures. While **policies are generally the only governance documents required by regulators**, mature programs also include detailed program processes and stakeholder-specific procedures.

Maturity is NOT based on having the most or longest documents.

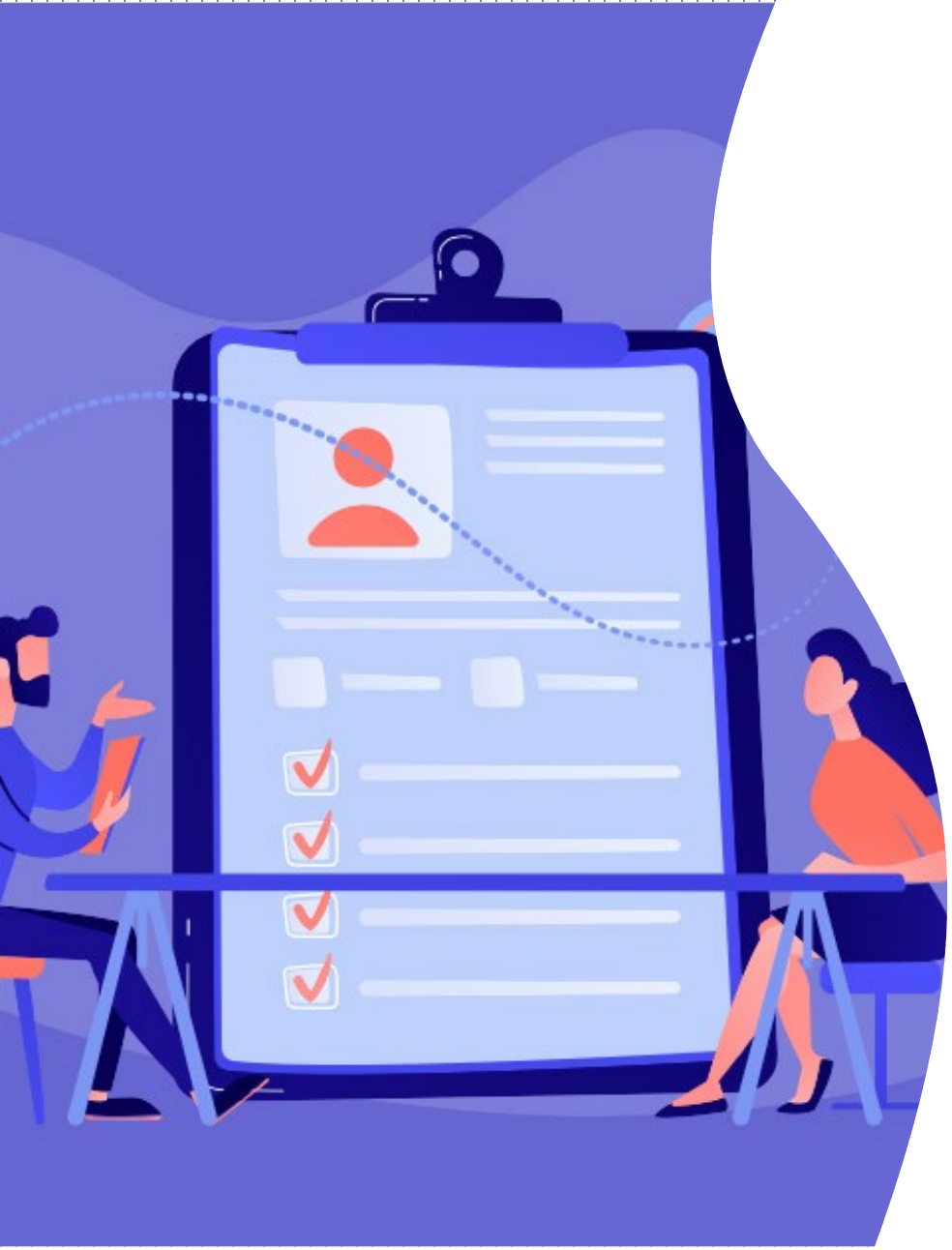
venminder

# Governance Documents

## ATTRIBUTES OF MATURE GOVERNANCE DOCUMENTS:

- Having practical requirements, guidelines, and instructions which align with **actual** practices
- Reflect regulatory requirements and best practices
- Are reviewed and approved by the appropriate level of management
- Documents that are accessible to all that can benefit from them

venminder



# Processes

Documented and tested processes are essential. Your processes should closely mirror activities and order of the third-party risk management lifecycle.

**Mature processes have the following attributes:**

- Direct relationship to policy rules and requirements
- Clear objectives and desired outcomes
- Documented workflows, roles, and responsibilities
- Identified inputs, outputs, decisions, or approvals
- Periodic testing to ensure the process works as intended

venminder

# Governance

Governance can be defined as: “The system by which entities are directed and controlled.” From a vendor risk/third-party risk management perspective, governance is essential for a successful program.

**Mature programs have the following governance attributes:**

- Policy approval at the highest level of the organization (Board or C-level)
- Visibility and reporting to the board (if you have one)
- Strong and consistent involvement from senior leadership
- Executive ownership at the enterprise level
- A defined escalation path for issue management and resolution
- Regular internal audits
- Vendor risk/third-party risk management program metrics
- Third-party risk management is member of risk governance committee

venminder

# People

The people element refers to all individuals, stakeholders, and teams that have a role in vendor risk management.

**Mature programs have the following people attributes:**

- Clearly defined roles and responsibilities
- Firm commitment and timely action from the vendor owners (first line or business line)
- Training and education for vendor owners and other stakeholders
- Feedback mechanism for stakeholders
- Performance metrics related to their vendor risk management duties
- Experienced and dedicated third-party risk manager, involvement in risk or governance committee
- Collaboration expected for problem-solving

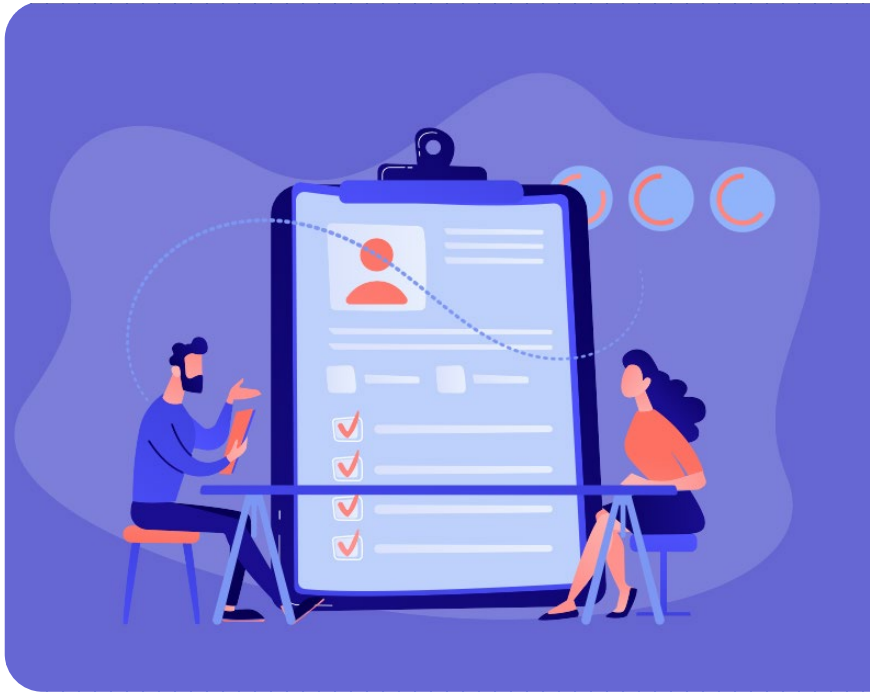
venminder

# Organizational Risk Appetite

Organizational risk appetite refers to how risk is considered both in the context of vendor risk management and enterprise risk.

**Mature programs have the following risk appetite attributes:**

- Defined risk management structure for the enterprise
- Documented risk thresholds and approval levels
- Risks taken align with strategic objectives and long-term goals
- Established risk committee
- Awareness and ownership of vendor risks
- Proactive risk consideration and identification by all stakeholders
- Credible review and challenge
- Compliance with the policy is the expected business norm



venminder

# Tools

Your tools include risk assessments and methodology for establishing risk ratings, standardized due diligence document requests, SME reviews, standard contract terms and conditions, issue management and escalation, and communications.

venminder

# Tools

## Attributes of mature tools:

- Inherent risk assessments are reviewed at least annually and updated when necessary to address new and emerging risks
- The methodology for risk ratings is documented and tested
- Criteria for critical vendors are documented
- Due diligence document requests are standardized by risk domain
- Vendor risk questionnaires are developed in collaboration with SMEs, reviewed periodically, and updated when necessary
- Subject matter experts with professional credentials perform vendor risk reviews
- Contracts for critical or high-risk vendors contain standardized terms and conditions - exceptions are tracked and monitored
- Issue management and escalations processes are documented, and issues are reported and tracked
- Communication channels are defined
- Changes follow an established change management process

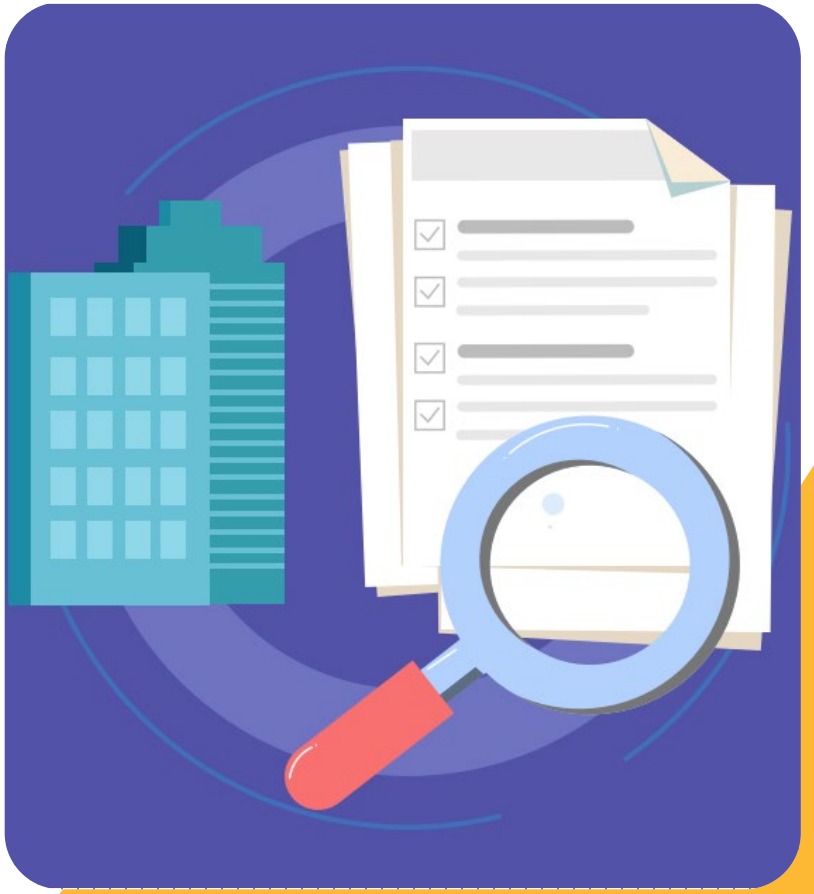
# Technology

Moving away from manual tools and processes can definitely drive program maturity. Manual processes are time-consuming, error-prone, and require additional administrative effort to remain current.

Software specifically designed to address vendor risk management enhances your organization's ability to manage the many interdependent processes and stakeholders involved.

Software as a Service (SaaS) vendor risk/third-party risk management solutions should entail the following to drive and support program maturity.

- Easy configuration
- Regular upgrades
- Document management, organization, and storage
- Workflow management
- Automated reporting
- Stakeholder communication tools
- Ability to connect to other data sources via API



venminder

# Reporting

Comprehensive reporting is paramount to program maturity. Reports should be used to provide information, drive action, and confirm compliance. Reporting should always be configurable, and standard automated reports must be available for stakeholders.

venminder

# Reporting

**Mature programs generate the following reporting:**

- Board and senior management reports
- TPRM metrics with progress against goals and objectives
- Critical vendors report
- Risk Committee reporting
- Issues management and tracking
- Personal Identifiable Information (PII) type report by vendor
- Vendor profile, status, issues, and actions
- Vendor due diligence and risk review status
- Scheduled action reports (risk re-assessments, vendor risk reviews, vendor owner training, policy review, etc.)
- Vendor performance management reports
- Inherent vs residual risk report
- Portfolio risk report
- Internal compliance at the enterprise, business unit, and vendor owner levels

## Which of these vendor risk/third-party risk program elements has been your biggest challenge?

a. Support from senior leadership and the board
b. Consistent participation and compliance from the line of business
c. Managing workload
d. Two or more of the above
e. None of the above
f. Not sure

# Considering Challenges and Barriers

- What is not working in your program?
- What are your most frequent challenges?
- If you could adjust or change a single element of your program, what would it be, and why?

venminder

# Identifying Root Causes –
## The Situation

**Situation:** Clara, a third-party risk manager, is having trouble getting the vendor owners to follow the TPRM processes.

**She thinks:** The first-line vendor owners don't care about vendor risk management. They don't follow the process and complain about the 'extra work' they must do before they can do something 'as simple as onboarding a vendor.'

**Her conclusion:** "This is wearing me out and causing delays and rework. I think this is a governance problem. I'm not in a position to push the issue. I'll talk to the manager, and they can enforce the policy."

venminder

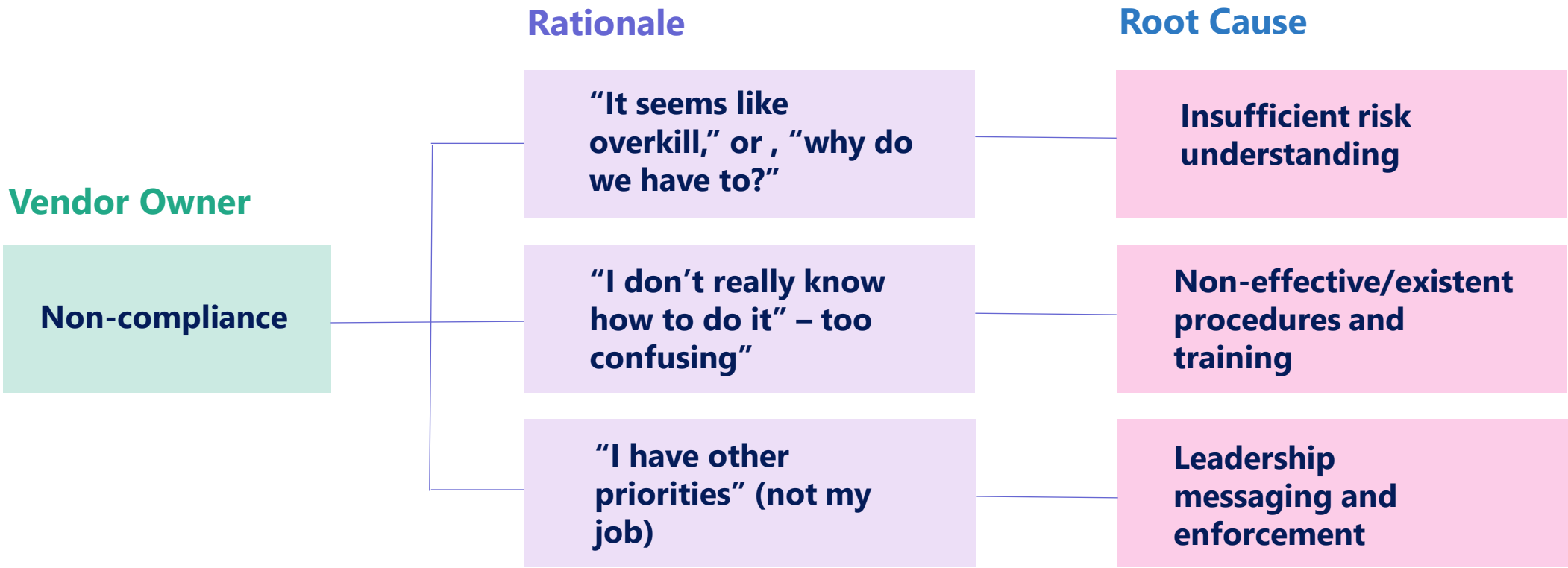
# Identifying Root Causes – The Outcome

The conversation did not go as she had planned.

The senior manager let her know that before he would enforce the policy, he must **identify the root cause(s) of non-compliance first.**

venminder

# Non-Compliance Rationale and Root Causes



# Non-Compliance Rationale and Root Causes

## Non-compliance

| Root Causes | | |
|---|---|---|
| Insufficient risk understanding | Procedures and training | Leadership messaging and enforcement |
| **Potential Solutions** | | |
| ▪ Risk Training and Risk Messaging | ▪ Training<br>▪ Well-Written Procedures | ▪ Risk Messaging (Tone-from-the-top)<br>▪ Program Guide<br>▪ Quarterly Check-In<br>▪ Metrics and Reporting |

# Ease of Program Change or Improvement

Concentrate your efforts where you have the most ownership.

## Owner

Full ownership of governance documents, processes, procedures, and framework

**Policy**
- TPRM Policy

**Program**
- Program
- Reporting

**Processes**
- Procedures
- Training

## Influencer

TPRM is a stakeholder, but does not have full ownership

**Governance**
- Other related policies
- Reporting
- Metrics

**People**
- Performance KPIs
- Procedures
- Reporting

**Risk Appetite**
- Organizational risk, threshold, and tolerance

## Collaborator

TPRM will collaborate with other stakeholders

**Tools and Technology**
- Metrics
- Reporting
- Notifications

**Reporting**
- Compliance
- Progress
- Issues

venminder

# Why You Need a Maturity Roadmap

- A maturity roadmap is a holistic plan to move your program from where you are to where you want to be
- Shows your current state and desired state and the gaps in between
- Identifies and consider internal or external dependencies that could affect your efforts
- Arranges your efforts in a step-wise and incremental plan
- Communicates the decisions, projects, or work required to improve program maturity
- Establishes timing necessary for change
- Provides the “big picture” for stakeholders

venminder

# Vendor Risk/Third-Party Risk Management Program Maturity Levels

| Initial | Developing | Implemented | Managed | Optimizing |
|---|---|---|---|---|
| ▪ Ad-hoc or nonrepeatable processes<br>▪ Processes aren't sufficiently defined and documented and aren't easily replicated<br>▪ No organizational awareness<br>▪ Roles and responsibilities aren't defined or inconsistent<br>▪ Minimal involvement from senior management | ▪ Foundational processes developed, but untested<br>▪ Rules and requirements are defined<br>▪ Low organizational awareness<br>▪ Some formal documentation<br>▪ Roles and responsibilities are emerging<br>▪ Some senior level sponsorship | ▪ Processes defined and are repeatable<br>▪ Rules and requirements are established<br>▪ Governance structure established<br>▪ Increasing organizational awareness<br>▪ Formal documentation<br>▪ Roles and responsibilities are defined<br>▪ Senior management ownership and accountability | ▪ Documented processes and procedures<br>▪ Engagement and oversight from senior management<br>▪ Strong organizational awareness<br>▪ Formal governance routines<br>▪ Stakeholders held accountable<br>▪ Program metrics defined and reported<br>▪ Compliance with regulatory requirements and best practices<br>▪ Strong process discipline | ▪ Processes evaluated for effectiveness and efficiency<br>▪ Process automation<br>▪ Vendor risk incorporated into corporate strategy<br>▪ Multi-source data integration<br>▪ Improvement strategies are documented, and progress is reported<br>▪ Review assessment and incorporation of new data sources and technology to support risk identification and management |

venminder

# Sample Maturity Roadmap

| | Q1 23 | Q2 23 | Q3 23 | Q4 23 | Q1 24 | Q2 24 |
|---|---|---|---|---|---|---|
| **Framework** | • Policy review and update<br>• Annual third-party inventory review | • Policy approval<br>• Establish exit plans for all critical vendors | • Establish QA review procedure, sample size, and standards | • Preparation for annual policy and procedure updates | • Policy review and update<br>• Annual third-party inventory review | |
| **Governance** | • Program Document Draft review – Vendor Risk Management Committee | • Implementation of new Program document | • Annual audit | • Preparation of Board TPRM Board program review<br>• Program metrics development | | |
| **People** | • Review vendor owner lists, confirm with Business Lines | | • Establish Enterprise Vendor Manager Roles | | • Role-based TPRM training for stakeholders | |
| **Processes** | | • Define process to address resellers/fourth parties | • Implement new monitoring requirements for critical and high risk | | • Define what reoccurring risk activities are required for moderate and low risk | |
| **Reporting** | • Vendor inventory report | • Upgrade monitoring reports | • Implement new critical fourth-party reports | | • Implement program level reports | |
| **Tools and technology** | • Identify SaaS VRM Solution | • System implementation and testing<br>• System training by role | Develop reporting Implement vendor spend data | Explore API capabilities between TPRM and Accounts Payable | VRM system/Jira integration | • Integrate TPRM reporting into Tableau |

venminder

Initial | Developing | Implemented | Managed | Optimizing

# Reporting Your Progress and Success

Implementing, maintaining, and managing your program requires hard work, but the work doesn't end once the program is implemented if constant improvement and program maturity is the goal.

Reporting your program and maturity objectives is important to drive awareness and garner support, but don't forget to report on your progress and success too. Keep in mind the following:

- Provide a full review of the program, roadmap, metrics, and other key data for the board and senior management at least once a year
- Provide a progress report for your roadmap at least twice a year
- Develop and implement program metrics and report on them quarterly
- Provide reporting for stakeholders engaged in program improvement efforts – don't forget to acknowledge efforts and say thank you

venminder

# Reporting Audience, Frequency, and Content

## MONTHLY

### Risk/Compliance Department

**Information and action**

- Upcoming communications
- Actionable now
- Needs intervention
- Need to know
- Deliverables due
- New vendors
- Terminated vendors

## QUARTERLY

### Risk/Compliance Committee

**Information, action, and planning**

- Dashboard and narrative with details
- Progress against goals and objectives
- Issues
- Emerging risks
- Internal compliance
- Upcoming deliverables
- Emerging risks
- Regulatory changes
- Process changes

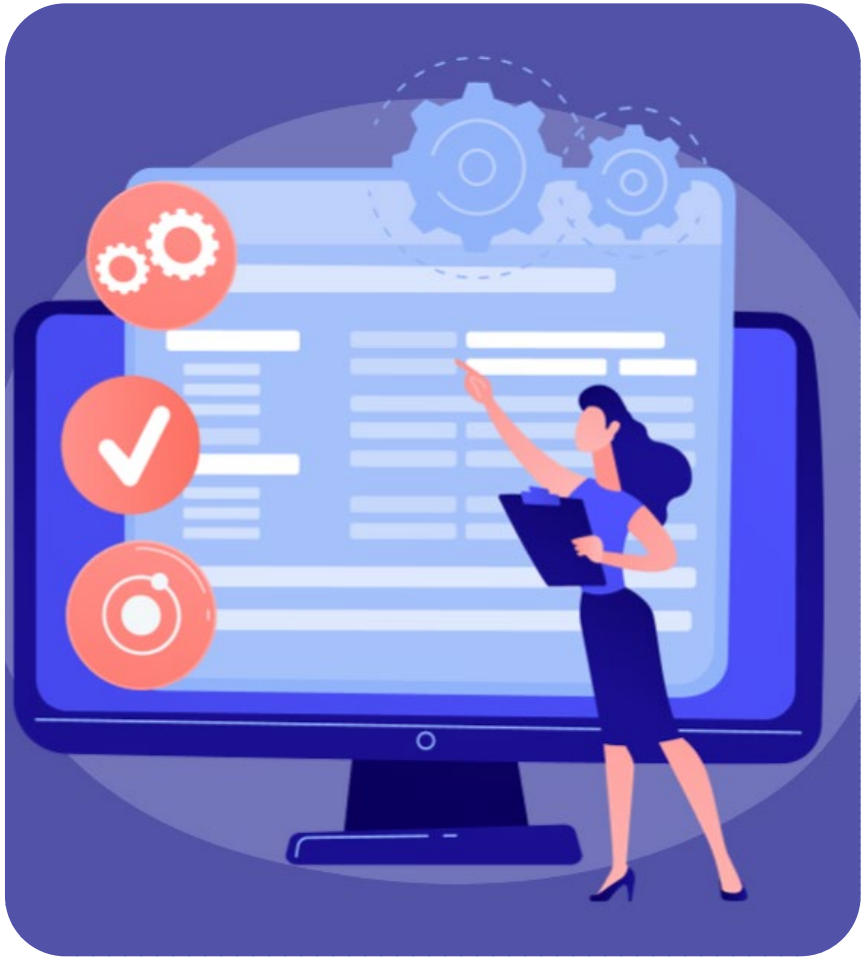
## ANNUALLY

### Full State of the Program Report (for the Board)

- Program metrics and progress
- Internal compliance
- Program highlights
- Program roadmap
- Policy updates
- Focus on critical and significant high-risk vendors
- Critical inventory with product
- Open issues or concerns
- New or terminated critical vendors
- Regulatory changes
- Internal compliance

# Steps to Take to Mature Your Program

- Review your program fundamentals against the third-party risk management lifecycle, regulatory requirements, and best practices
- Identify gaps or weaknesses and document them
- Determine where you have ownership, influence, or the need to collaborate
- Consider dependencies, order of improvement, resources, and reasonable time frames for action
- Establish priorities (regulatory compliance, ineffective processes, inefficient processes)
- Investigate root causes
- Identify specific actions or projects, roles and responsibilities, go or no-go decisions, or approvals
- Outline improvements on your program maturity roadmap



venminder

**Overall, our vendor risk/third-party risk management program maturity level is:**

a. Initial stage
b. Developing stage
c. Implemented stage
d. Managed stage
e. Optimizing stage
f. Not Sure

# Program Maturity Derailers

1. Building your program to standards that don't apply to your industry or organization
2. Building your program without understanding and consideration of regulatory guidelines
3. Policies that are unclear, unenforceable, or do not reflect the current state and practices
4. Using procedures that are unclear or poorly written
5. Expecting adherence to complex procedures without education or training
6. Lack of defined roles and responsibilities
7. No improvement or updates to aging policies or processes
8. No feedback from program users
9. No integration with other risk functions, teams, or committees
10. Not enough, too much, or not the right data used in reporting

venminder

# Key Takeaways to Mature Your Vendor Risk/Third-Party Risk Management Program

1. Focus on the fundamentals first
2. Build and mature your program to align with what your organization needs and will accept culturally
3. Focus on continuous improvement vs optimization
4. Explore issues and challenges by identifying root causes
5. Keep actions doable
6. Keep processes simple
7. Keep rules enforceable
8. Leverage your ownership to drive influence and support collaboration
9. Use reporting to drive influence, support problem solving, and validate program necessities
10. Stay informed from a regulatory perspective

venminder

venminder

# THANK YOU

ALSO JOIN US AT

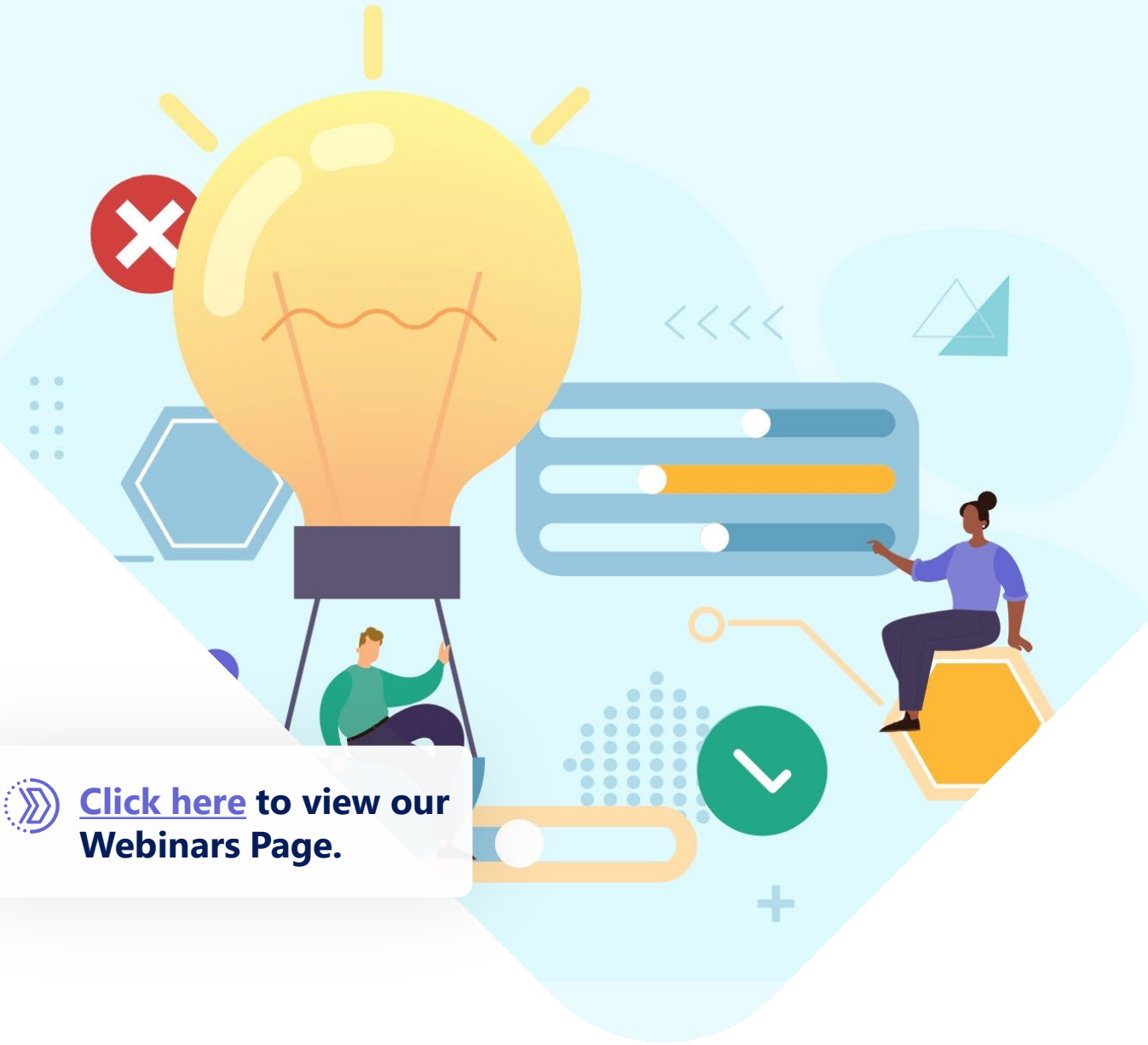
# Our Upcoming Webinars:

MARCH 30, 2023

**Vendor Financial Red Flags Your Credit Union Should Watch For**

APRIL 4, 2023

**Fourth-Party Risk: What to Know and How to Manage It**



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

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