Third/Fourth-Party Risk Management; How to Conduct an Effective Audit

PRESENTED BY
Gordon Rudd

Third-Party Risk Officer
Venminder
gordon.rudd@venminder.com

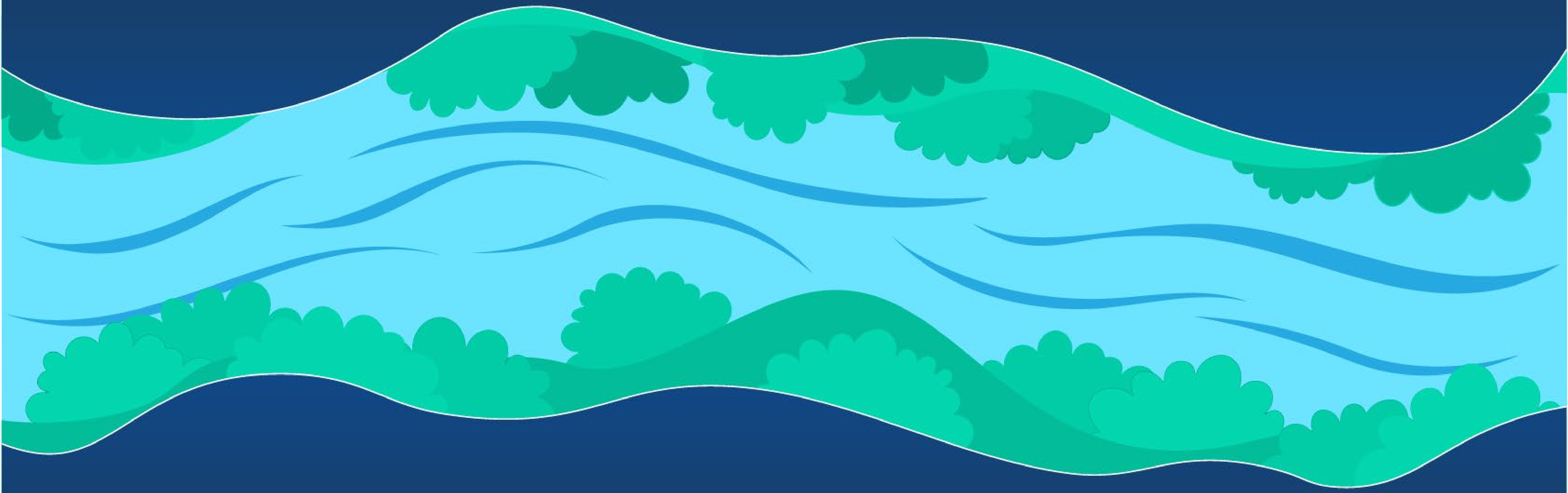
October 8, 2020

Session Agenda

1. Levels of Third-Party Risk Management Success
2. The Third-Party Risk Management Lifecycle
3. Frameworks vs. Regulatory Requirements
4. How to Conduct an Audit
5. Best Practices

venminder

We see the river...



without seeing a single drop of water.

Poll Question

How mature would you rate your third-party risk management program?

a. Very mature
b. Mature
c. Just getting started
d. Not sure

venminder

Levels of Third-Party Risk Management Success

Level 1

Ad hoc or no TPRM process

- Little structure
- Employees working diligently, but with an inefficient TPRM process
- Little or no formal planning for process changes
- Does not follow TPRM lifecycle

Level 2

Managed but isolated TPRM tasks & projects

- Requirements identified and documented
- Project planning, monitoring & controls
- Manages vendor/supplier agreements
- Measures and analyzes data
- Does process & product quality assurance
- Configuration and process changes are applied in isolated projects
- Follows parts of the TPRM lifecycle

Level 3

Defined TPRM processes & multiple task & project capabilities

- Requirements are defined and refined through governance documents
- Processes are priority, defined and continually improved
- Utilizes technical solutions
- Tools are integrated into processes
- Verification & testing of assumptions
- Organizational training plans are operational
- Universal project management
- Actively manages vendor risk
- Follows the full TPRM lifecycle

Level 4

Quantitatively managing TPRM to organizational standards

- Everything is measured, monitored and reported on periodically to teams, senior management and the board
- Decisions based on quantitative analytics
- TPRM organization-wide standards and methods are broadly deployed for managing and leading change
- Analyzes organizational TPRM process performance

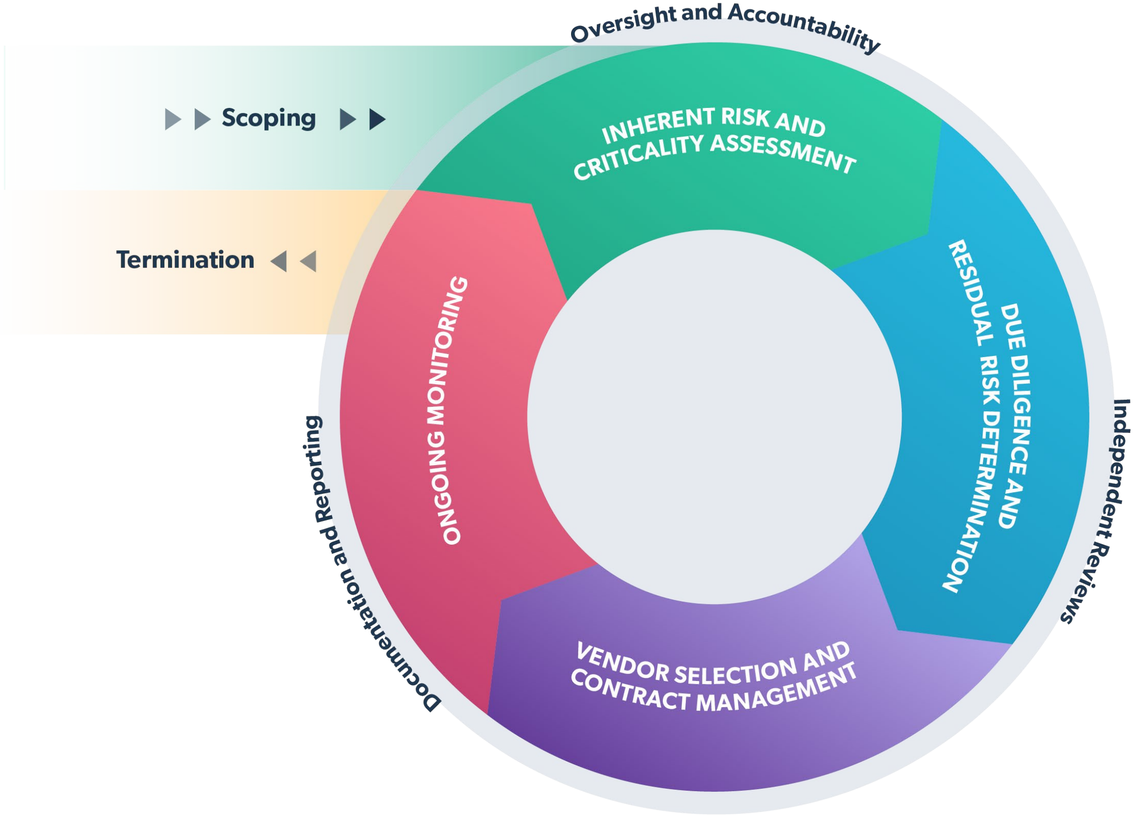
Level 5

Continuous process improvement fully operational

- TPRM innovation and deployment
- Causal analysis and resolution to evaluate what's working and improve what's not
- TPRM is an organizational competency

venminder

The Third-Party Risk Management Lifecycle

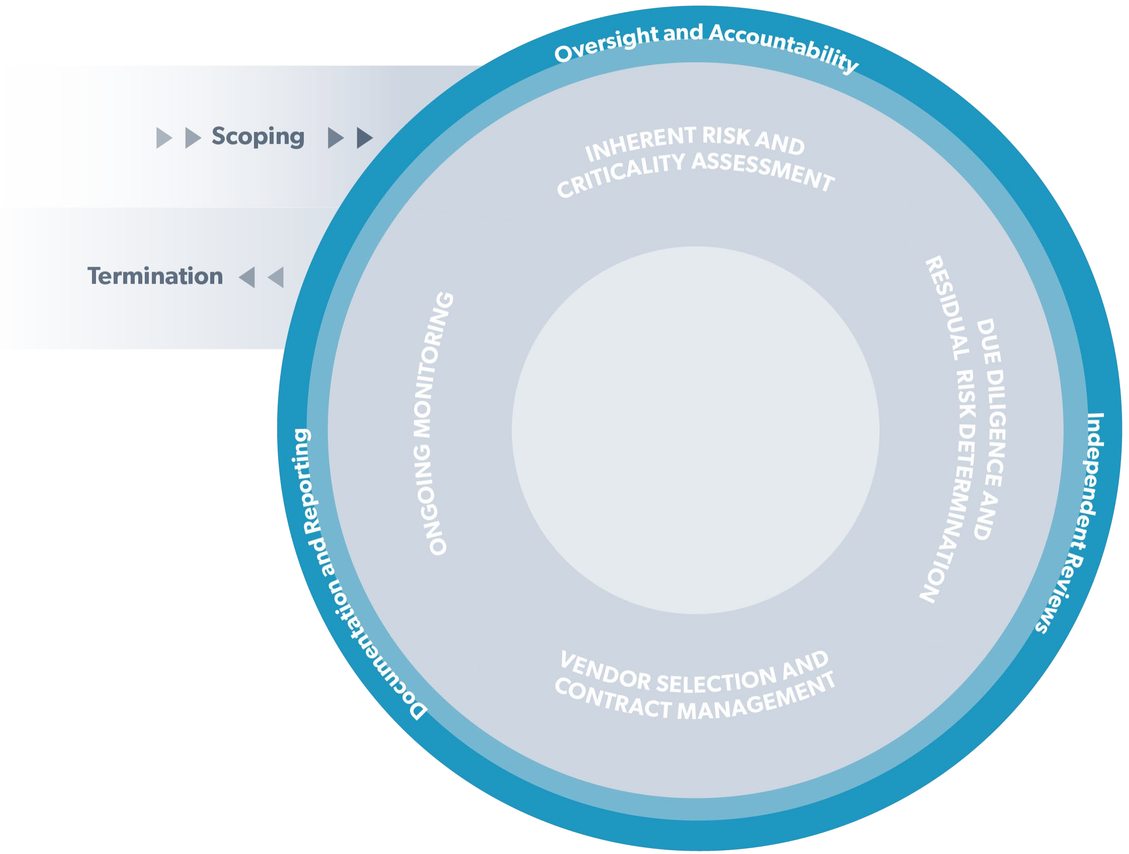


venminder

Guiding the Lifecycle

Documentation & reporting, oversight & accountability and independent review are peripheral to, but an integral part, of the third-party risk management lifecycle.

- Who will perform oversight on your third parties?
- Policies, programs, procedures, control evidence and reports
- Reporting is essential
- Bring in internal audit teams to keep your organization honest

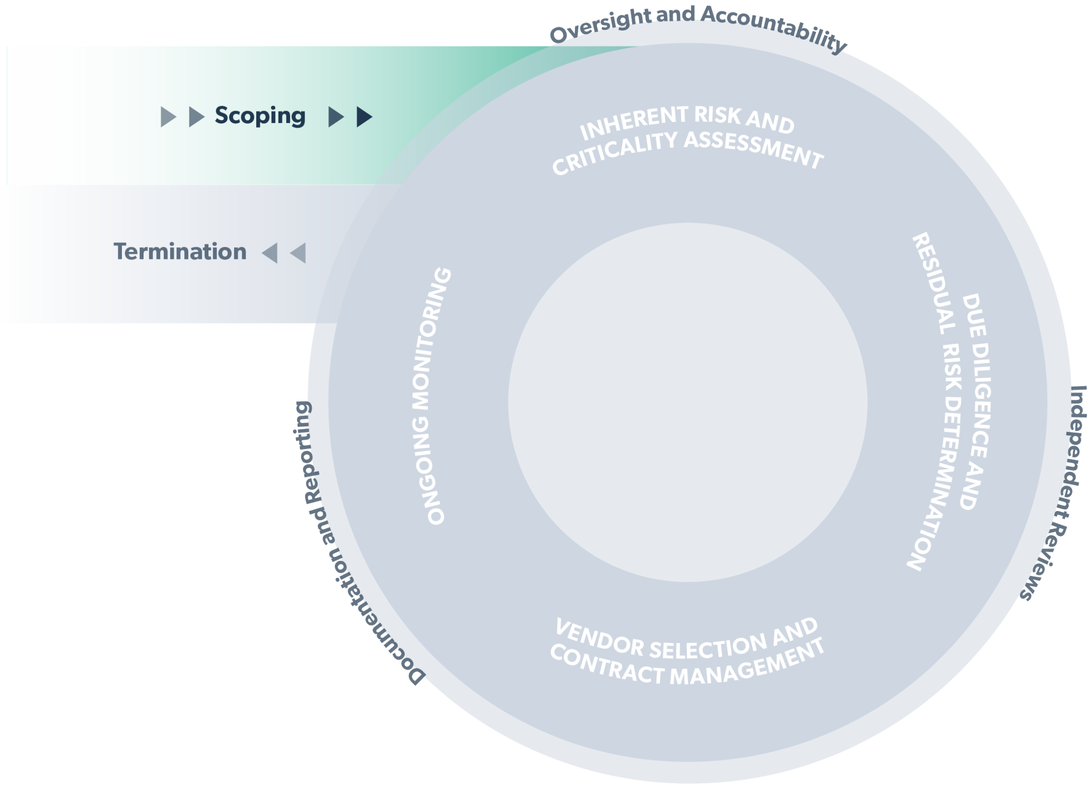


venminder

Scoping

Determine the scope of relationships that should and should not be a part of this lifecycle.

- Define what a vendor/third party/provider is to you
- Scoping is essential in getting the best of your third-party risk management resources

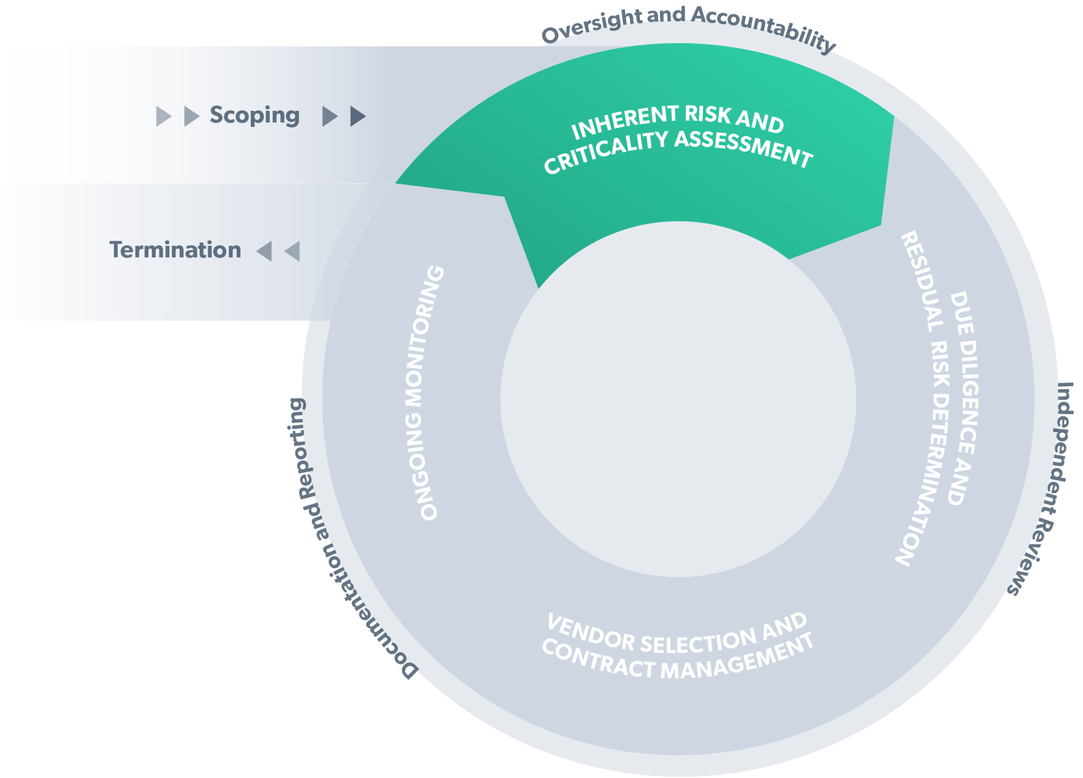


venminder

Inherent Risk and Criticality Assessment

A strong risk assessment process is vital to a comprehensive third-party risk management program.

- In order to understand the risk a vendor poses your organization, you must understand the relationship
- Evaluate all considerations of outsourcing
- Understand the most amount of risk the engagement could pose, and how critical they are (or will be) to your organization

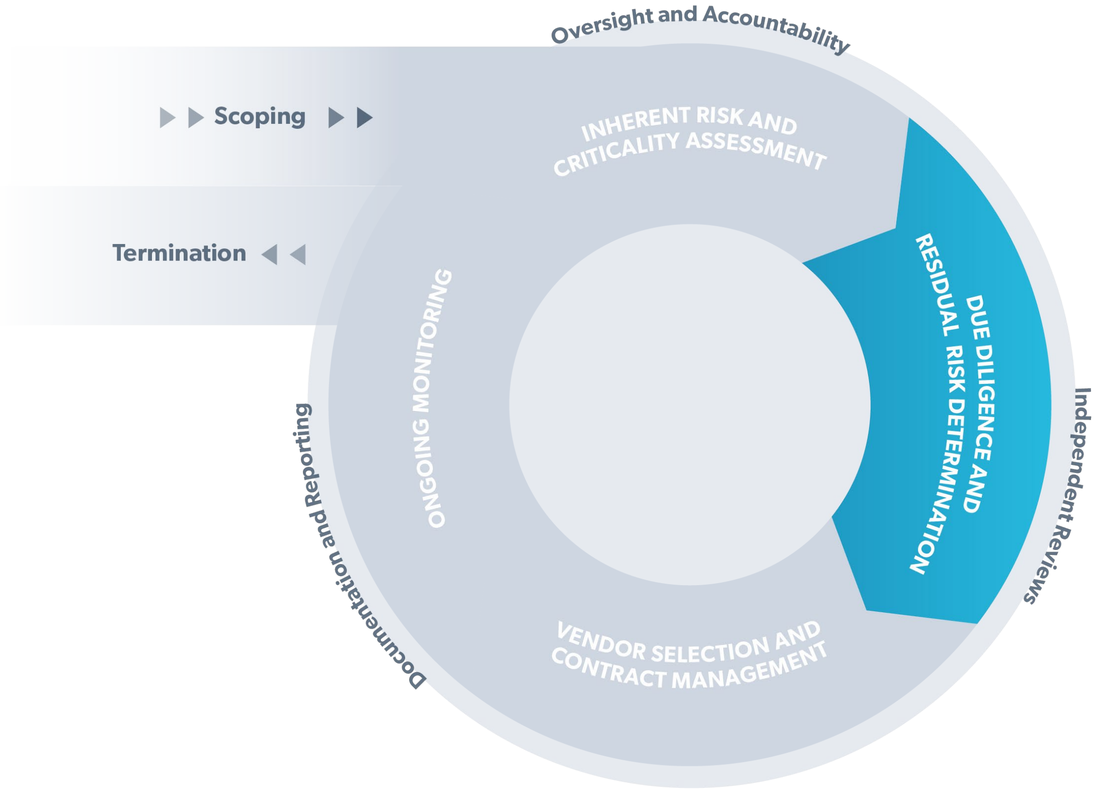


venminder

Due Diligence and Residual Risk Determination

Due diligence is one of the most important activities in third-party risk management.

- Support RFPs
- Conducted for new engagements and periodically for existing engagements
- Collect, review and assess applicable vendor information and controls
- Determine the remaining risk

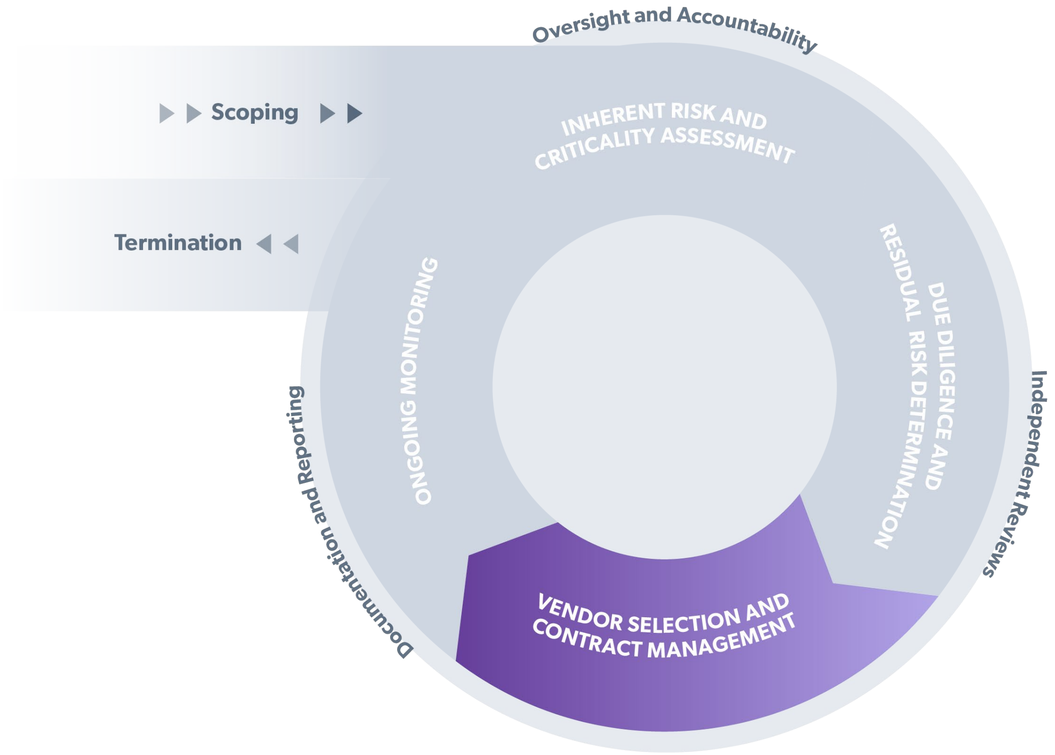


venminder

Vendor Selection and Contract Management

Choose the best vendor and go through the process for administering sound written agreements with third parties.

- Negotiation
- Change Management
- Ongoing Maintenance

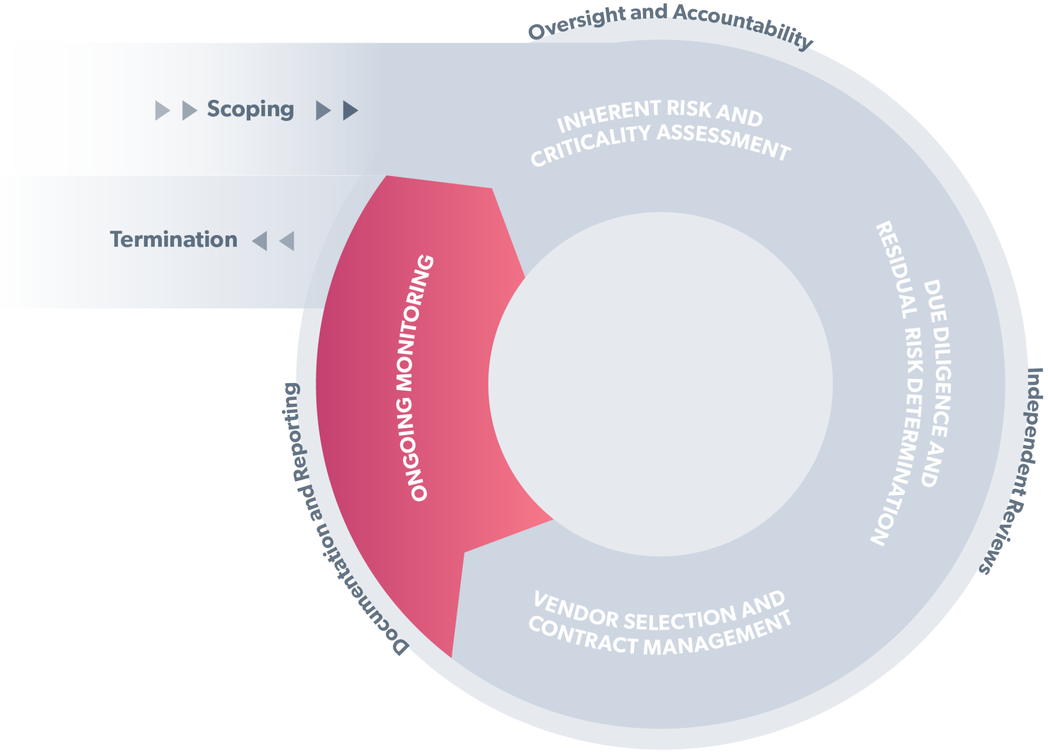


venminder

Ongoing Monitoring

Keep abreast of a vendors' performance and well-being throughout the engagement and continued periodic assessments.

- Verify vendors still meet expectations
- Identify areas of concern
- Discover contract gaps, poor vendor trends and declining service levels

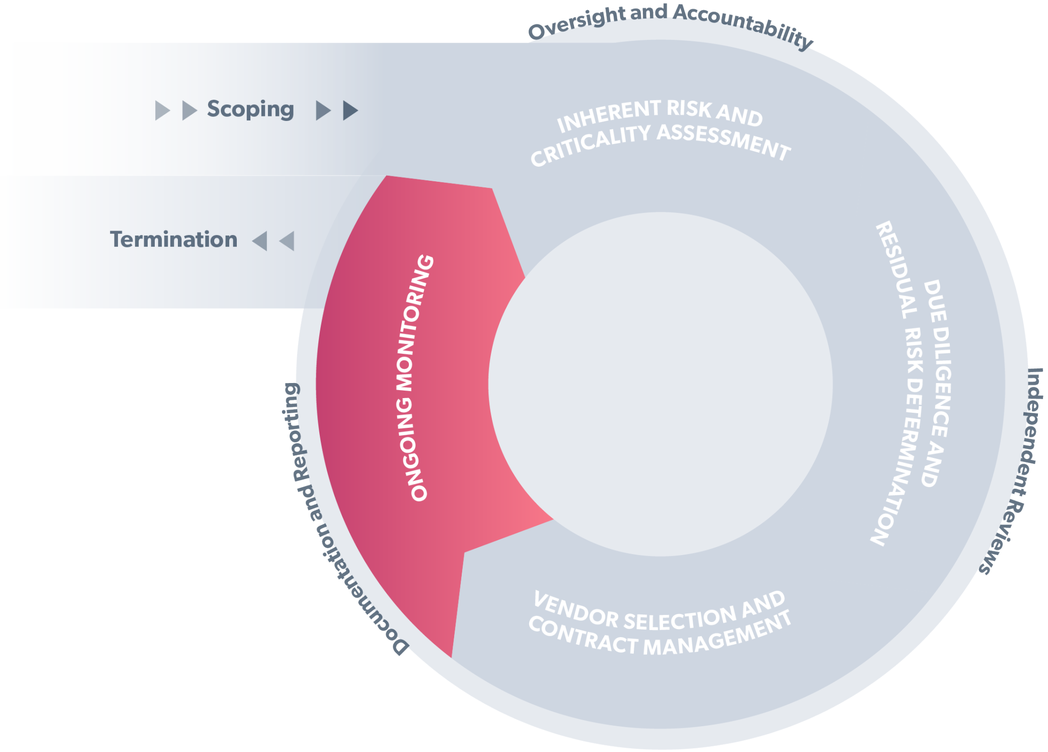


venminder

Ongoing Monitoring During COVID-19

Ongoing monitoring is crucial during the COVID-19 pandemic.

- Determine if vendor controls are adequate
- Check your vendors' financial posture
- Evaluate your vendors' cybersecurity

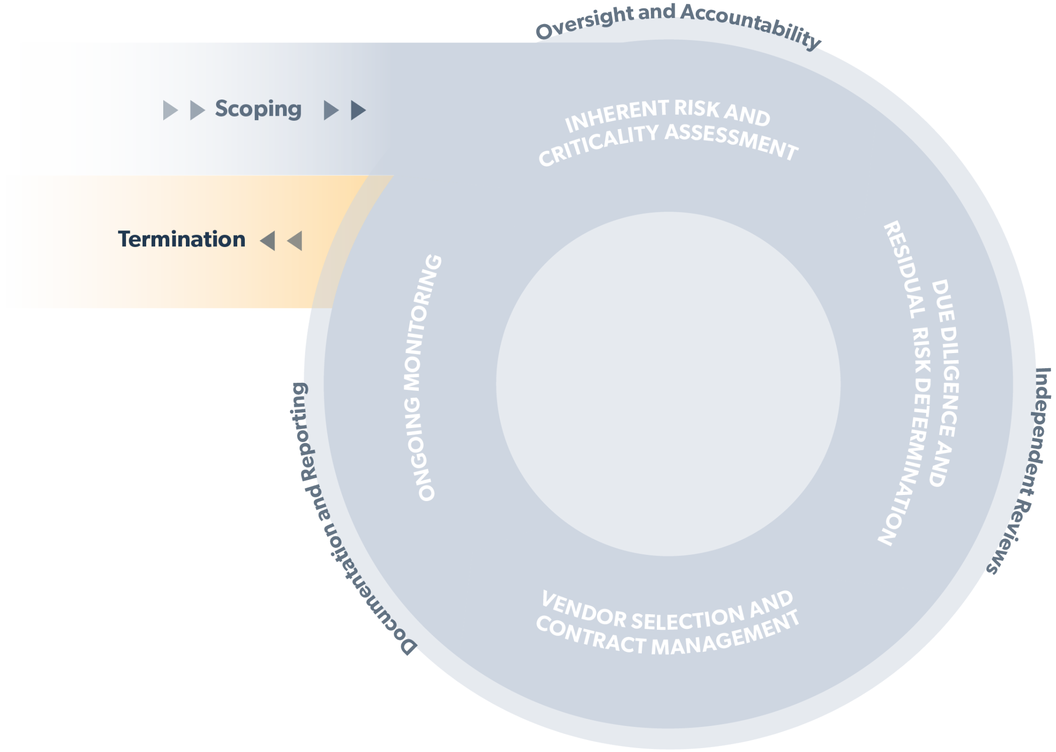


venminder

Termination

If the vendor relationship has come to an end:

- Ensure exit strategy requirements are met
- Notify the vendor of contract non-renewal



venminder

Poll Question

In your organization, where does vendor management sit (i.e., which line of business or function)?

a. Compliance
b. Risk Management
c. Executive Management / Board
d. Information Technology
e. General Counsel
f. Inside a line of business (i.e., marketing, operations, branch management)
g. I don’t know

Fourth Parties

Who is a fourth party?

Follow the data

Why should you care?

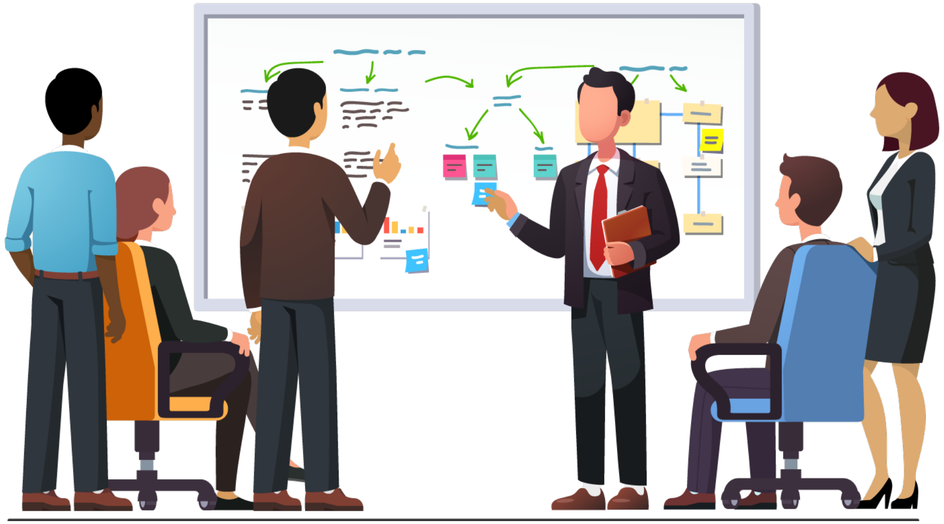
Challenges associated with fourth-party due diligence

venminder

Program Management

Just like safety and soundness, management matters

- Planning
- Organization
- Control
- Leadership



venminder

Regulatory Requirements & Frameworks for the FI

Regulatory Requirements

- CCPA
- NYDFS
- Cybersecurity: 23 NYCRR 500
- FFIEC Guidelines
- Prudential Regulator Guidance

Frameworks

- Capability Maturity Model
- COBIT
- COSO
- FFIEC CAT (Cybersecurity Assessment Tool)
- HIPAA/HiTECH
- HITRUST
- ISO/ IEC 9001, 27000, 31000
- ITIL/ITSM
- NIST 800-53
- NIST CSF (Cybersecurity Framework)
- OCTAVE
- PCI DSS
- SIG
- TOGAF
- Zachman

venminder

Federal Information Security Modernization Act Metrics

Department of Homeland Security & OMB

Fiscal Year 2020 CIO FISMA metrics focus on:

- Identify
- Protect
- Detect
- Respond
- Recover

FY 2020 CIO FISMA Metrics Version 1

venminder

Poll Question

What is your biggest challenge as an organization in exercising oversight over your third-party relationships?

a. Finding time to exercise oversight consistently
b. Getting vendors to respond timely to requests for information/reports
c. Interpreting the data received
d. Determining what change(s) to require based on data received
e. Obtaining management/board support to require change/reconsider the relationship, based on data received
f. Not sure

venminder

NIST Audit Standards

You can't focus on all 2,000+ controls

- Access Control
- SETA (Security Education, Training & Awareness)
- Cybersecurity Assessments
- Privacy
- Information Security

venminder

Change Management

Configuration Management Matters

- SDLC
  - Originated in the 1960s
  - 80% of project time is analysis
- DevOps
  - Wholistic business model
  - Packaged delivery

venminder

Do your third and fourth parties have these in their plans?

Storage Media Protection

- Backup strategy
- Encrypted backups
- Locking out USB ports

Privacy Authorization

- Is the paperwork in order?
- Do they ask to keep PII?

Physical & Environmental Protection

- Physical security
- Properly prepared physical environment

venminder

Development of Cybersecurity Policy & Compliance

- Tone from the top
- Policies… there are many
- Framework adoption (NIST 800-53 & CSF)
- Regulatory requirement breakdown

venminder

Business Continuity Management (BCM)

- BCM is an umbrella term that encompasses business continuity, disaster recovery and pandemic planning.
- A vendor's BCM program should align with its strategic goals and objectives. Management should consider a vendor's role within and impact on the overall industry when it develops a BCM program.
- Requires management to have processes in place to oversee and implement resilience, continuity and response capabilities to safeguard employees, customers, products and services.
- Resilience incorporates proactive measures to mitigate disruptive events and evaluate an organization's recovery capabilities.

Audit & Examinations: What the regulators expect

The board and senior management should engage internal audit or independent personnel to review and validate the design and operating effectiveness of the BCM program.

- Examiners will want:
  - ✓An analysis and review of the third party's business continuity, disaster recovery and pandemic plans
  - ✓Documentation available

- Examiners will review for the following:
  - ✓Alignment of BCM elements with the vendor's strategic goals and objectives
  - ✓Board oversight
  - ✓Management assignment of BCM-related responsibilities
  - ✓Development of BCM strategies

venminder

Risk Management Nomenclature

RISK

Exposing (someone or something valued) to danger, harm or loss.

INHERENT RISK

An assessed level of raw or untreated risk. That is, the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap. Literally, the amount of risk before the application of any risk reduction controls.

RESIDUAL RISK

The amount of risk or danger associated with an action or event that is remaining after inherent risks have been reduced by risk controls.

venminder

Risk Assessment and Management

Your third/fourth-party risk management program should have:

- Common rating scale
- Calculating Inherent risk

  Inherent Risk = Probability **x** Loss
- Calculating Residual Risk

  Inherent Risk **–** Impact of Mitigating Risk Controls **= Residual Risk**
- Risk appetite Statement
- Tiering Vendors

venminder

Poll Question

What has been your organization's biggest challenge in driving change(s) you determine are needed at your vendor as a result of monitoring the vendor?

a. Convincing the vendor that a change is necessary
b. Getting vendor buy-in to your desired method for fixing an identified issue, and/or timeframe for implementation
c. Insufficient/lack of contractual protections to ensure/require vendor cooperation in making such change(s)
d. Not sure

venminder

Best Practices

- Audit to a framework
- Breakdown regulatory requirements, then audit from your breakdown
- Find a platform for third/fourth-party risk management
- Track your findings, management responses and resolutions
- Don’t be afraid to “officially” accept the risk
- Imbed yourself in the third/fourth-party risk management program… you are the third line of defense

venminder

Third-Party Risk Regulatory Guidance

FIL-49-1999
Bank Service Company Act

FIL-81-2000
Risk Management of Technology Outsourcing

FIL-22-2001
Security Standards for Customer Information

FIL-50-2001
Bank Technology Bulletin: Technology Outsourcing Information Documents

FIL-68-2001
501(b) Examination Guidance

FIL-23-2002
Country Risk Management

Outsourcing Technology Services

FIL-121-2004
Computer Software Due Diligence

FIL-27-2005
Guidance on Response Programs

FIL-52-2006
Foreign-Based Third-Party Service Providers

FIL-105-2007
Revised IT Officer's Questionnaire

NCUA 08-cu-09
Evaluating Third-Party Relationships Questionnaire

NCUA 2007-cu-13
Evaluating Third-Party Relationships

FIL-44-2008
Guidance for Managing Third-Party Risk

FIL-127-2008
Guidance for Payment Processor Relationships

Supervision of Technology Service Providers

FIL-3-2012
Managing Third-Party Payment Processor Risk

CFPB 2012-03
Service Providers

OCC-2013-29
Guidance on Third Party Relationships

Federal Reserve SR 13-19/CA 13-21
Guidance on Managing Outsourcing Risk

FFIEC Social Media Guidance

FFIEC IT Handbook

OCC-2017-7
Supplemental Examination Procedures for Risk Management of Third-Party Relationships

OCC-2020-10
Frequently Asked Questions to Supplement OCC Bulletin 2013-29

NCUA SL-17-01
Evaluating Compliance Risk

OCC-2017-43
Risk Management Principles

FIL-19-2019
Technology Service Provider Contracts

OCC-2020-65
UDAP/UDAAP Exam Procedures

venminder

Questions & Answers

Post a Question:

www.thirdpartythinktank.com

THIRD PARTY thinktank

Email Us:

gordon.rudd@venminder.com

Follow Us:

@venminder

venminder

Thank You