July 23, 2019

venminder

Vendor Management 101

Branan Cooper
Chief Risk Officer
branan.cooper@venminder.com

Agenda

Vendor Risk Management
- why it's required today and how it can protect your company

The key components of a strong vendor risk management program

Determining the level of risk your vendor poses

Examples of what you should be reviewing on your vendors

Best practices to implement and mistakes you should avoid

Key Components of a Good Vendor Management Program

Recognition that vendor management is not a check box activity

Board approved vendor management policy, program and procedures

Executive staff who understand the importance of assessing and managing risk

Access to qualified due diligence resources

Adequate budget and relevant to size to do the job

Software tools to organize, manage, track and report

Execution of well-defined processes to onboard new vendors and manage existing vendors

Managing the Risk…It's the Whole Point

1

ASSESS THE RISK

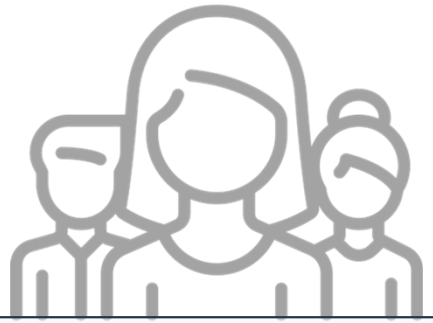
2

MANAGE ACCORDINGLY!

Definition of a **Critical Vendor**

Significant company functions (payments, clearing, settlements, custody) **or shared services** (internal audit, information technology)

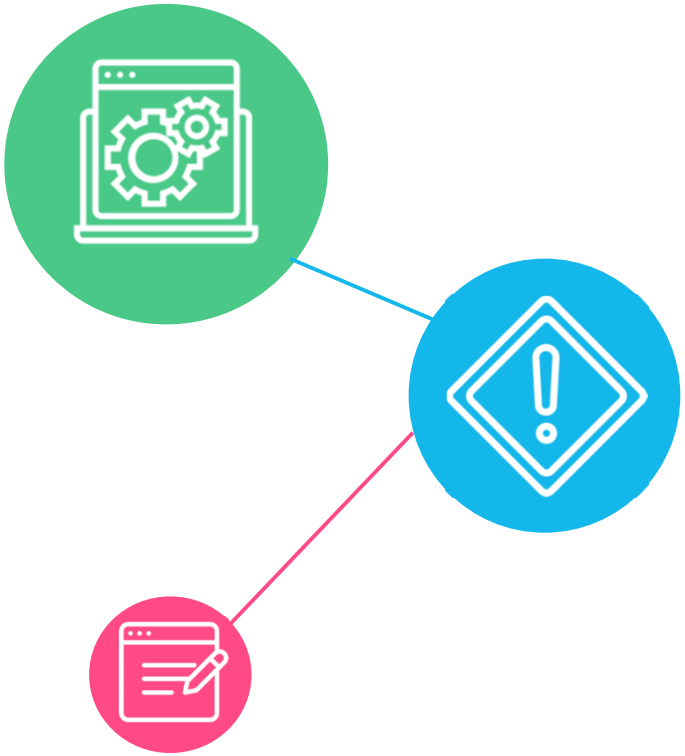
- Could cause a company to face significant risk if the third party fails to meet expectations.
- Could have significant customer impacts.
- Require significant investment in resources to implement the third party relationship and manage the risk.
- Could have a major impact on company operations if the company has to find an alternative third party or if the outsources activity has to be brought in-house.



Wide Range of Interpretation

Regulators mostly leave it up to the company

Definition of a **Critical Vendor**



Any service provider that could attract regulatory scrutiny or have an impact on the business, including the risk of loss in the event of a service disruption.

Definition of a **Critical Vendor**

Our advice to clients?
Ask yourself these 3 questions

1. Would a sudden disappearance of this vendor (e.g., due to insolvency, due to sudden termination) cause a material disruption to the business?

2. Would the disappearance have an impact on your customers / members?

3. Would the time to recover be greater than 24 hours / 1 business day?

If the answer is **yes** to any 1 of the 3 questions, your vendor is **critical**.

The Risk Assessment Process

The best solution is one that works for your company and leads to risk management being embraced and used to effectively manage third party risks.

Assess the inherent (initial) risk
Inherent risk is the level of risk before action is taken to manage it.

Mitigate risk through controls
Due Diligence – A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence.

Understand and manage to residual (modified) risk
The remaining risk after controls have been implemented and the considered effectiveness of those controls.

Inherent Risk

Definition

Inherent risk is the level of risk before action is taken to manage it.

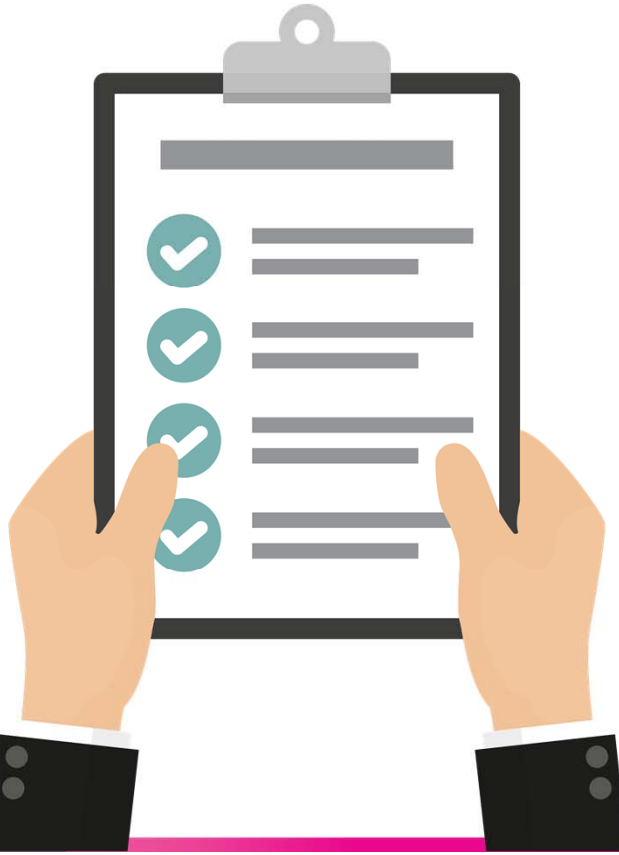
Categories

- STRATEGIC
- FINANCIAL
- COMPLIANCE
- OPERATIONAL
- TRANSACTION
- REPUTATION
- COUNTRY
- CONTRACTUAL

venminder

Due Diligence Components

- **SOC Reports**
- **Financial Reports/Audits**
- **BCP/DR Documentation**
- **Insurance Certifications**
- **Cybersecurity Preparedness**
- **Information Security Analysis**
  - Questionnaire
- **Fourth Party**
  - Reliance
  - Management
- **Legal and Regulatory**
- **Volume, nature and trends of consumer complaints**



The Obvious

Is the remaining (residual) risk acceptable?

IF YOUR INHERENT RISK WAS **HIGH**

AND YOUR RESIDUAL RISK IS **HIGH**

You have a PROBLEM

What do you do?

- ✓ Is it temporary or situational?
- ✓ Or systemic/long-term?
- ✓ Closely and frequently monitor
- ✓ Develop a Plan B
- ✓ Refer to your contract for recourse
- ✓ Talk to your vendor about remediation
- ✓ Replace when warranted

The Obvious

Is the remaining (residual) risk acceptable?

IF YOUR INHERENT RISK WAS **HIGH**

AND YOUR RESIDUAL RISK IS **LOW**

Wash, rinse & repeat annually

What will the **Examiners expect in 2019?**

It’s fairly simple

Demonstrate you **understand the risk** associated with the key vendors (inherent risk) and that you have **taken steps to mitigate/reduce** the risk (due diligence) to you and your customers.

Best Practices and **Mistakes** to **Avoid**

- ✓ Stick to the basics – don't be influenced by regulatory uncertainty
- ✓ Study new regulations
- ✓ Be responsive to new regulations
- ✓ Invest in education and industry resources
- ✓ Continue to grow the maturity of your third party risk management
- ✓ Keep policy and program updated
- ✓ Use enforcement actions as a lens through which to view your business

- X Wait till the examiners find fault
- X Nothings broken / don't fix it
- X Collect documents but doesn't review
- X Inadequate or no budget approval
- X Prisoners of non-compliant vendors
- X Unidentified risk

Third Party 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

FINRA Rule 3190

FINRA Regulatory Notice 11-14

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 Handbooks (esp Appendices E & J)

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

OCC-2017-21
Frequently Asked Questions to Supplement OCC Bulletin 2013-29

NCUA SL-17-01
Evaluating Compliance Risk

OCC-2017-43
Risk Management Principles

SEC Statement on Cybersecurity

OCIE Observations from Cybersecurity Examinations

FIL-19-2019
Technology Service Provider Contracts

Questions & Answers

branan.cooper@venminder.com

venminder

Follow us on:

venminder.com

Thank You