



Rules to Receive CPE Credit

By attending today's session, you are eligible to receive 1 CPE Credits 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



Creating or Maturing Your Vendor Risk Management Program

JUNE 9, 2020

PRESENTED BY
Gordon Rudd



Third-Party Risk Officer
Venminder

gordon.rudd@venminder.com



Session Agenda



Guidance in creating the right third-party risk program framework



The 3 primary components essential to building an exam proof vendor management operation at your organization



What senior management and the board must know



Best practices and key mistakes to avoid

Creating the Right Third-Party Risk Framework



- Senior Management and Board Support
- Appropriate Budget and Talented Staffing
- Documentation
- Time
- Autonomy from Lines of Business
- Rigorously Tested

3 Primary Components for Vendor Management

Governance documents,
which may include a policy
and program

Appropriate budget
assigned

Active involvement
by senior management and
board

Let's Start at the Top

Writing an Effective Policy for Vendor Management



Assemble the facts – new policy or revised?
» New guidance or revised guidance?



Who is the author?
» Many contributors but only one author for consistency



Involve experts and even trusted outside expertise
» Cite guidance



Speak to the board and regulators in terms they will understand by using their language
» Don't waste words, keep it high level



Set forth basic premise, scope, relevance to other policies and governance

The Meat of the Policy

A high-level summary of each stage of the third-party risk management lifecycle:

- ✓ Planning
- ✓ Risk Assessment
- ✓ Due Diligence & Third-Party Selection
- ✓ Contract Management
- ✓ Ongoing Monitoring
- ✓ Exit Strategy
- ✓ Termination



Stress the need for senior management and board involvement:

- ✓ OCC Bulletin 2013-29
- ✓ OCC Bulletin 2017-7
- ✓ OCC Bulletin 2017-21



Who is your primary regulator?

- a. OCC
- b. Fed
- c. FDIC
- d. NCUA
- e. CFPB
- f. State agency
- g. Other
- h. Not sure

Hand in Glove

Writing an Effective Program for Vendor Management



Build on the foundation laid by the Policy

Policy is the proverbial “50,000 foot view” – this is perhaps skyscraper height

You can see the details but not every little step

Who Writes These Documents?

Stick to one author

Involve experts from around the organization and beyond to provide details and context

Multiple readings and re-readings needed



How Should the Program Be Formatted?

- Scope of actively managed third parties
- Relevance or overlap with other standards (e.g., GLBA, enhanced due diligence)
- Define process for each lifecycle stage mentioned in the Policy

Mirror the structure in terms of sections laid out in the Policy

Be more expansive in detail as this is instructional for senior management

Get into numbers and detail and clearly define key objectives

Define Exceptions to the Process



What is generally acceptable or always unacceptable?

Who reviews, reports and approves exceptions?

What is the actual process for obtaining an exception?

What Senior Management and the Board Must Know

- Accountability flows from front line management all the way up to and rests with the board
- Set “tone-from-the-top” and empower vendor management
- Reporting is crucial and expectations should be defined
- Evidence of active involvement
- Codified in regulatory guidance



- Total inventory of actively managed third parties
- Status of assessing risk
- Due diligence items (how many, upcoming, any overdue or missing items)
- Ongoing monitoring activities
- Contract details (upcoming renewals, terminations or notable problems)
- Important upcoming updates to various committees

Examples of What to Report to the Board



Board Reporting Frequency and Format



Typically, reports should be on a regularly scheduled, recurring basis

For example:

- ✓ Monthly to risk or compliance committee
- ✓ Quarterly to audit committee or board

Report is typically an easy to follow PowerPoint or Word narrative



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. Information Security
- f. General Counsel
- g. Inside a line of business (e.g., marketing, operations, branch management)
- h. Not sure

Maintaining the Relevance of the Documents



When regulations change, Policy and Program **MUST** be reviewed

Additionally, review Policy and Program in context of new enforcement actions

Approve Policy and Program annually and keep a thorough change log

Maintain documents collected from vendors

Best Practices



- ✓ Thorough coverage of the third-party risk management lifecycle
- ✓ Supports other areas of your CMS
- ✓ Firm senior management support
- ✓ Robust due diligence and risk assessment processes
- ✓ Timely updates
- ✓ Follows changes to regulatory guidance
- ✓ Looks at industry news / enforcement actions



- ✓ Audited regularly, perhaps 3 lines of defense
- ✓ Processes for new products or services
- ✓ Management “buy-in”
- ✓ Robust and insightful reporting
- ✓ Accounts for all regulatory guidance, not just prudential regulator
- ✓ Invests in education, training, resources and expertise



Which stage of the third-party risk management lifecycle is your weakest point?

- a. Planning
- b. Risk Assessment
- c. Due Diligence & Third-Party Selection
- d. Contract Management
- e. Ongoing Monitoring
- f. Exit Strategy
- g. Termination
- h. Not sure

Common Mistakes



- Overlooking a lifecycle stage, such as ongoing monitoring or contract management
- Failure to link to other areas of the organization
- Weak or inefficient processes for new third parties
- Documents grow stale
- Ineffective senior management support or lack of accountability
- Exceptions to policy run amok
- Following a checklist mentality
- Unresponsive to feedback or criticism
- Failing to react to consumer complaints



What's Driving the Focus on Third-Party Risk Management?

- Multiple regulators, often appear incongruous
- CFPB focus on consumer complaints
- CFPB's broadsword approach to enforcing UDAAP
- The role of third parties in some notable actions (Equifax, Microsoft)
- Focus on cybersecurity
- Analysis of subservice providers

What to Do When There's a Breakdown

- React quickly but not foolishly
- Inform senior management and the board
- Assess the situation
- Determine the root cause
- Document, document, document
- Test



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

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

Post a Question:

www.thirdpartythinktank.com



Email Us:

gordon.rudd@venminder.com

Follow Us:

@venminder



ALSO JOIN US AT **Our Upcoming Webinars:**

June 23, 2020:

The Basics of Vendor Risk Assessments

July 14, 2020:

How to Classify Who Is a Critical Vendor

[Click here](#) to view our Webinars Page.



Thank You

