Writing an Effective Vendor Management Policy & Program Document

Presented by Branan Cooper
Chief Risk Officer at Venminder
branan.cooper@venminder.com
(502) 909-0325

April 27, 2017
Session Agenda

- Tips on writing a program
- Walk through a policy
- Fundamentals of the documents
- Creation Logistics
Poll Question:

How mature would you rate your vendor management program?
Fundamental Principles of the Documents

Policy and Program may be unique documents but should correlate heavily.

Policy is Board level and appropriately high level.

Program is Senior Management level and more instructive.

REFER TO OUR UMBRELLA SERIES FOR AN ILLUSTRATION OF THE IDEAS.
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 using their language
  » Don’t waste words, keep in high level

✓ Set forth basic premise, scope, relevance to other policies and governance
A high level summary of each of the pillars of third party risk management:

- Select a New Third Party
- Due Diligence
- Risk Assessment
- Ongoing Monitoring
- Contract Management
- Board Reporting

Stress the need for Senior Management and Board involvement

- OCC Bulletin 2013-29
- OCC Bulletin 2017-7
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 it?

- 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 it be formatted?

- Mirror the structure in terms of sections laid out in the Policy
- Get into numbers and detail and clearly define key objectives
- Be more expansive in detail as this is instructional for Senior Management
- Scope of actively managed third parties
- Relevance or overlap with other institution standards (e.g. GLBA, Enhanced Due Diligence)
- Define process for each pillar mentioned in the Policy
Define Exceptions to the Process

- What is generally acceptable or always unacceptable?
- Who reviews, reports and approves exceptions?
Key Components of your Third Party Risk Management Policy

1. Overview of Policy
2. Statement of Policy
3. Relevance to other compliance policies
4. Risk assessment process and tolerance
5. Due diligence process and exceptions
6. Oversight and monitoring
7. Contract standards
8. Reporting and board accountability
The role of Senior Management and the Board

✓ Accountability flows from front line management all the way up to and rests with the Board

✓ Reporting is crucial and expectations should be defined
Maintaining the Relevance of the Documents

When regulations change, Policy and Program MUST be reviewed

Additionally, review in context of new enforcement actions

Approve annually and keep a thorough change log
VISIT OUR RESOURCES LIBRARY FOR MORE FREE VENDOR MANAGEMENT TOOLS

DOWNLOAD OUR FREE UMBRELLA INFOGRAPHIC SERIES to learn more about writing Policy, Programs & Procedures documents

- FDIC FIL 44-2008
- OCC BULLETIN 2013-29
- OCC BULLETIN 2017-7
- FFIEC APPENDIX E
- FFIEC APPENDIX J
Understanding and Dissecting a Vendor SOC Audit Report

Mike Morris
Partner
mmorris@pkm.com
(404) 420-5669

Mary Beth Marchione
Systems Manager
mmarchione@pkm.com
(404) 548-2825

April 27, 2017
Session Objectives

Understand SOC1 vs SOC2

Understand Key Components
- System description
- Subservice organizations
- Opinion
- Tests of controls and evaluating results
- Unaudited information

Control Considerations

Industry update: SSAE18
SOC1 vs SOC2

REPORTS ON:
Internal Controls over Financial Reporting

USERS:
Accounting, Compliance, and Financial Statement Auditors

REPORTS ON:
Security, Availability, Confidentiality, Processing Integrity, and/or Privacy

USERS:
Risk Management and Data Security Overseers
Key Components

**System Description**

Has the vendor provided the correct report?

The system description section of the report will detail the services/products provided.
Key Components

Subservice Organizations

Service providers used by your vendor

Report should clarify exactly how subservice organizations are used

Inclusive vs. Carve Out Method
Key Components

Tests of Controls and Evaluating Results
Clean?

Opinion

Does this directly impact the service provided?

Exceptions

Is management’s response sufficient?

If not, how is the subservice organization addressing the issue(s)?

Are other controls/procedures in place that give me comfort?
Poll Question:

Do you currently map end user controls contained in SOC Reports to organization controls?
Control Considerations

- Are you in compliance?
- Are you documenting compliance?
- Is this done annually?
Poll Question:

Do you know what the update from SSAE16 to SSAE18 includes?
Standards and Industry Update

SSAE16 vs AT101

Replace with SSAE18
Conclusion

✓ SOC1 is focused on internal controls over financial reporting
✓ SOC2 is focused on Security
✓ Key components of audit reports include:
  – System description
  – Subservice organizations
  – Opinion
  – Tests of controls and evaluating results
  – Unaudited information
✓ Control considerations should be evaluated annually
✓ SSAE18 is the new industry standard
Questions & Answers

mmorris@pkm.com
mmarchione@pkm.com
Vendor's Financial HEALTH from a Management Point of View

Presented by Mike Bowers

Chairman at Venminder

michael.bowers@venminder.com

April 27, 2017
Session Agenda

Importance of financial health

Financial health ratings

What to pay attention to

Declining financial health
Where are you spending your time

Reading a 32 page financial analysis

Financial performance is NOT “event of default”
You need to focus on vendor’s financial health, NOT performance

The analysis is not about the numbers or financial analytics; it is about making decisions

Does the financial health of this vendor pose a potential problem to the services they provide my customers and to help others in your organization evaluate the vendor

You are determining vendor health, not making an investment or loan decision

Quickly determine if you have a problem

Don't sweat the small stuff
Here is the Challenge

We do 60 to 70 analyses a month

97% of vendors provide some sort of financial statement

65% are private companies

32% are public companies
Financial Health Ratings

- ADEQUATE
- MODERATE
- NEED MONITORING
- INTENSE MONITORING
Poll Question:

Is your Financial Health Rating similar to example?
Financial Health Ratings

- **ADEQUATE**: 22%
- **MODERATE**: 41%
- **NEED MONITORING**: 23%
- **INTENSE MONITORING**: 14%
Out of 100 vendors, who are at the bottom?

- ADEQUATE: 22%
- MODERATE: 41%
- NEED MONITORING: 23%
- INTENSE MONITORING: 14%
What to Really Pay Attention to

The keys to what we believe is important:

**Making money and/or have sufficient capital to support their ongoing operations**
*(This is the biggest driver of financial health)*

*Domino Effect*

**Debt to worth:** important item but harder to get your arms around. Third party reviewers are critical: Moody’s, Standard and Poor’s, Altman Z-Score
The domino effect of declining financial health is crippling:

- Declining income means cost cuts
- Cost cuts mean cutting staff
- Cutting staff means declining service levels
- Declining service levels
- Declining response time
- Declining maintenance of security and systems
- Which means findings on SOC reports and Sunset of products
Other non-numbers to review; especially in the 10K

(The 10K is formatted identically for all publicly traded companies)

1. **First**, look at risk factors. These are outlined in detail with special note to any regulatory action that might have occurred.

2. **Next**, look for any legal proceedings or lawsuits that are pending, along with the estimate of the anticipated settlement charges.

3. **Finally**, the auditor’s opinion: Their opinion on financials, especially on comprehensive income, and their assessment of the adequacy of the internal controls as well as going concern.
Here is What you Need to Think About

1. How quickly are you getting to a decision?
2. Does my analysis look beyond the numbers?
3. Have we begun to see the domino effect?
4. Who can provide similar service?
5. Are their financials better than my current provider?
6. What is the estimated time to convert?
7. What is cost to switch?
Poll Question:

Does senior management review SLA's prior to execution of contract?
One More Thing When Financial Health is Declining

Vendor financial health is not a secret to the vendor (your sales person, maybe, but not to the company)

Conversation with current vendor *Management*

Outline concerns; how are they fixing and by when

Service Level Agreements (SLA) are your best course of action. Most under appreciated part of any vendor contract

The contract gets lots of reviews (attorney, CFO, product manager), but SLA are rarely brought to attention of executive management; nor is their compliance to the agreements. *(Only reported by the vendor)*
Summary

As management, it is essential that you understand the financial health of your vendor.

- It’s required by regulation
- Qualified subject matter experts must do the analysis
- Decoding a 10K can be challenging, but a must do
- Don’t let the domino effect of declining financial health surprise you
- Assess your risk and (escalate) monitoring accordingly
- Use your SLA’s, Use your SLA’s
- Understand your options quickly
Questions & Answers

michael.bowers@venminder.com
Thank You