Vendor Risk Management™
A Magical Mystery Tour

Presented by:
J Michael Edison (Mike)
CEO, Fortrex Technologies, Inc.
edisonj@fortrex.com
240-575-7476
This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships.
The Magical

OCC 2014-53 Cyber Security Assessment

National banks and federal savings associations (collectively, banks) need to understand their inherent cybersecurity risks and consider current practices and overall preparedness, focusing on the following:

• Risk management and oversight
• Threat intelligence and collaboration
• Cybersecurity controls
• External dependency management
• Cyber incident management and resilience
The Magical

FIL-9-2015 Appendix J – Business Continuity Plan

Appendix J of the BCP Booklet discusses the following four key elements of BCP that a financial institution should address to ensure that their technology service providers (TSPs) are providing resilient technology services:

• Third-Party Management.
• Third-Party Capacity.
• Testing with Third-Party TSPs.
• Cyber Resilience.
The FDIC, in coordination with the other members of the Federal Financial Institutions Examination Council (FFIEC), is issuing the FFIEC Cybersecurity Assessment Tool to help institutions identify their cybersecurity risks and determine their preparedness.
The truth is that it is not magic at all. The guidelines are very clear.
So why does it seem so magical?

Because sometimes we strive to give the **illusion** that we have a thorough program. This is a **Mystery** to me.
The Mystery Revealed

In general, the industry has been conditioned to see how little they can do in order to pass examination scrutiny. Why?
The Mystery

Reasons for minimalist approach by C-level management:

Cost
Personnel Count
Lack of Understanding
Historical Lack of Enforcement
The Mystery

Cost

- Cost concerns create a lack of BoD and upper management support
  - Too often management’s goal is a grade of C---
  - VRM is viewed as only overhead having no positive impact on revenue
  - Management has the following view: Why pay? It’s already free.
The Mystery

Personnel

○ No new head count for VM. Add it to someone's job description. Result:
  ▪ New Vendor Manager has:
    • Too many job responsibilities
    • No budget
    • No upper management support
    • Little authority to assign tasks to others
The Mystery

Lack of Understanding

Why does every institution have to conduct due diligence on a vendor that “everyone” utilizes?

We’ve never had a problem before!
The Mystery

Historical Lack of Enforcement

The examiners have threatened to crack down on this before and never did.

They’ll warn us before writing us up so we have plenty of time.
Solving The Mystery

Cost

- Understand the true cost of minimal action
  Many man-hours are wasted preparing for the VM portion of Safety and Soundness exams due to:
  a. Difficulty locating contracts
  b. Discrepancy in identification of critical vendors
  c. Proving due diligence conducted
Solving The Mystery

Cost

How many unintentional contracts auto renewed in the past two years?

a. What was the dollar amount spent/lost?

b. Was the data returned without additional unexpected charges/fees?
Solving The Mystery

Cost

Did you lose track of any lease agreements in the last two years?

a. Did you lose office space as a result?

b. If you were the lessor, did you lose revenue?
Solving The Mystery

Cost
Maximize Efficiency
How much time did you spend tracking down the following?

a. Due diligence documents
b. An SME to review financials, SSAE 16’s, contracts, insurance?
Solving The Mystery

Cost
Investment Protection

Are you using a spreadsheet for VRM?

a. Are you paying to have the spreadsheet developed?
b. Have you trained the individual on VRM?
c. What does the spreadsheet do for you when it is not opened?
d. What does the spreadsheet do for you when the individual responsible changes jobs?
e. Will you pay the next person to start over with the same process?
Cost
Consistent Pre Contract Due Diligence

Is your vendor boarding process consistent?

a. Due diligence documents requested and reviewed pursuant to the criticality of the proposed relationship

b. Does the contract have the language as defined by the FFIEC?

c. Has an internal assessment of the institutions ability to manage the relationship been conducted?
Solving The Mystery

Personnel

Efficiency

Are your lines of business engaged?

a. Does your current program promote LOB involvement?

b. Do they find the task overwhelming?

c. Do they waste time chasing down subject matter experts to review due diligence?

d. Do they waste time acquiring vendor due diligence data?
Solving The Mystery

Lack of Understanding

- BoD’s must understand their role.
- Executive management must understand the hidden costs of doing nothing.
Solving The Mystery

Historical Lack of Enforcement

The trend that we see in the industry is that examiners will no longer give a verbal suggestion. They understand that budgets get approved when items show up on an MOU.
The Tour

Industry Trends
Regulatory Trends

- Regulators have increasing expectations for managing vendor risk
- Enhanced focus on cyber security
- Less tolerance for inaction
- Acceptance of third-party due diligence assistance
New Report Highlights 2015 Regulator Expectations
In 2015, regulators will expect banks to step up standards for governance, consumer protection compliance, third-party risk management, cybersecurity, credit quality and anti-money laundering compliance, according to a new report from Deloitte.
Solution Trends

- Organic solutions are only sufficient for institutions tracking just a few vendors
- Point solutions are growing in capability and service add-ons which have allowed them to be effective in larger, more complex environments
- More focus on one-stop for all vendor management related activities (Compliance Information Exchange)
- Efficiency will grow in importance as new regs are issued
Magical Mystery Tour Summary

- Regulators have increasing expectations for managing vendor risk
- If you are using a home grown solution, you may be wasting time and money
- As regulations increase, efficiency becomes more critical
- Automated solutions solve many of the issues above
Magical Mystery Tour Summary

Questions?

VendorPoint

VendSure