Session Agenda

- Understand the elements of a complete vendor management program
- Understand how to clearly document your vendor management program activities
- Learn of prevalent vendor management issues that we are seeing
Why Vendor Management?

The use of vendors to outsource critical processes

You cannot outsource your risk!

You must have a mechanism to evaluate and monitor your key vendor’s providers

Your risk might extend past your vendor to subservice providers

The use of vendors to outsource critical processes
Where to Begin?

Every good vendor management program starts with a **complete list of vendors.**
Documentation

- Formal Vendor Management Program (policy and procedures)
- Vendor Risk Assessment (all vendors)
- Individual vendor due diligence (for high-risk vendors)
- ‘Appendix J’ elements
- Board reporting
Vendor Management Program

- Directive control — Policy document to guide program
- Define risk-based methodology
- Tools for management
- Process to report and track issues
- Update annually
Vendor Risk Assessment

Identify all critical vendors

Risk buckets:
- Strategic
- Operational/Transactional
- Legal/Regulatory
- Compliance
- Security

Risk Factors:
- Type of Information Accessed
- Controlled or Ongoing Access to Systems
- Type of Access (Read Only or Change/Edit)
- Criticality of Vendor Service
- Financial Impact
Individual Vendor Reviews

- Financial statements
- SOC report review
  - SOC 1 versus SOC 2
  - Complementary User entity controls
- Key contract provisions/
  Service Level Agreements (SLAs)
- Penetration testing results (cyber resilience)
  - Breaches
  - Incident response responsibilities
Poll Question:

As part of your vendor management review, do you review business continuity planning and/or testing?
Individual Vendor Reviews

- Business continuity planning
- Business continuity testing
- Secure coding
- Issue resolution/remediation
- Insurance coverage
Individual Vendor Review

How to Document

Narrative

Summary

Checklist

Supporting Documentation
New Vendor Due Diligence

- Risk-based procedures
- Reputation
- Insurance coverage
- Audit reports
- Penetration testing results
- Business continuity planning
- Business continuity testing
- Technology used/integration
Board Reporting

- Program
- Risk Assessment
- Ongoing Monitoring
- Reportable Issues
- SLAs
Poll Question:

Have you had an audit or exam review finding related to vendor management in the past year?
Prevalent Issues

Vendors with access to non-public customer information have not been identified
Prevalent Issues

For new vendors, vendor risks are not being evaluated (or are not documented) before signing the contract.
Prevalent Issues

Subservice organizations have not been identified or appropriately evaluated.
Prevalent Issues

The institution has not mapped the complementary user entity controls listed in key SOC reports to specific controls maintained and tested by the institution.
Prevalent Issues

Management has not obtained third-party service provider business continuity plans or testing documentation to determine the vendor can appropriately recover and continue service in a disaster situation.
Prevalent Issues

Management has not participated in third-party service provider business continuity testing to ensure operating capabilities in a disaster situation.
Conclusion

✓ A complete vendor management program includes policy, risk assessment, vendor review (monitoring), due diligence, and reporting

✓ Activities should be clearly documented

✓ To avoid the pitfalls of prevalent issues, it is important to:
  – Review all vendors
  – Consider business continuity
  – Document due diligence efforts
  – Document compliance with end user control considerations
Questions & Answers

mmorris@pkm.com
mmarchione@pkm.com
Vendor Risk Assessment Workshop

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

April 25, 2017
Session Agenda

- General webinar instructions
- How to ask questions
- What to do if technical problems occur
Poll Question:

Do you have a documented Risk Assessment process as part of your vendor management protocol?
Regulatory Guidance

What the guidance says:

Regulatory guidance mandates any well managed program includes a risk assessment of third parties

- OCC Bulletin 2013-29
- FDIC FIL 44-2008
- OCC Bulletin 2017-7
Categories of Risk

Business Impact
Critical vs Non-Critical
The 3 threshold questions you should ask

Regulatory Risk
High, Moderate, Low
What categories you should consider
Why a Risk Assessment Needs to be Done

- Fundamental pillar that informs all other areas of risk management
- What to do in follow up
High Risk

High risk does not always mean Critical or vice versa

High risk is not at all a bad thing
Quick Definitions

Inherent

Residual

Mitigating Control
And now let’s create a risk assessment...
Questions & Answers

branan.cooper@venminder.com
Thank You