QUANTIVATE

VENDOR MANAGEMENT 101

Enterprise Risk Management
Vendor Management
Business Continuity
IT GRC
Internal Audit
Regulatory Compliance Manager

Introduction to Vendor Management

About Your Presenter

Andrea Tolentino

Lead Operations Consultant

Quantivate LLC

425-947-5829

Andrea.Tolentino@quantivate.com

www.quantivate.com

About Quantivate

- Founded: 2005
- HQ: Woodinville, WA (Seattle Area Tech Core)
- NAFCU Services Preferred Partner for Vendor Management
- Offer complete GRC Suite

Outline

- Introduction to VM
- The VM Process
- Vendor Classification
- Due Diligence and Oversight
- Vendor Risk Assessment
- Preparing for a VM Audit

Introduction to VM

- What is Vendor Management
- 6 Components of Vendor Management
- Regulations
- Who owns the VM program?
- Business Benefits

What is Vendor Management?

- Vendor Management is the art of getting more out of your suppliers.
  - More Service
  - More Assurance
  - …and More Value

The 6 Components of VM

- Vendor Selection
- Vendor Inventory
- Contract Management
- Due Diligence and Oversight
- Risk Assessment
- Vendor Performance Management

1. Vendor Selection

- RFPs
- Legal Review
- Negotiation
- Onboarding

2. Vendor Inventory

Best Practice #1: Start with your Accounts Payable system

Common Mistake #1: Don’t include every vendor in your VM program.

3. Contract Management

- File Management
- History
- Dates
- Terms

4. Due Diligence and Oversight

"Prove to us that you reducing the risk to our member/customers"

- Look for independent documentation of controls where possible
  - Financial Risk – Audited financial statements
  - Legal Risk – Insurance certificate
  - Info Security Risk – SSAE 16

Common mistake #2: Don't let IT/Info Sec control the Due Diligence Process.

Best Practice #2: Get subject matter experts involved for each part of the DD review.

5. Risk Assessment

Comparing

The Likelihood vs. The Impact

of a vendor failing

and hurting your organization

6. Vendor Performance Management

- SLAs
- Service
- Long term strategy
- Leverage for contract re-negotiation

Regulations

- 2007 NCUA Letter to the Credit Unions 07-01: Evaluating Third Party Relationships Link
- April 2012 CFPB Bulletin on Service Providers Link
- FDIC Compliance Manual : Third party Service Providers Link
- FFIEC IT Examination Handbook: Third Party Oversight Link
- *OCC Bulletin 2001-47, Third Party Relationships: Risk Management Principles* Link

Who Owns the VM Program?

- Finance
- IT
- Compliance
- Risk
- Legal

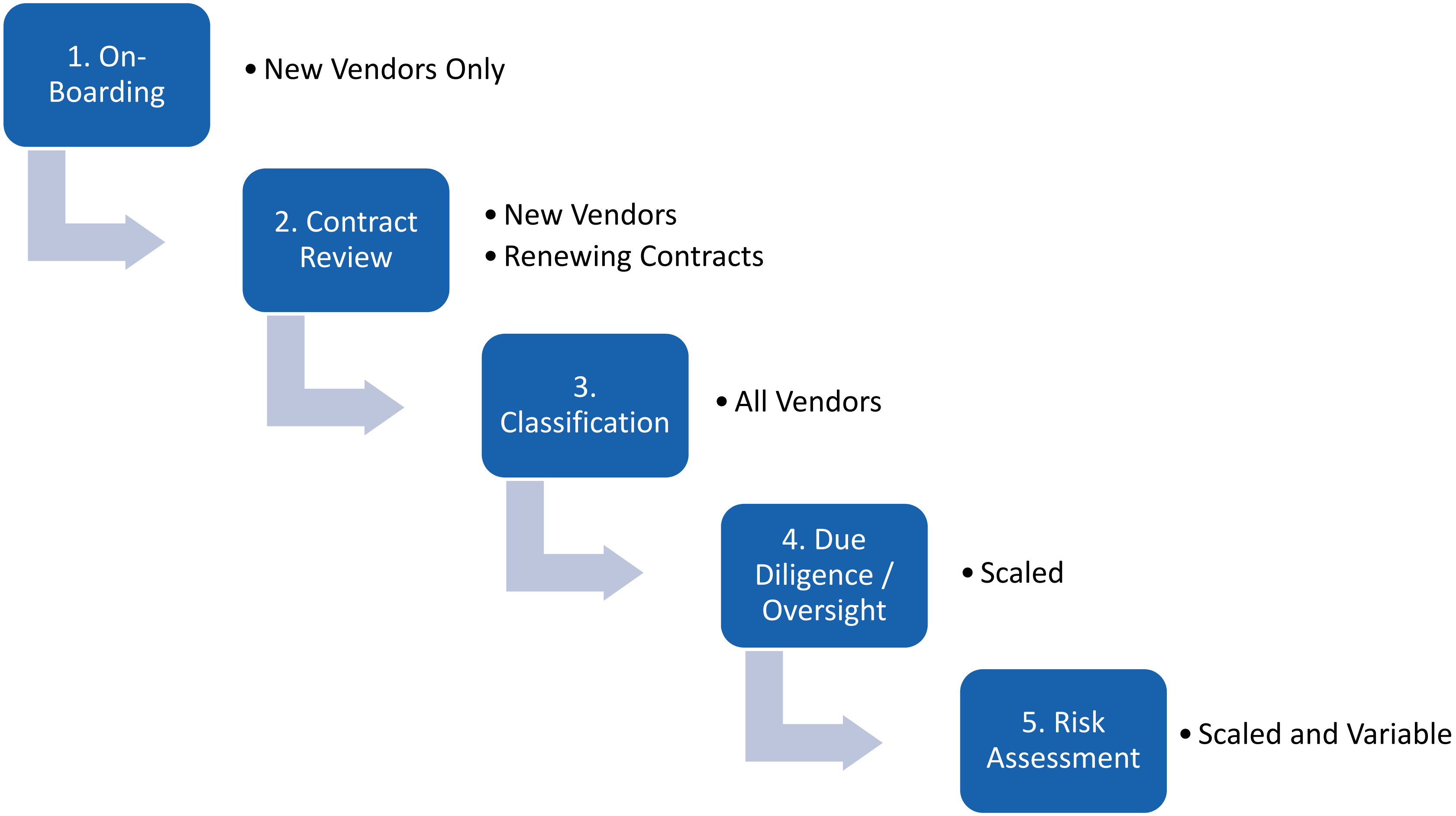
Business Benefits

- Better Service
  - From your vendor
  - To your member/customers
- Increased Assurance
- More Value

VM Process

1. Example VM Process
2. Vendor On-Boarding
3. Contract Negotiation
4. Classification
5. Due Diligence and Oversight
   - SSAE 16 reviews
6. Risk Assessment

1. Example VM Process



1. On-Boarding

- New Vendors Only

2. Contract Review

- New Vendors
- Renewing Contracts

3. Classification

- All Vendors

4. Due Diligence / Oversight

- Scaled

5. Risk Assessment

- Scaled and Variable

2. Vendor On-Boarding

- Business Objectives
- Rational for Outsourcing
- Cost vs. Benefit Analysis

Tip #1: Track starting & ending costs of vendor services – Helps prove the ROI of your VM program.

- Final Recommendation and Approval

Tip #2: Document reasons for making a new relationship with the vendor

3. Contract Negotiation

14 areas to check (minimum)

1. Scope of service
2. SLAs/Performance
3. Confidentiality
4. Security and Controls
5. Financial/Audit Reports
6. Software License/ Intellectual Property Ownership
7. Warranties

3. Contract Negotiation (con’t)

8. Limitation of Liability
9. Indemnification
10. Pricing Fees and Payment
11. Term
12. Termination
13. Dispute Resolution
14. Assignment

Tip #3: Remember/customer it is a give and take process – the process is needed for everybody to feel like they have arrived at win-win deal.

4. Classification

- Financial Impact
- Information Sharing
- Cost
- Operational Impact
- Third Party Reliance
- Transactional (risk of fraud)
- Other categories to think about:
  - Reputation, Legal/Liability, Confidentiality/Integrity, Regulatory, Member/Customer Satisfaction, Competitive Advantage

Tip #4: Be consistent when classifying vendors, have clear definitions and make sure each vendor owner treat them the same.

5. Due Diligence and Oversight

“Prove to us that you are reducing our risk”

- Business changes/strategic plan
- Financials (D&B if needed)
- Legal
- Operations/Performance
- Regulatory/Compliance
- Dependencies
- Human Resources
- Information Security
- Reputation
- Business Continuity

SSAE 16 reviews

- Date, Time, and Reviewer
- Exceptions to testing and Management Response

6. Risk Assessment

- Risk = Likelihood x Impact
- Comparing the likelihood vs. the impact of the vendor failing and hurting your organization in each of the associated risk areas.
- Requires both SME of area and Vendor Owner.
- Likelihood comes from DD information, Impact comes from business owner

Tip #5: Remember- Rate the Risk but do something about it.

Tips Review

- Track starting and ending value of vendor services – Helps prove the ROI of your VM program.

- Document reasons for making a new relationship with the vendor.

- Remember - it is a give and take process – the process is needed for everybody to feel like they have arrived at win-win deal.

Tips Review (cont’t)

- Be consistent when classifying vendors, have clear definitions and make sure each vendor owner treat them the same.

- Remember - Rate the Risk but do something about it

Agenda Vendor Classification

- The Importance of the Classification Step
- Step 1: Review your Vendor Management Policy
- Step 2: Create Consistent Classification Levels
- Step 3: Classification Definitions
- Step 4: Audit Trail
- Common Questions

Why are classifications important?

- Helps you understand your inherent risk.
- The more critical vendors you have the more time you will spend later in the process.

Step 1 VM Policy

Review your Vendor Management Policy

- Ensure your VM policy helps define your VM classification.

Tip 1: Keep your policy focused on what you will do, not how you will do it.

Step 2 Classification Levels

Create consistent levels of classification

- 3 Levels
  - Level 1: Critical
  - Level 2: Significant
  - Level 3: Non-Essential

Step 3 Classification Definitions

Create consistent definitions for each of the six categories

1. Financial Impact

- Would the vendor failure cause a major impact to your Revenue or Expenses?

2. Information Sharing

- Does the vendor have access to or store non-public customer data?

Step 3 (con't)

3. Cost

- How much money do you spend each year with the vendor?

Tip 2: Audit yourself, pull the top 10 vendors from Accounts payable and ensure they are covered in your VM program.

4. Operational Impact

- Would the vendor failure cause a critical disruption to your operations or customer service?

Step 3 (con't)

5. Third Party Reliance

- Does the vendor market your services, or are you heavily reliant upon a third party vendor to provide your products?

Tip 3: Integrate your VM classification process with your BC program's BIA (Business Impact Analysis)

6. Transactional (risk of fraud)

- Does the vendor play an instrumental role in member/customer transactions?

Step 3 (con’t)

- Other categories to think about:
  - Reputation
  - Legal/Liability
  - Confidentiality/Integrity
  - Regulatory
  - Member/Customer Satisfaction
  - Competitive Advantage

Tip 4: Be consistent when classifying vendors. Have clear definitions and make sure each vendor owner treats them the same.

Step 4 Audit Trail

- Who?
- When?
- Review Annually

Six Common Questions

1. What do we do with government entities?
2. What if different vendor owners classify the same vendor differently?
3. What do we do with vendors that we pay but we don’t have contracts with?
4. How do we handle vendors that provide us multiple products?
5. What should trigger a review of the classification rating?
6. Should we make classification ratings automatically calculated?

Tips Review

1. Keep your policy focused on what you will do, not how you will do it.

2. Audit yourself, pull the top 10 vendors from Accounts payable and ensure they are covered in your VM program.

3. Integrate your VM classification process with your BC program's BIA (Business Impact Analysis)

4. Be consistent when classifying vendors, have clear definitions and make sure each vendor owner treat them the same.

Due Diligence

- Oversight vs. Due Diligence
- When to Perform Due Diligence
- 9 Areas to Review
- Common Questions

Oversight vs. Due Diligence

- Oversight - Ongoing review of vendors
- Due Diligence – Done once before contract signing

When to Perform Due Diligence

- New Vendors –Before contract signing

- Critical –Annually
- Signification- Every other year
- Non-Essential – On contract renewal

- Tip: Scale the review

1. Business changes/strategic plan

Key Question:

- *“Do you know how the vendor makes money?”*

Documents:

- Mission statement / strategic plan

Public Sources:

- Analysts opinions

Analyze:

- Changes to business model and technology.

2. Financials (D&B if needed)

Key Question:

- *"Is the vendor going bankrupt?"*

Documents:

- Financials

Public Sources:

- D&B
- SEC

Analyze:

- Debt vs. Capital
- Market Share
- Trend

3. Legal

Key Question:

- *“Are we getting our money’s worth?”*
- *“How is the insurance for the vendor?”*

Documents:

- SLAs
- Contract Terms
- Insurance Certificate

Public Sources:

- None

Analyze:

- Customer service
- Satisfaction

4. Regulatory/Compliance

Key Question:

- *"Are they complying with all regulations?"*

Documents:

- Audit Findings /Opinions

Public Sources:

- New laws

Analyze:

- Proposed laws
- Operating rules

5. Dependencies

Key Question:

- *"Who else are we doing business with?"*

Documents:

- Vendor Management
- Info Sec policy

Public Sources:

- None

Analyze:

- Access to data
- Third parties

6. Human Resources

Key Question:

- *“How do they treat their employees?”*
- *“Are they performing background checks and who are they hiring?*

Documents:

- Training
- Support process

Public Sources:

- Senior management changes

Analyze:

- Attrition
- Employee capabilities

7. Information Security / Privacy

Key Question:

- *"How safe is my data?"*

Documents:

- SSAE16
- Incident Response
- Penetration/Vulnerability results

Public Sources:

- Privacy policy

Analyze:

- History of incidents
- Where the data resides
- Results of tests

8. Reputation

Key Question:

- *"Are you happy with the vendor?"*

Documents:

- Complaints
- Reference checks (new vendors)

Public Sources:

- User groups
- Blogs
- News articles

Analyze:

- Renewal rates

9. Business Continuity

Key Question:

- *“If the worst happens, will the vendor be there to serve us?”*

Documents:

- BC Plan
- Exercise results

Public Sources:

- History of service

Analyze:

- RTO vs RT
- RPO vs RP

10. Cloud Computing

Key Question: How and where is my data being stored?

Documents:

Third party (data center) policies

Data center BC/DR plans

SSAE 16

Public Sources: None

Analyze:

Cloud Service Model Type

Deployment Model

Data center outsourcing process

Common Questions:

- How good/important is Dunn and Bradstreet data?
- What if a vendor won’t share their financials?
- How often should a DD review be performed?
- Who in the organization should perform the DD review?
- What about cloud vendors?
- Do we have to do DD on our significant vendors every year?

Risk Assessment

- Purpose
- Risk Management Terms
- Calculating Risk
- 8 Common Angles of a Vendor Risk Assessment
- So you have calculated a risk rating… now what?
- Common Questions

Purpose

- Boil all of the Due Diligence information down into a single risk rating.

Putting Vendor Management in Risk Management terms

- Classification = Inherent/Raw Risk
- Due Diligence = Controls
- Risk Assessment = Residual Risk

Calculating Risk

- Risk = Likelihood x Impact

- **Likelihood** is based on the information you learned during the Due Diligence review.

- **Impact** is based on how your organization utilizes the vendor.

8 Common Angles for Vendor Risk Assessments:

1. Financial
2. Legal/Liability
3. Operations/Transactions
4. Regulatory Compliance
5. Market/Dependencies
6. Information Security
7. Reputation
8. Business Continuity

1. Financial:

- Impact Considerations:
  - If the vendor fails, what’s the impact on my: Revenue, Expenses, Interest Rate, Liquidity, Credit etc…
- Likelihood Considerations:
  - Now, based on the vendor’s own financials what is the likelihood of that happening?

2. Legal/Liability

- Impact Considerations:
  - Where does the liability sit?
  - Is it contractually limited to the some party's insurance policy?

- Likelihood Considerations:
  - Can we get sued if the vendor does/doesn't do something?

3. Operations/Transactions

- Considerations:
  - What is the complexity and value of the vendor’s service?

- Likelihood Considerations:
  - What is the volume and threat of fraud?

4. Regulatory Compliance

- Impact Considerations:
  - Would your organization be subject to fines?

- Likelihood Considerations:
  - How is the vendor’s compliance program?

5. Market/Dependencies

- Considerations:
    - Could other vendor’s provide the service?

- Likelihood Considerations:
    - How many parties are involved in the delivery of the service?

6. Information Security

- Impact Considerations:
  - What type of data does the vendor have access to?

- Likelihood Considerations:
  - What did the DD review tell you about the vendor’s internal Information Security program?

7. Reputation

- Impact Considerations:
  - Would the vendor’s mistake or failure adversely affect our member/customer’s / the public’s view of the organization?

- Likelihood Considerations:
  - Has the vendor or it’s competitors failed in the past?

8. Business Continuity

- Impact Considerations:
  - If the vendor is harmed by a natural disaster, how does that affect you?

- Likelihood Considerations:
  - Does the vendor’s RTO/RPO align with your business continuity plans?

So you have calculated risk rating… now what?

- DO SOMETHING ABOUT IT!
  - Accept it
  - Mitigate it
  - Insure against it

Common Questions

1. Who should be involved in the risk assessment?
2. How does this risk assessment integrate with our overall ERM program?
3. How long does it typically take to do a risk assessment?
4. How often should a risk assessment be performed?
5. Should risk assessments be scaled based on vendor criticality?

Preparing for a VM Audit

- Know your audience
- Audit Area 1: Vendor Management Policy
- Audit Area 2: Vendor Management Program/Process
- Audit Area 4: Classification
- Audit Area 5: Due Diligence
- Audit Area 6: Risk Assessment
- Audit Area 7: Performance and contract review
- Self Audit

Know Your Audience

- Review past audit findings/recommendations
- Review the regulations and ensure you are up-to-date with all changes

Audit Area 1: VM Policy

- Provide: Current location of VM policy
- Explain: Approval process
- Prove: Date of last review and approval

Audit Area 2: VM Program/Process

- Provide: VM Program RACI (Responsible, Accountable, Contributor, Informed)
- Explain: Program timeline
- Prove: Current status

Audit Area 3: Vendor Inventory

- Provide: List of critical vendors

- Explain: Which vendors make it on your vendor list.

- Prove: Consistent on-boarding process

Audit Area 4: Classification

- Provide: Classification definitions
- Explain: Defend your classifications
- Prove: Who was involved in your classification process.

Audit Area 5: Due Diligence

- Provide: Past 3 years of Due Diligence history
- Explain: Who reviews the documents received from vendors
- Prove: What documents were requested and/or received from vendors

Audit Area 6: Risk Assessment

- Provide: Vendor Risk Assessments performed in the last year
- Explain: How vendors were risk rated
- Prove: Approval and Mitigation plans for your vendors

Audit Area 7: Performance and Contract Review

- Provide: Inventory of contracts

- Explain How contract dates are managed

- Prove: Consistent contract negotiation process

Self Audit

1. Accounts Payable vs. Vendor List
2. Business Continuity Plan vs. Vendor List
3. SSAE16s for every vendor that has member/customer data?
4. Acceptance or mitigation plan for high risk vendors

Common questions:

- How good/important is Dunn and Bradstreet data?
- What if a vendor won’t share their financials?
- How often should a DD review be performed?
- Who in the organization should complete the DD review?
- What about cloud vendors?

Contact Us

- Web: www.quantivate.com
  - Sign up for a demo

- Phone: 800-296-2416

- Email:
  - Info@quantivate.com
  - sales@quantivate.com