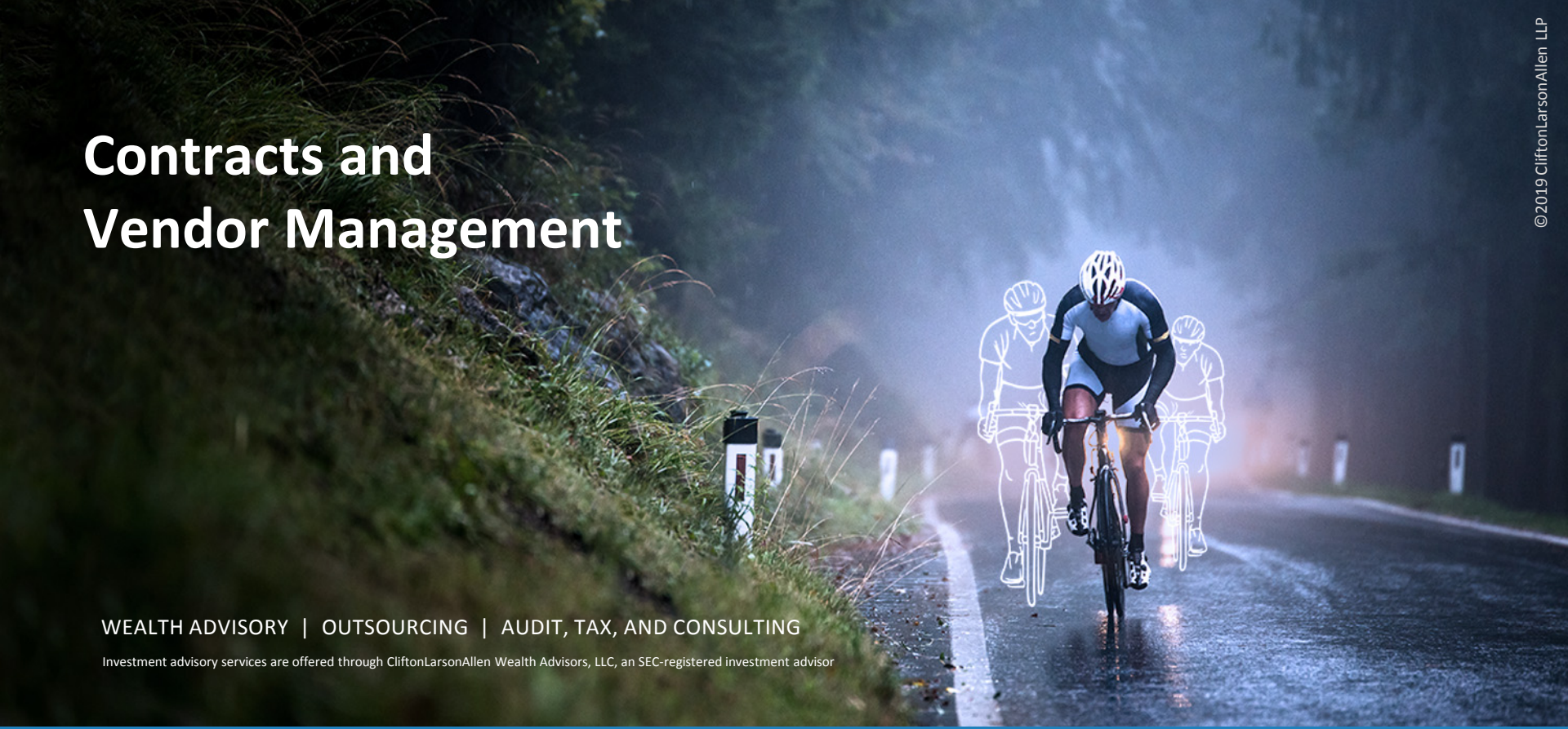
Contracts and Vendor Management



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Discussion Objectives

1. Identify risk factors related to third party service providers and vendors throughout your organization.

2. Contractual requirements to look out for and consider for your vendors.

3. Implementing a mature vendor management process throughout your organization.

4. Identify what risks are present when managing vendor contracts.

Vendors vs Third Party Service Providers vs Subcontractors

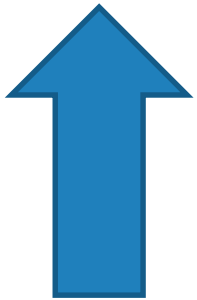
- Vendor – “a business that sells a particular type of product”
- Third Party – “a person other than the principals”
- Subcontractor – “a contract between a party to an original contract and a third party”
- IIA defines as External Business Relationships (EBR)

No Organization is an Island

Why Manage Third Parties?

Risks

- Data Breaches
- Vendor Access
- Organizational Cost
- Vendor Bankruptcy
- Compliance/Legal
- Business Continuity
- Financial
- Reputation



Opportunities

- Security
- Efficiencies
- Organizational Savings
- Compliance/Legal
- Availability
- Competitive Advantages
- Growth/Savings

Third Party Breach Examples

- Okaloosa County Water and Sewer
  - Breach of debit/credit card data occurred outside of the county's bill payment system at third party
  - https://www.securelink.com/blog/hackers-target-government-agencies-through-third-party-security-vulnerabilities/
- Atrium Health
  - The largest healthcare data breach of 2018 was caused by a hack on billing vendor AccuDoc Solutions
  - https://healthitsecurity.com/news/2.65m-atrium-health-patient-records-breached-in-third-party-vendor-hack
- 'Cryptojackers' Hit Government Websites
  - Attacker targeted the Browsealoud product, an accessibility tool that websites use to make it easier for people who are blind
  - https://www.govtech.com/security/Cryptojackers-Hit-Government-Websites-A-New-Flavor-of-Hacking-Courtesy-of-Third-Party-Code.html
- Ransomware Cyberattacks Knock Baltimore's City Services Offline
  - Government emails are down, payments to city departments can't be made online and real estate transactions can't be processed.
  - https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline

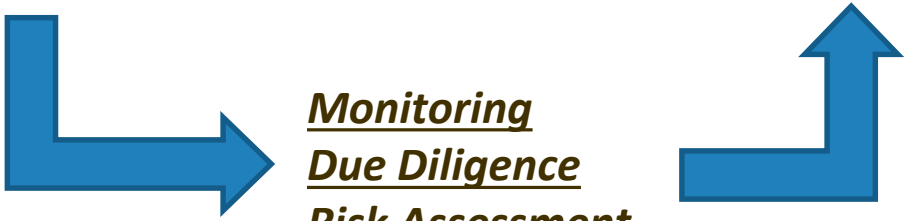
Vendor Relationship Lifecycle

On-Boarding

1. RFP (Request for Proposal)
2. Due Diligence/Risk Assessment
3. Vendor Selection
4. Contract Review
5. Contract Negotiation
6. Contract Execution

Off-Boarding

1. Contract Term Date
2. Auto-renewals
3. Notice of Termination Requirements
4. Return or Destroy Data
5. Remove any Access (Physical and Electronic)



Monitoring
Due Diligence
Risk Assessment

Due Diligence/Risk Assessment

- History
  - Existence and corporate history;
  - Mergers and acquisitions;
  - Strategy and **reputation**;
- Financial
  - Financial status, including reviews of **audited** financial statements;
  - **Insurance** coverage; and
- Compliance
  - Legal and regulatory compliance including any complaints, **litigation**, or regulatory actions;
  - HIPAA, OCC, NCUA, State and Federal Laws
  - PCI, Red Flags (Identity Theft), and many others depending on industry.

Due Diligence/Risk Assessment

- Security
  - Technology and systems architecture;
  - **Internal controls** environment, security history, and audit coverage;
  - Data storage/Encryption
  - Need for **access** to network and data
  - Ability to meet disaster recovery and business **continuity** requirements.
- Qualifications/Experience
  - Qualifications, backgrounds, and reputations of company principals, including criminal **background checks** where appropriate;
  - Other companies using similar services from the provider that may be contacted for **reference**;
  - Service delivery capability, status, and **effectiveness**;
- Geography
  - Location to your organization
  - Footprint of third party
  - International locations for data storage

Due Diligence/Risk Assessment

- How to use a SOC report to gain insight into a potential vendor:
  - If the vendor is processing any data or storing any data on your behalf – request a SOC report.
  - Look for “carve-outs” to determine what they are outsourcing.
    - May need to request additional SOC reports.
    - Example: Managed IT solutions outsourcing their Data center
  - Determine the period covered (Type 1, Type 2)
  - Make sure your specific service is covered.
    - ASPs have many software solutions but may not include them all in their SOC report

Vendor Contracts

Contract Review Considerations

- **Performance Clauses**
- Protection Clauses
- Scope
- Subcontractors
- Duration
- Fees
- **Right to Audit**
- Compliance
- **Confidentiality and Security**
- **Business Continuity**
- Insurance
- Warranties
- Indemnification
- Modification
- **Termination**

Performance Clauses

- Service Level Agreements / Key Performance Indicators
  - Example: Vendor will achieve and maintain a customer satisfaction rating of not less than 75% each calendar quarter
- Availability
  - Example: Product/service will be fully functional not less than 98% per day/month/quarter excluding standard maintenance periods
- Reporting
  - Outline all reports needed from vendor.
  - Include type and frequency of reports needed (performance, security, business continuity, etc.) and specific information to be included.
- Compensation
  - Damages for failure to meet SLAs usually are in the form of a % credit of fees with right to terminate for repeated failures.

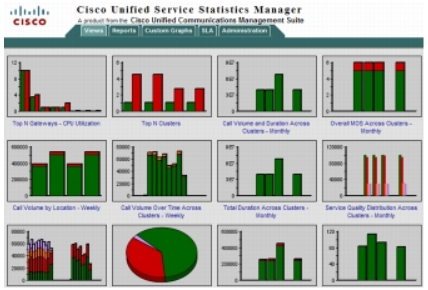
Performance Clause Reporting

– Vendor will achieve and maintain a customer satisfaction rating of not less than 75% each calendar quarter.

Define:

- Measurements
  - Based on customer survey only
  - 75% satisfied
  - 1 – 5 Rating but 3 is still satisfied
- Reporting Period
  - Calendar Quarter
  - When do you report by?
- Reliability of Report
  - Ability to verify data

- Report Type
  - Dash Board
  - Annual BCP Test
  - Breaches/Incident
  - Presentation/Formal Report



Right to Audit

Allows party (or third party agents) to audit company information/records to test internal controls or prove compliance with contract terms.

Considerations:

- Overly broad property/information access language.
  - Define: Number of audits in a specific period without cause (i.e. not more than once annually),
  - Audit schedule (i.e. during company's normal business hours) and scope of audit.
  - Access to data and personnel.
- Who pays for cost of audit? Who approves the auditor?
- Termination upon negative result.
- SOC Reporting vs. Right to Audit

Confidentiality and Security

- **Standard Requirements:** Prohibit disclosure or using certain company information except as necessary to perform pursuant to the contract.

  Example: Healthcare companies selling HIPAA data.

- **Standard exceptions**:
  - Previously known/becomes publicly available without breach
  - Developed independently
  - Provided by a third party without restriction

Confidentiality and Security

- **Specific Considerations:**
  - **Return or destroy** confidential information upon termination of contract or other designated time.
  - Adequate security within **industry standards** and not less than used to protect own confidential information.
  - Require **prompt** notification and **full disclosure** of security breaches of confidential information or that will affect company or its customers.
  - Specify necessary corrective action.

Confidentiality and Security

- **Specific Considerations:**
  - Vendor Access
    - Full time access or as needed
    - Specific users or generic account
    - Predefined termination of access
    - Monitoring activity

Confidentiality and Security

- **Security Metrics and Standards**
  - Annual SOC reporting
  - HITRUST Certification
  - ISO 27001
  - Request all reporting from NCUA, OCC, SEC, examinations

Business Continuity

- **Specific Considerations:**
  - Back-up and protection plan in case of disaster or other extraordinary event that prevents use of primary/standard systems.
  - Vendor should provide copy of plan. Updated and tested regularly. Provide results.
  - Include business recovery time frames and other metrics.

Business Continuity

- Consider interdependencies among all service providers:
  - Requirements for vendor to participate in your own business continuity plan and test.
  - Who will pay for their time?
  - Vendor contact information and phone tree.

Contract Termination

Considerations:

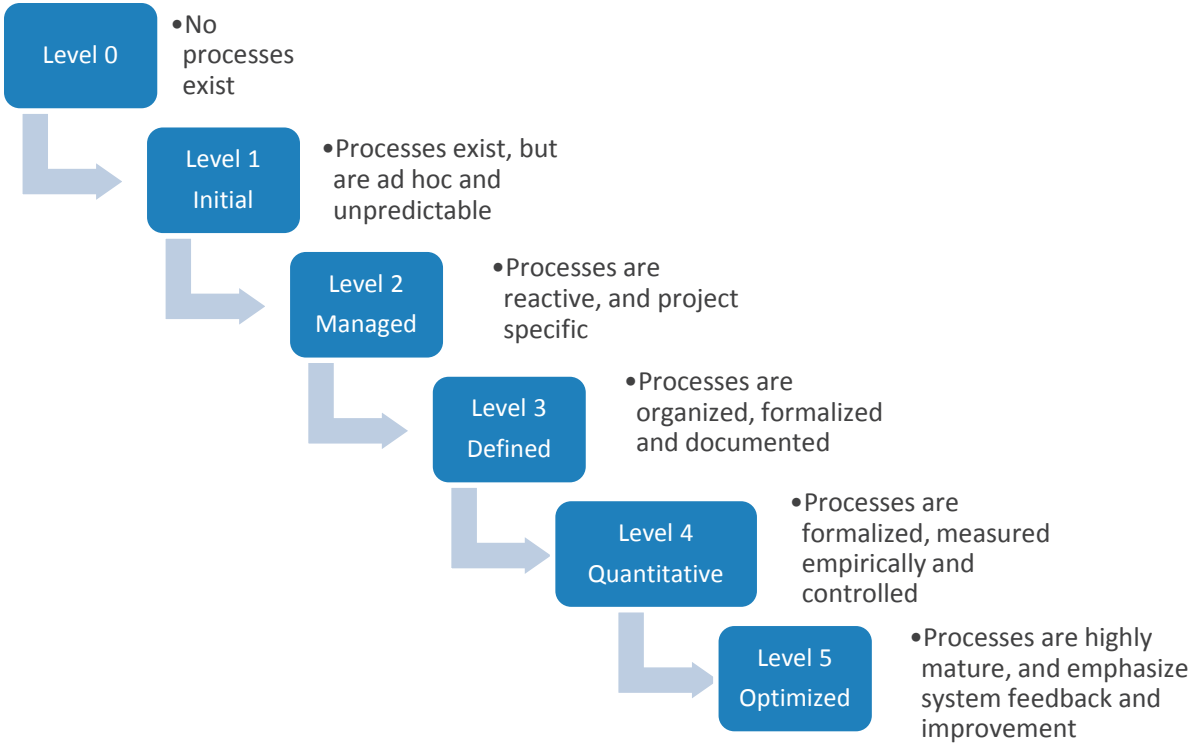
- Who has the right to terminate the contract?
  - You? The vendor? A third party?
- How much notice needs to be provided to terminate prior to completion?
- Define the contract termination date.
- Look out for auto-renewals.
- Ensure continuation of products/services during any dispute period.

Contract Termination

- Data considerations:
  - What data does the vendor have?
  - How can I ensure they provide 100% of it back or destroy 100% of it.
  - Do they have backups of my data at an offsite location?
  - Is there an additional fee to get my data back if I terminate the contract early?

Vendor Management Program

Vendor Management Maturity Model



Vendor Management Considerations

- Implement a cost effective solution for your organization.
  - You may only need to be at a level 3 based on risks.
- Start with “low-hanging fruit” when in early stages.
  - Organization wide Vendor Management Policy.
  - **Not just in IT**
- Executive Support
- Integration with ERM, Internal Audit, Compliance, and Legal.

Vendor Management Considerations

- Ensuring each outsourcing relationship supports the institution's overall requirements and strategic plans;
- Ensuring the institution has sufficient expertise to oversee and manage the relationship;
- Evaluating prospective providers based on the scope and criticality of outsourced services;
- Tailoring the enterprise-wide, service provider monitoring program based on initial and ongoing risk assessments of outsourced services; and
- Notifying its primary regulator regarding outsourced relationships, when required by that regulator.

Where does Vendor Management Live?

- Legal
- Information Technology
- Department Responsibility
- Vendor Management Department
- Internal Audit

Periodic Vendor Risk Assessments

- Defining Critical Vendors
  - What risk factors is your organization most concerned about?
    - Size of Contract – Dollar and Scope
    - Impact on your organization
    - Data involved
    - Personnel involved
    - Compliance

Periodic Vendor Risk Assessments

- Updating due diligence documentation
  - History
  - Financial
  - Compliance
  - Security
  - Geography

- Review Contract Language for Compliance
- Assessing changes to the scope of services

Internal Audit Role in Vendor Management

Considerations:

- Ensure consistent contracting process
- Evaluate due diligence process
- Executing right to audit clause
- Evaluate periodic Vendor Risk Assessments
- Review of SLAs and Metrics
- NOT deciding on vendors for management

Risk Areas:

- Fictitious vendors
- Fictitious, inflated and / or duplicate invoices
- Conflicts of interest
- Kickbacks
- Bid-rigging
- Audit AP transactions against Vendor List

Compliance with Regulations

Financial Services

- Federal Financial Institutions Examination Council (FFIEC)
  - Cybersecurity Assessment Tool – Domain 4 External Dependency Management
- Gramm Leach Bliley Act (GLBA)
  - Section 501B

Healthcare

- HIPAA- HITECH: 164.308(b)(1)
  - Administrative safeguards covered by the BAA

5 Key Lessons

1. Trust no one
2. Inventory and risk rank vendors
3. Always negotiate
4. This is a team sport
5. Right to audit

References

- https://www.privacyandsecurityforum.com/wp-content/uploads/2015/10/25092-Privacy-and-Data-Security-Breach.pdf
- http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/service-provider-selection/due-diligence.aspx
- http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/board-and-management-responsibilities.aspx
- https://www.isaca.org/chapters5/Cincinnati/Events/Documents/Past%20Presentations/2014/Third%20Party%20Risk%20Management.pptx

Thank you!

CLAconnect.com

Phil Del Bello, CPA, CISA
Manager
CLA, Specialty Advisory Services
Phillip.Delbello@CLAConnect.com
410-308-8181

Scott Carbee
Deputy Chief Information Security Officer
State of Vermont, Agency of Digital Services
Scott.Carbee@vermont.gov
802-828-0911