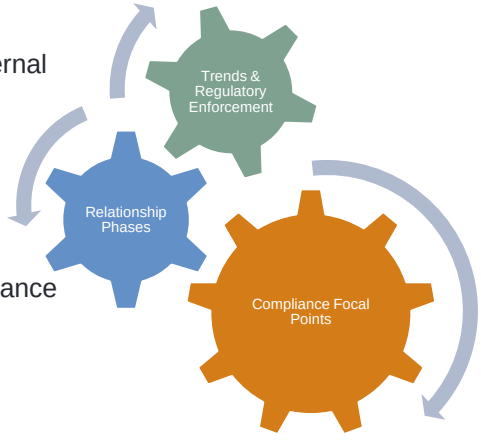
Internal Audit and Managing Third Party Risk

Presented By:
Tim Lietz – Regional Practice Director - Risk Advisory Services

Monday, October 08, 2018

Our Time Today

- Third Party Vendor Management – Current Trends
- Why Organizations Leverage External Resources
- Phases of Each Relationship
  - Evaluate Options
  - Negotiate Agreement
  - Monitor Service Level Performance
- Case Study Examples
- Focal Points for Your Organization



Third Party Relationships – Current Trends

What we're seeing from the regulators

- OCC's Semiannual Risk Perspective
  - Elevated Operational Risk Level is expected to continue; with Reliance on Third Party Service Providers increasing
  - Concentration areas of reliance on third parties could lead to single points of failure without effective oversight
- OCC Bulletin 2017-7: Third-Party Relationships: Supplemental Examination Procedures
  - Assess the institution's Quantity of Risk
  - Assess the institution's Quality of Risk Management

Our Unique Perspective

Kaleidoscope of clients

- Industry: Financial Services, Manufacturing, Government, Not-for-Profit, Insurance, Healthcare, SaaS, Automotive
- Size: Revenues to Head-Count
- Internal Audit Department Footprints
- Regulatory Requirements

What We Are Seeing – 2018

- OCC & Fed – Increased focal points
- CEB – Top 10 Audit Plan Hot Spots of 2018
- Large Carolinas financial services client – 4 people on site performing vendor audits
- Large regulated client – assistance in developing vendor management program and completion of annual audits
- FSI Exchange Conference – hot topic of 2 day event – Sept 2018

What We Are Seeing

25th year of the Top Technology Initiatives Survey
American Institute of CPAs®

United States	Canada
1. Securing the IT environment	1. Securing the IT environment
2. Managing and retaining data	2. Managing and retaining data
3. Managing IT risk and compliance	3. Managing IT risk and compliance
4. Ensuring privacy	4. Ensuring privacy
5. Enabling decision support and analytics	5. Enabling decision support and analytics
6. Managing System Implementations	6. Managing System Implementations
7. Preventing and responding to computer fraud	7. Preventing and responding to computer fraud
8. Governing and managing IT investment/spending	8. Governing and managing IT investment/spending
9. Leveraging emerging technologies	9. Leveraging emerging technologies
10. Managing vendors and service providers	10. Managing vendors and service providers

- 25th Anniversary North American Top Technology Initiatives Survey Results

Recent Trends

- **42%** of companies now describe themselves as highly vulnerable to vendor, supplier, or procurement fraud
  - Kroll Global Fraud Survey
- A current survey indicates that **85%** of companies recently suffered at least one supply chain disruption
  – Zurich Financial Survey
- **90%** of all FCPA cases involved third-party intermediaries – organizations need to evaluate their understanding of and compliance with statutes such as the FCPA and UK Bribery Act.
  - Corporate Executive Board

Recent Trends - continued

- **Facilitation Payments** – 3rd parties must follow your company's policy – The Biebs Example
- 3rd party service providers handling customer credit card data – storing, processing and transmitting, customer card data
- **COSO 2013 Compliance** – controls over outsourced service providers are a big focal point today. In the past, SOC reviews seemed sufficient, but now more in depth review of controls and monitoring activities are required. Formal, documented controls are being implemented.

Recent Trends - continued

- Controls over information going to/from third parties. More formalization required.
- Increased complexity of supply chains and "opacity" of individual links. Cumulative risk of multiple weaknesses.

- Increased business leader accountability for third-party relationships and risks to business.
- Russia Sanction Compliance – most complex sanctions ever for businesses, especially in energy. OFAC compliance – are your business partners compliant?

Recent Trends - continued

- Vendor Risk Management is definitely getting more attention and demanding maturity
- Executive Boards and Audit Committees regard cybersecurity as a key risk, but maybe not as it relates to VRM!
- Metrics matter – how does your company measure, monitor and report on its vendor footprint?
- VRM – There's always room for improvement

Polling Question

Polling Question 1:

What percentage of companies with FCPA violations are related to 3rd Party activities/transactions?

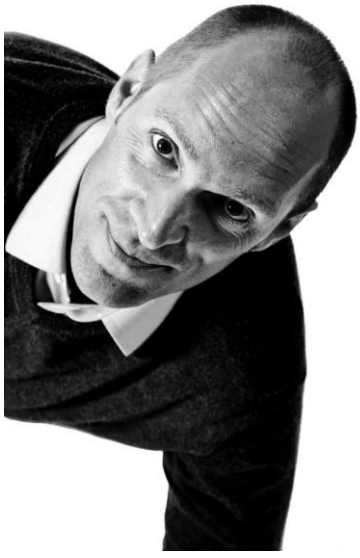
A. 30%
B. 48%
C. 70%
D. 90%

Why Organizations Leverage External Resources

Duke University/CFO Magazine Outlook Survey

Top 10 Concerns for U.S. Businesses

1. Economic Uncertainty
2. Cost of benefits
3. **Attracting and retaining qualified employees**
4. Regulatory requirements
5. Government policy
6. Weak demand for product/services
7. Data Security
8. Employee productivity
9. Employee morale
10. Access to capital



By 2020, there will be

123 million

high-skill, high-pay jobs available in the U.S., but only

50 million

Americans with the right education to fill them.

Economist Intelligence Unit

Workplace "Out of" Balance

Cut costs
Leaner Operations
People for Technology

Knowledge Management
Engagement
Productivity
Innovation
Flexibility

Top 5 Reasons Organizations Outsource

75%	• Reduce & Control Operating Costs
65%	• Focus on Core Competencies
59%	• No Available Internal Resources
52%	• Reduce Internal Headcount
51%	• Reallocate Internal Resources for Higher Value Purposes

Top 5 Functions Outsourced

69%	• Information Technology (all categories)
29%	• Operations & Administration
26%	• Customer Service
21%	• Other
20%	• Financial (Payroll, etc.)

Reliance on Vendors and the Regulatory Impact

Regulators acknowledge the risks associated with vendor relationships and have demanded that leaders monitor and take responsibility for the actions of their vendors through various laws and standards:

- Sarbanes Oxley Act
- Gramm-Leach-Bliley Act
- FCPA
- Health Insurance Portability and Accountability Act,
- Payment Card Industry Data Security Standard (PCI DSS)
- CFPB guidance

Consequently, vendor management is currently at the forefront of organizational risk management priorities.

Polling Question

Polling Question 2:

What is the number 1 function outsourced by organizations today?

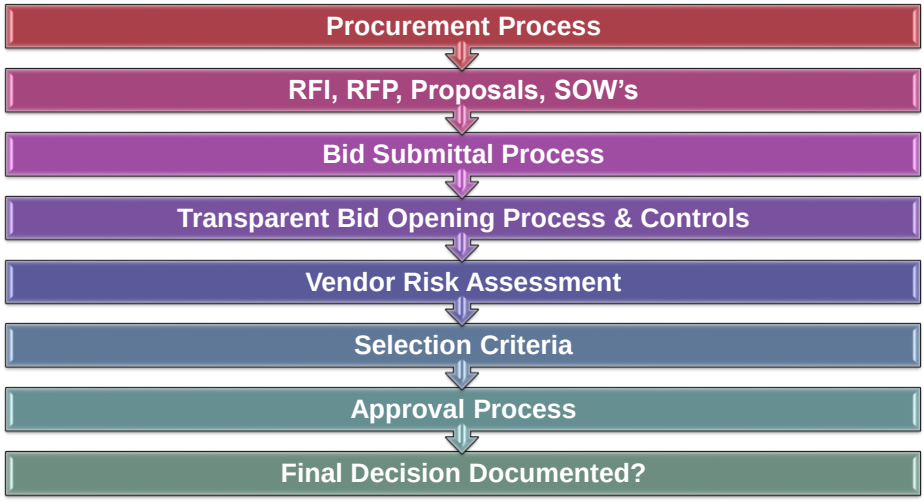
A. Finance
B. Human Resources
C. IT
D. Legal

Phases of the Vendor Relationship

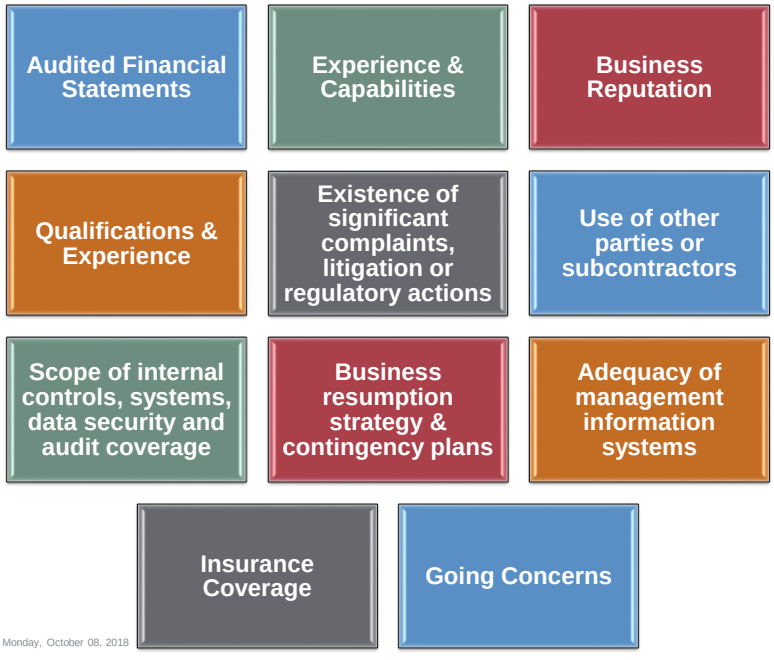
Phases of the Relationship

- Evaluate Options / Vendor Risk Assessment
- Negotiate, Contract & Onboard
- Service Level Monitoring

Evaluate Options



Vendor Risk Assessment



Negotiating and Managing Vendor Contracts

- Centralized?
- Trained Negotiators?
- Legal Department ALWAYS Involved?
- Delegation of Authority Verified PRIOR to Execution? Business Owner?
- Contract Repository? Review Frequency?
- Access to Repository Limited?

Content of the Contract

- Scope
- Cost / Compensation
- Business Reputation
- Performance Standards / SLA
- Management Information Reports
- Right to Audit
- Confidentiality & Security
- Business Resumption and Contingency Plans
- Default & Termination
- Dispute Resolution
- Indemnification

Contract Structuring & Review – The Obvious

- Management should ensure that the specific expectations and obligations of both parties are outlined in a written contract prior to entering into the arrangement.
- Board approval should be obtained prior to entering into any significant third-party arrangements.
- Legal counsel should review significant contracts prior to finalization.

Oversight of Third-Party Activities

- Management should periodically review the Third party's operations to verify that they are consistent with the terms of the written agreement and that risks are being controlled.
- Management should consider designating a specific officer to coordinate the oversight activities with respect to significant relationships and, as necessary, involve other operational areas (audit, IT) in the monitoring process.
- An effective oversight program will generally include the monitoring of the third party's quality of service, risk management practices, applicable internal controls and reports.

Monitor Performance – Questions to Ask

- **Monitoring adherence** to the agreement – Who performs?
- **Annual scoring of performance** – Are there documented performance statistics for each vendor where appropriate? Who/How scores? Are performance scores shared internally?
- **Renewal process** – How is it coordinated between procurement and process or business owners?

Polling Question

Polling Question 3:

What wording should always be included in executed contracts?

A. Indemnification
B. Right to Audit
C. Dispute Resolution
D. Business Reputation

Case Studies

Regulatory Enforcements

- Cadbury Limited/Mondelez International - The global snacking business agreed to pay a $13 million penalty for FCPA violations occurring after Mondelez (then Kraft Foods Inc.) acquired Cadbury and its subsidiaries, including one in India that proceeded to make illicit payments to obtain government licenses and approvals for a chocolate factory in Baddi.

- Anheuser-Busch - The Belgium-based global brewery agreed to pay $6 million to settle charges that it violated the FCPA by using third-party sales promoters to make improper payments to government officials in India and chilled a whistleblower who reported the misconduct.

Regulatory Enforcements

- **Consulting Firm** – Edward Snowden Incident (Booze Allen) – released top secret info to Wikileaks
- **Layne Christensen**
  - $5.1 million dollar FCPA fine for paying bribes in Africa during the 2000's.
  - Improper payments to government officials over a 5 year period.
  - Series of payments, *often made by third parties*, made under the guise of "cost of doing business".

Lessons Learned

- Vendor management has become a core competency
- Increased need for Vendor Risk Management program beginning with an inventory and risk assessment –
- Companies need monitoring processes for on going vendor performance as part of the overall VRM program
- **Be Proactive!**

Focal Points – Managing Increased Oversight of Vendors and Adding Value

Vendor Management – A Growing Trend

- Issued guidance has been around for years, yet implementation and impact on operations continue to grow.
- Some vendors have indicated that since 2012, the number of audits of their operations have quadrupled.
- Companies have reported growing areas of inquiry & oversight (i.e. PCI, SOC).
- Increased regulatory focus on a vendor's operational compliance.
- Primary responsibility lies with the organization managing the vendor relationship.

Coping with the Onslaught of Review Requirements

The increased frequency of audits, together with the rise in scope, can be daunting for both risk managers and their vendors.

Do you have Right to Audit Vendors? Do Vendors have the right to audit you?

Solution – Vendor Risk Management Program!

Pre-2013 Areas of Audit of a Vendor

Sampling of vendor questionnaires from pre-2013. Typical areas of inquiry included:

- Basic vendor information
  - Tax identification number
  - State of Organization
  - Business Type
- Financial Information
- Professional licenses
- Insurance Coverage
- Privacy policy/confidentiality of data
- Business continuity

2018 Areas of Audit

- **Business information**
  - Licensing
  - Financial
  - Management
  - Employee qualifications
  - Litigation
  - Regulatory actions
  - Ownership of products
  - System development lifecycles
- **Security**
  - Network
  - Physical
  - Application
  - Hardware
  - Access control
  - Identity access management
- **Privacy/GLBA/PCI**
- **Operations**
  - Polices and procedures
  - Change management
  - Consumer complaints

- **Risk Management**
  - Enterprise risk management program
  - Insurance risk management
  - Information risk management
  - Vendor risk management
- **Compliance**
  - Policies – mine and yours
  - Procedures – mine and yours
  - Applicable laws
  - Records retention
  - Training
  - SOC Attestation
- **Business Continuity Planning**
  - Disaster recovery
  - Pandemic plan
- **Diversity, Environment, Reputation – Corporate Culture**

Compliance Management: Planning

- Be educated. Whether you are the reviewer or the subject, you must:
  - Know your client/vendor
  - Understand the services
  - Understand your business, including the regulatory oversight
  - Understand your contract
    - Scope of audit provisions
    - Compliance obligations
- Plan in advance:
  - Are the limits to the disclosure of my information? Why?
  - Are there materials available only for onsite review? Why?
  - Are there materials that can be provided in advance?
  - Who grants exceptions?

Audit Preparation

- Create a library of commonly asked questions (data room)
  - Collect data on commonly asked questions and create acceptable answers in advance
- Set review periods of library to prevent stale answers
  - Employee Handbook – annual
  - Litigation – monthly or quarterly
- Create collateral that can be provided on predictable topics
  - Privacy policy
  - Disaster recovery
  - Records retention

Audit: Execution

Examiners/Auditors

- Set expectations of team members
- Appoint a team lead/project manager
- Define roles
- Require remediation plans

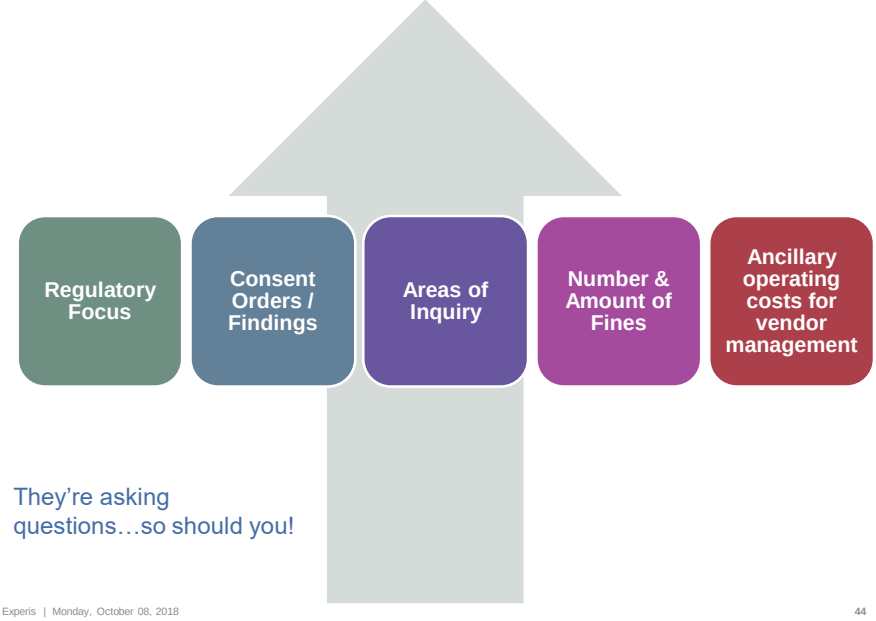
Vendors

- Dedicate a team for managing inquiries
- Centralize communication
- Use standard responses
- Manage timeline
- Build client trust and relationships
- Gather data and spot trends

Audit: Post Mortem

- Save your work!
  - Identify focus areas for next review
  - Reduce time needed to respond to ongoing requests
  - Create collateral for regulatory compliance exam
- Track and communicate results internally
- Act on noted issues
  - Terminate or reduce use of problem vendors
- Test remediation efforts
  - Follow up and request proof of completed remediation
  - Test

VRM is no longer just nice to have….



They're asking questions…so should you!

Lessons Learned

- **Transparency** – a must from start to finish with each vendor!
  - December 2015 IIA Magazine – "The Importance of Auditing for Conflicts of Interest"
  - Hotline Reporting Number on RFP's?
- **Consistency** – centralized or decentralized environment?
- **Control Environment** - strong or weak?
  - Evaluate the process of monitoring vendor performance

Gaming the System, Ethical Dilemmas or Fraud?

- Inflated "Rack Rates" vs. final "Negotiated Rates" – increased annual bonus tied to cost savings
- CFO Request – split into separate SOW's to prevent Board Approval
- Inappropriate Relationships -- $25 million telecomm cabling contract & dual invoicing
- International Locations – further from the Corporate Office, the likelihood for fraud increases.

Theme: One person was involved..no VRM process!

Lessons Learned

- FCPA & UK Bribery Act Compliance
  - payments made through 3rd Parties
  - FCPA fines related to bribes made through third parties
- Right to Audit Clause
- Financial Stability
- Sole Source Providers
- SOC Report Availability
- Background and Drug Screening
- PC & Internet access – start & finish of project (ours vs theirs)
- Equipment and Badges – monitoring them
- Building Access – too liberal? Audit visitor badges!
- Data Access and Retention Policies – do vendors comply?

Polling Question

Polling Question 4:

What is a certain red flag/high risk situation while negotiating, executing and renewing large dollar contracts?

A. No Review by Legal
B. Single Individual Involved
C. Negotiation Not Done
D. Vendor Performance Not Monitored
E. All of the Above

Control Focal Points

Third-Party Governance Review

Ensure internal procedures regarding the use of third parties are comprehensive and consistently applied. These should cover processes, such as due diligence, contract management, and relationship termination.

Audit Rights Review

Look through contracts to see whether audit rights are included over third-party vendors. As contracts are renegotiated and new relationships are formed, ensure a right to audit clause is included.

- *CEB 2016 Audit Plan Hot Spots*

Control Focal Points – cont'd

Due Diligence in Selecting Third-Party Relationships:

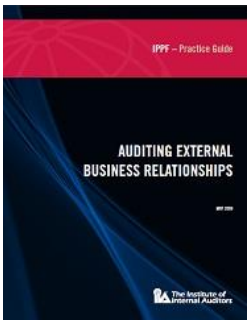
Assess due diligence process used to select vendors and other partners, including an examination of the third parties' internal control environment, security history, legal compliance (including complaints, litigation, and regulatory actions), and financial status.

Supply Chain Management Health Check:

Review whether risk management is appropriately integrated into supply chain management—cutting across individual parts, such as procurement, logistics and distribution—and includes a focus on lower likelihood but higher impact risks, such as business continuity, currency crises, and commodity volatility.

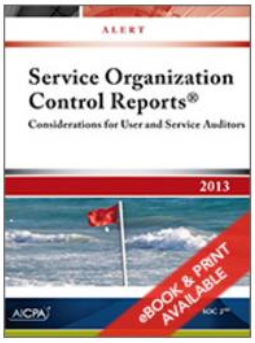
- *CEB 2016 Audit Plan Hot Spots*

Resources



CSCMP's Supply Chain [QUARTERLY]

CEB Procurement Strategy Council®



Contact Info

Tim Lietz
Director Risk Advisory Services
Experis Finance
Timothy.Lietz@experis.com
919-838-7859