Managing Third Party Risk

Presenters:
Lori Daniels – Engagement Manager – Risk Advisory Services
Tim Lietz – Regional Practice Leader – Risk Advisory Services

Tuesday, January 12, 2016
Our Time Today

• Third Party Vendor Management – Current Trends and Program Management
• Why Organizations Leverage External Resources
• Phases of Each Relationship
  – Evaluate Options
  – Negotiate Agreement
  – Monitor Service Level Performance
• Case Study Examples
• Internal Audit Focal Points – How to Add Value to Your Organization
Our Unique Perspective – Best Practices in Procurement
2015 – A FULL Perspective

- 441 meetings completed
- 22,439 miles driven
- 250 meals on the road
- 63 nights in a hotel
- 20 flights
- 11 train rides
- 1 Harley Ride to Key West!
What We Are Seeing – 1Q 2016

- OCC & Fed – Increased focal points
- Large Carolinas financial services client – 3 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 2015
- Great opportunity for Internal Audit to add value to the organization
What We Are Seeing – 1Q 2016

• **Large NC Client:**
  - Centralized procurement process is key
  - Existing or NEW vendor?
  - NEW: risk assessment is critical on how to manage inherent risks
  - Data security key
  - Get MSA and onboarding process cleared ahead of time to make new vendor onboarding easy
  - ID risks ahead of time with new vendors
  - OCC focal point in Oct. that produced finding
What We Are Seeing – 1Q 2016
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 out to third parties and controls over info coming back in from them. Need to be more formalized now.
• Increased complexity of supply chains and “Opacity” of individual links. Organizations are not seeing the cumulative effect of weaknesses within a supply chain.
• Business leader accountability is increasing to know the third parties they utilize and their effect on the organization.
• Russia Sanction Compliance – most complex sanctions ever for businesses, especially in energy. OFAC compliance – are your business partners compliant?
Why Organizations Leverage External Resources
Duke University/CFO Magazine Outlook Survey

- Two-thirds of firms expect to increase employment in 2016, with the increase averaging about 2 percent.
- Employment growth will be strongest in services/consulting, retail/wholesale and construction.
- Manufacturing employment should shrink 1 percent.
- Manufacturing firms will reduce fulltime employment in 2016.
- CFOs list the difficulty in attracting and retaining qualified employees as one of their top three overall business concerns.
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 Balance

- Cut costs
- Increase flexibility
- Enhance innovation

Knowledge management
- Engage
- Increase productivity
Top 5 Reasons Organizations Outsource

- **75%** Reduce and control operating costs
- **65%** Focus on core competencies
- **59%** Resources not available internally
- **52%** Reduce internal headcount
- **51%** Reallocate internal resources for higher value purposes
Top 5 Functions Outsourced

- **69%**: IT (all categories)
- **29%**: Operations and administration
- **26%**: Customer service
- **21%**: Other (wide variety)
- **20%**: Financial (payroll, etc.)
Reliance on Vendors and the Regulatory Roadmap

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

- Consequently, vendor management is currently at the forefront of organizational risk management priorities.
Phases of the Vendor Relationship
Phases of the Relationship

- Evaluate Options
- Manage and Negotiate Agreement
- Monitor Service Level Performance
Evaluate Options

- Procurement Process
- RFI, RFP, Proposals, SOW’s
- Bid Submittal Process
- Transparent Bid Opening Process & Controls
- Selection Criteria
- Due Diligence
- Final Decision Documented?
Due Diligence Review

- Audited Financial Statements
- Experience & Capabilities
- Business Reputation
- Qualifications & Experience
- Existence of significant complaints, litigation or regulatory actions
- Use of other parties or subcontractors
- Scope of internal controls, systems, data security and audit coverage
- Business resumption strategy & contingency plans
- Adequacy of management information systems
- Insurance Coverage
Negotiating and Managing Vendor Contracts

- Centralized?
- Trained Negotiators?
- Legal Department ALWAYS Involved?
- Delegation of Authority Verified PRIOR to Execution?
- Contract Repository?
- Access to Repository Limited?
Content of the Contract

- Scope
- Cost/Compensation
- Business Reputation
- Performance Standards/SLA’s
- 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 scores?

• **Renewal process** – How is it coordinated between procurement and process owners?
Case Studies
Regulatory Enforcements

**Large Retailer** – access gained through HVAC vendor

**Consulting Firm** - Edward Snowden Incident

**Large Retailer** – FCPA violations in Mexico

**Layne Christensen** – October 27, 2014
$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”.
Alleged Navy Shipyards Gunman

- 34 yr. old Military Contractor from Texas
- The Washington Naval Shipyards reportedly has over 3,000 civilian, military, and contract support personnel working in the building attacked by the gunman last November
- Location of shooting described as a “highly secure” military site
- Lapses suggested in security screening and Base protection, subsequent to the event
- Arrested in 2004 for shooting out tires of a car
- Security clearance granted in 2008
- Reported history of mental illness
Lessons Learned

• Vendor management has become a core competency

• Increased need for standardized vendor oversight

• Companies need monitoring processes for on going vendor performance
Audit Focal Points – Managing Increased Oversight of Vendors and Adding Value
Vendor Management Continues to be a Growing Area

The 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 and oversight.

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.
Pre-2013 Areas of Audit of a Vendor

From a 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
2015 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
  - Policies 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
- Business Continuity Planning
  - Disaster recovery
  - Pandemic plan
- Diversity, Environment, Reputation
2016 Viewpoint

There is a renewed focus within IA Departments to identify new areas to add value to their organization and reprioritize risks.

Top 10 Risks for Internal Audit in 2016:

- #2 – Operational Risk – Third Party Relationships
- #9 – Information Risk – Third Party Relationships

-2016 Pulse of Internal Audit CEB
Audit 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/Risk Assessments: Preparation

- Create a library of commonly asked questions
  - 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/Risk Assessments: Execution

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

For 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/Risk Assessments: 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….

• Increased regulatory focus
• Increasing number of consent orders and findings, even on past vendors
• Increasing areas of inquiry
• Increasing number and amount of fines
• Increased ancillary operating costs for vendor management
Focal Points for IA:

- **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.
Risk Focal Points

- FCPA & UK Bribery Act Compliance – payments made through 3rd Parties – numerous recent FCPA fines related to bribes made through third parties
- Right to Audit Clause
- Financial Stability
- Sole Source Providers
- Background and Drug Screening
Risk Focal Points

- PC & Internet access – start & finish of project
- Equipment and Badges – monitoring them
- Building Access – too liberal?
- Data Access and Retention Policies – do vendors comply?
2016 Audit Plan Additions?

**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.

**Due Diligence in Selecting Third-Party Relationships:** Assess the 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

CEB Procurement Strategy Council®
Contact Info

Lori Daniels
Engagement Manager
Experis Finance
lori.daniels@experis.com
919.755.5863

Tim Lietz
Director Risk Advisory Services
Experis Finance
timothy.lietz@experis.com
919.755.5859