SearchFinancialSecurity.com INFORMATION SECURITY FINANCIAL INFORMATION SECURITY DECISIONS

Vendor Management

Presented by:

Eric Holmquist
President
Holmquist Advisory, LLC
eric@holmquistadvisory.com
www.holmquistadvisory.com

Vendor Management is…

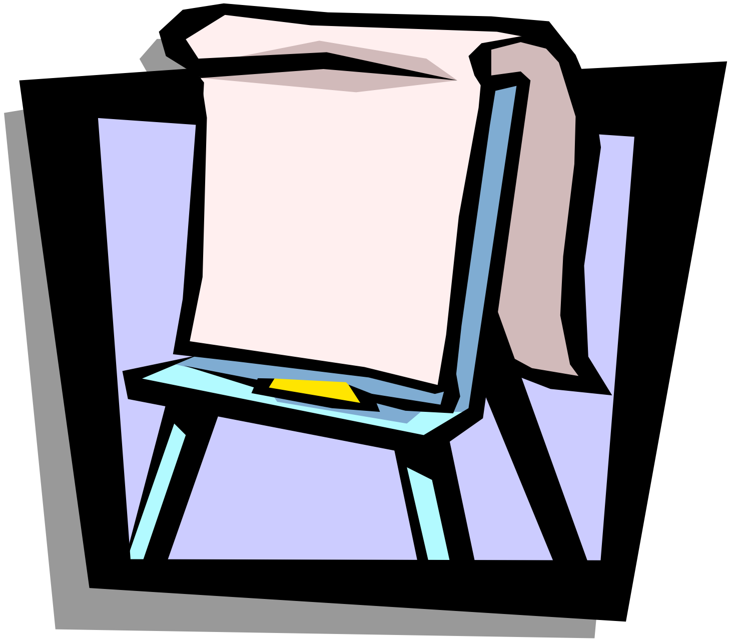
- Time consuming
- Messy
- Inexact
- Disruptive
- An infinite number of loose ends
- Answers that only lead to new questions
- At best, a marginal control
- **Absolutely critical**

As a subcomponent of Operational Risk Management, it’s all about…

- Awareness
- Accountability
- Actionability

Agenda

- Terms & conditions
- Governance
- Program components
- Due diligence
- Ratings
- Risk Assessment
- Final points
- Q & A



Terminology

- Third Party
  - Generic term for any external relationship
- Service Provider
  - Strictly, any provider of a service
- Third Party Service Provider
  - Regulatory phrase, company providing a key service
- Vendor
  - Company providing a product or minor service
- Partner/affiliate

For this presentation we’ll simply use “vendor”

Program Components

- Policies & procedures
- Standards
- Guidelines
- Training
- Clear accountability
- Processes for:
  - Identification
  - Due diligence – Initial
  - Due diligence – Ongoing
  - Monitoring and reporting
  - Termination

Third Party Identification

- Legal
  - Identified during contract review
- Strategic Approval Process
  - Identified during budgeting process
- Project Management Office
  - Identified during project scoping
- Accounts Payable
  - Identified during payment process

Governance

- Vendor Mgmt (procurement) Department
  - Valuable but not critical
- VM Coordinator
  - Extremely valuable – borderline critical
- Vendor Relationship Manager
  - Extremely critical
- Subject matter experts
  - Extremely critical
- Vendor Management Committee
- Board, senior and executive management

Subject Matters Experts

- Business area (operational aspects)
- Risk Management
- Internal Audit
- Information & Physical Security
- Business Continuity Planning / Disaster Recovery
- Legal
- Compliance
- Finance
- Facilities
- Regulators
- External experts

New Third Parties

- Initial profiling
- Definition
- Due diligence
- Risk assessments
- Acceptance
- Approval
- Execution
- Monitoring

Due Diligence

- Company demographics
- Contract
- Process flows
- Impacted policies and procedures
- Operations
- Financial statements
- Internal controls
- Insurance coverage
- BCP / DR
- Regulatory oversight
- OFAC checks
- Information access/control
- Technical requirements
- Training requirements
- External data sources
- Reference checks
- Interviews
- Site visit

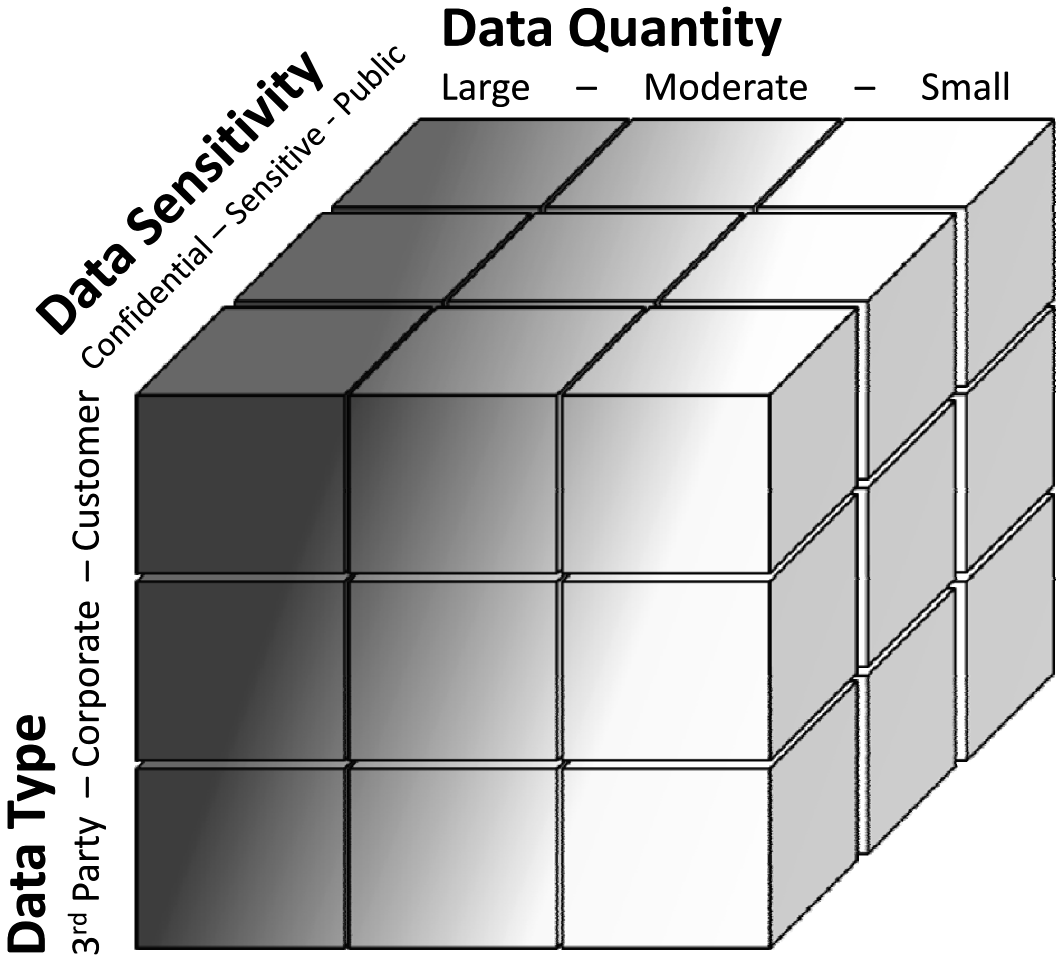
Information Security

- Information Type
  - Customer/applicant
  - Corporate
  - Third party
- Information Sensitivity
  - Confidential
  - Sensitive
  - Public

- Quantity
  - Large
  - Moderate
  - Small

Should match internal data classification standards

Information Security


Data Quantity
Large – Moderate – Small
Data Sensitivity
Confidential – Sensitive - Public
Data Type
3rd Party – Corporate – Customer

Information Security

- What data (classified)?
- Where will it be physically?
- How and who accessing?
- Breach notification
- Data destruction
- Ongoing communication mechanism?
- Integrates with info security risk assessment
- PCI compliance?

Ratings

- Classification (contract)
  - Critical (or key), Important, Standard
- Business criticality (contract)
  - Need, specialization, exclusivity, etc.
- Availability (contract)
  - Uptime, availability, fault tolerance, etc.
- Risk Ratings (company)
  - Financial
  - Operational (Info sec, BCP, service/delivery, concentration)
  - Legal, Compliance
  - Reputation
  - Regulatory

Risk Assessment

- Completed prior to execution, then annually
- Only rating specific to company not contract
- Simply stated, “What could go wrong?”
- Consider implementation + operating risk
- Accept that the relationship manager is biased
- Intended to establish a risk profile
- Risk profile must be accepted by business

Ongoing Oversight

- Monitoring
- Cycle-based due diligence
- Updated risk assessments
- Incident response process
- Testing
- Audits
- Change management
- Board & senior management reporting

Keys to Success

- **Communication!**
- Clear expectations
- Clear responsibilities
- Honesty
- Cross disciplinary involvement
- Ultimately, the degree to which the organization takes the process seriously, thoughtfully and timely

Final Thoughts

- Outsourcing service does not outsource risk
- Be clear about what is centralized versus what resides with relationship managers
- If you can’t clearly articulate the business need you aren’t ready to contact candidates
- Attestations are meant for recourse not proof
- Trust but verify
- All companies have skeletons in their closet
- This is a relationship, treat it like one

Questions