THIRD PARTY (VENDOR) SECURITY RISK MANAGEMENT

KLC™ CONSULTING

About Kyle Lai

- Kyle Lai, CIPP/G/US, CISSP, CISA, CSSLP, BSI Cert. ISO 27001 LA
- President of KLC Consulting, Inc.
- Over 20 years in IT and Security
  - Security Assessment, Network and Application Security
  - Third Party Security Risk Assessment / Management
  - Information Assurance and Regulatory Compliance
- Past Experience includes consulting for DoD, NIH, VA, RBS, Boeing, CIGNA, HP/EDS, PWC, RBS, Major Financial Institutions, and Fortune 1000 firms
- Author of the security software - SMAC MAC Address Changer, WebDAV Scan

KLC CONSULTING

Typical Vendor Experience

KLC CONSULTING

Overview of Vendor Security Concerns & Risk

KLC CONSULTING

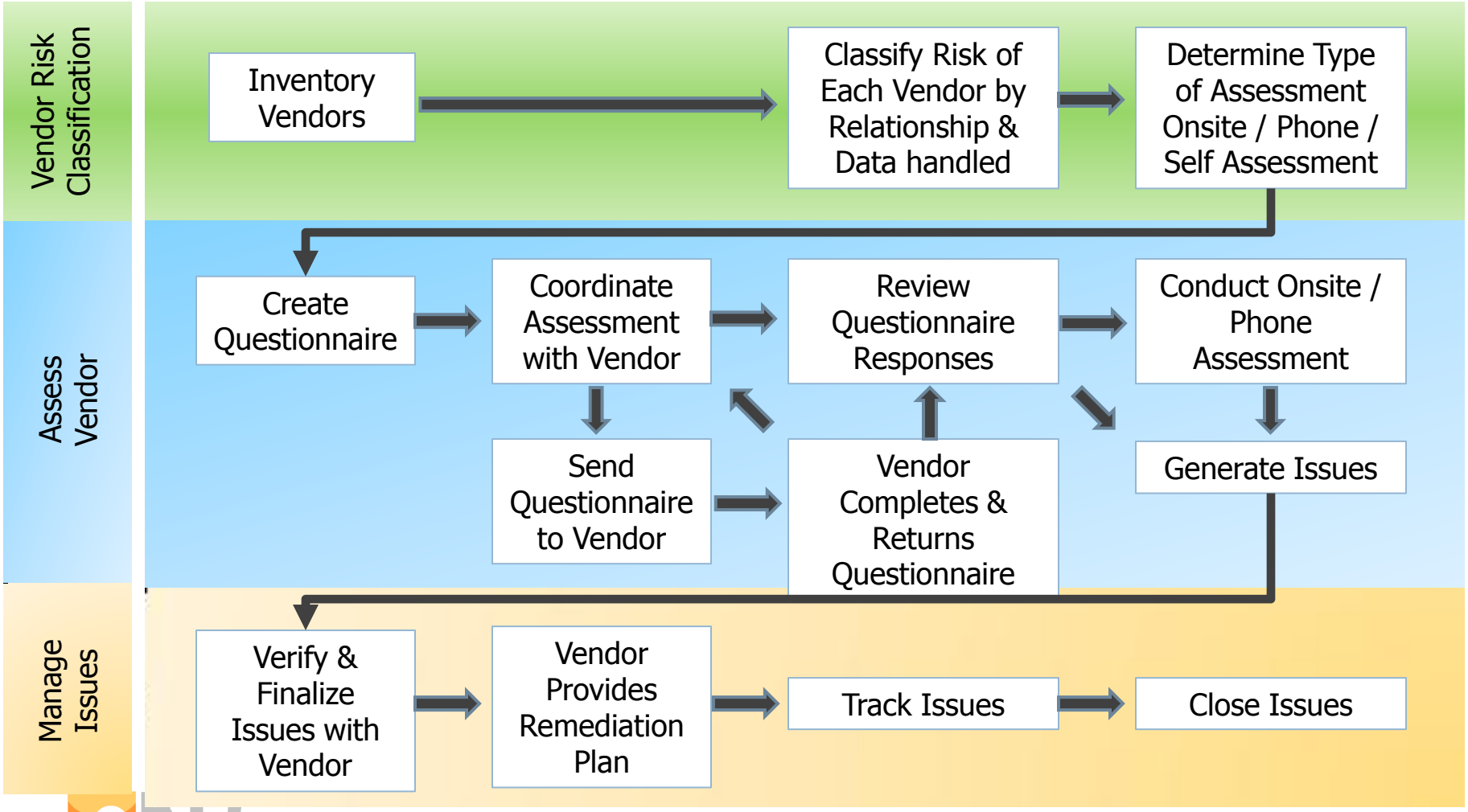
Why is Vendor Security Management Important?

- Outsourcing to a 3rd party vendor does not mean you are off the hook
- Do you know who has your data?
- Do you know how secure your data is with your 3rd party vendor?
- Will you know if there is a security breach at your 3rd party vendor?
- If you need to be meet regulatory compliance, are your vendors meeting the same level of compliance requirement?

- ❑ FFIEC
- ❑ PCI
- ❑ GLBA
- ❑ FISMA / DIACAP
- ❑ SOX
- ❑ HIPAA / HITECH

KLC CONSULTING

Vendor Security Management Process



KLC CONSULTING

Vendor Security Management Program

- How many vendors in total?
- How many reviews can you complete in a year?
- How to classify vendor security risk based on data classification?
- What vendor gets onsite vs. phone assessments?
- What is the baseline framework (ISO 27002, SIG, GLBA, HIPAA…)?
- What baseline questions to include in the questionnaire?
- How will the vendor responses be documented?
- What results make a vendor High, Medium or Low Risk?
- How to address and track issues raised? **Exception Process?**
- What tool should I use to manage Vendor Security Program?
- What reports should be generated to track vendor security risks?

Dealing with Vendors

- Define roles and responsibilities
  - Internal Vendor Relationship Manager
  - Internal Program/Project Manager
  - Internal Vendor Security Assessor
  - Vendor's Contact
- When should the Vendor Security Assessor engage the vendor?
- What is the process to schedule an assessment?
- How much lead time should be given to complete the questionnaire?
- **How much time do you spend assessing the vendor?**
  - What is the right level of security assessment?
  - Do you / Can you pull samples? (Do you have the Right To Audit)?
- What is the escalation process if a vendor is NOT COOPERATING?

KLC CONSULTING

Managing Issues

- What tool will you use to track issues?
- Where will you store the issues?
- How do you efficiently generate management report?
- What is the **allowed timeframe** for vendor to address Critical, High, Medium and Low risk issues?
- What is the process for following up issue status?
- What is the process to close the issues?
- **What is the Risk Acceptance Process?**
  - Who has the authority to make the decision?
  - Can any findings that pose risk to regulatory compliance be accepted?

KLC CONSULTING

Some Common Findings with Vendors

- Lack of Mobile Device Security (Bring Your Own Device - **BYOD**)
- Lack of Cloud Computing Usage Policy and Standards
- Lack of USB Lockdown / Encryption
- Lack of Laptop Hard Drive Encryption
- **Lack of Local Administrator Privilege Lockdown**
- Lack of regular vulnerability testing or penetration testing (Continuous Monitoring)
- Lack of Incident Response Management Policy and Procedures

KLC CONSULTING

Top Concerns from Program Mgr, CISO and COO
(Financial, Healthcare, Consulting, Software and Energy sectors)

1. Cloud Computing Service Providers
2. Contract Compliance (meet security req, get notified when using a new 4th party)
3. 4th (+) parties service providers
4. Mobil Device Security Management (mobile apps, BYOD)
5. Regulatory Compliance Program (true level of compliance)
6. Data Destruction / Return after termination (Who, what, when, where, how, Cloud?)
7. Continuous Monitoring / Assessment (vuln scan, penetration test)
8. Incident Response Management Program (maturity, client notification process)
9. Appropriately handling of the regulatory changes and the regulator's expectation
10. Availability
11. Balancing risk, effort, and area of focus on the follow-up assessment

KLC CONSULTING

Regulatory Authority's Expectations

- Will expect more every year or two years
- Expect proof of regulatory compliance from your 3rd party vendors
- Compliant (or in process) with new regulations, i.e. Dodd-Frank
- How do you improve the vendor security management program?
  - May expect more than just paper exercise
  - May expect you to conduct audit: Testing, i.e. sampling, evidence
- How do you manage the risk for the ultra high risk vendors?
  - Example:
    - 3rd party CRM firm may contain data sensitive to stock trading
    - 401K / Retirement benefit management firm

KLC CONSULTING

Case Study 1

Scenario:

- A large Bank conducting general banking and mortgage underwriting
- Issued a Cease and Desist order from OCC due to inadequate Third Party Service Provider Security Review Management Program
- 800+ vendors are in-scope for the security review
- 8 month deadline to develop an effective program, improve the process, assess the vendors
- Merger and Acquisition (M&A) activities are blocked by OCC until OCC approves the program

Action:

- Hired a consulting firm and assigned 30 consultants to assist with vendor security assessments
- Designed a vendor security review program and established processes to implement
- Quickly started executing the vendor security reviews

Results:

- Initial push back from some vendors on the depth of processes and security reviews
- Made significant improvements in processes and quality, and received OCC approval
- Able to continue with regular M&A activities

KLC CONSULTING

Case Study 2

Scenario:

- A firm offers off-site backup tape and document storage, cloud based backup services
- Very limited resources for the vendor security review program
- About 200+ vendors and increasing
- The firm does not process regulatory related transactions, but stores data for companies that are regulated

Action:

- Established a vendor security review program with defined processes
- Acquired GRC software, automated the vendor security questionnaire response process
- Automatically calculated the risk score for the vendor security questionnaire response
- Vendor Security Analyst identifies higher risk vendors and performs additional phone interviews. Also conduct on-site reviews with vendors as appropriate.

Results:

- Efficient, effective and automated vendor risk questionnaire response and risk calculation
- The program is effectively managed using limited resources

KLC CONSULTING

Other Items to Consider

- What Management Reports to generate?
- How to assess application development vendors?
- How do you assess vendors that are **outside of USA**?
- How about assessing vendors that are **no longer doing business with you** but have the obligation to store your data for 7 years?
- Before getting into security concerns, is the vendor financially stable?

KLC CONSULTING

Contact

Kyle Lai

KLC Consulting, Inc.

President

klai@KLCConsulting.net

www.klcconsulting.net

Linkedin Group:

Vendor Security Risk Management

KLC CONSULTING

Reference

- GLBA – FDIC Exam Procedures - http://www.fdic.gov/news/news/financial/2001/fil0168a.html
- Verizon Data Breach Investigation Report - http://www.verizonenterprise.com/DBIR
- Third-Party Presentation from OCC - http://www.occ.gov/static/past-conferences-and-seminars/edited-outsourcing-transcript-final-110404.pdf
- Cross-border outsourcing and Risk Management for banks - http://www.occ.gov/topics/bank-operations/bit/cross-border-outsourcing-risk-mgmt-for-banks.pdf
- Cloud Computing – Legal and Regulatory Issues: http://technet.microsoft.com/en-us/magazine/hh994647.aspx

KLC CONSULTING