THIRD PARTY (VENDOR) SECURITY RISK MANAGEMENT

IAPP KnowledgeNet Presentation

knowledge net

KLC™ CONSULTING

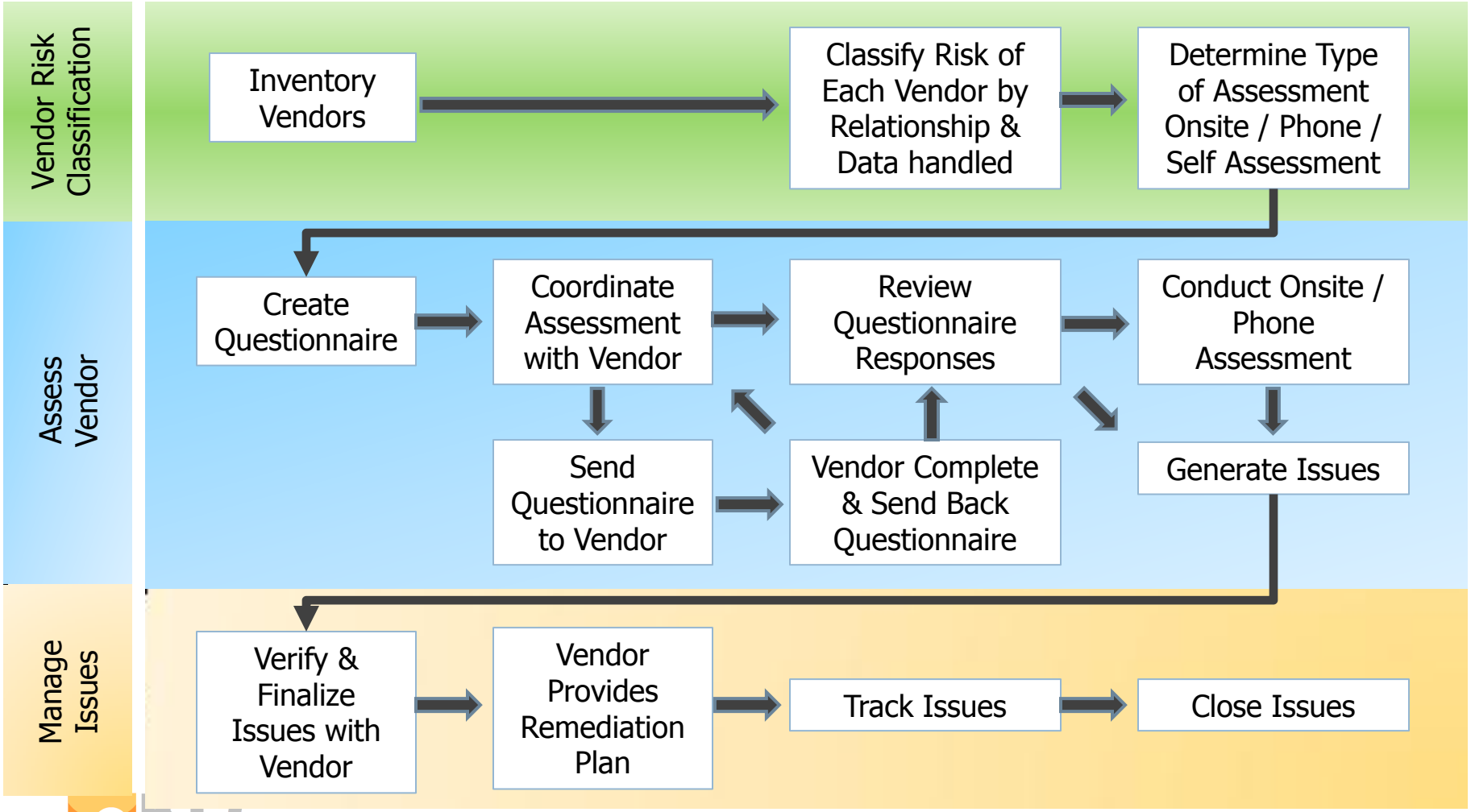
Boston, April 24, 2012

About Kyle Lai

- Kyle Lai, CIPP/G/US, CISSP, CISA, CSSLP, BSI Cert. ISO 27001 LA
- President and CTO of KLC Consulting, Inc.
- Over 20 years in IT and 15 years in Information Security
  - Security Assessment, Network and Application Security
  - Third Party Security Risk Assessment / Management
- Information Assurance Expert in Financial, Healthcare, and Federal Government sectors.
- Past Experience consulting for DoD, NIH, VA, RBS, Boeing, CIGNA, HP/EDS, PWC, Major Financial Institutions, and Fortune 1000
- Author of the security and privacy software, SMAC MAC Address Changer, with over 1.5 million users

KLC CONSULTING

KLC Vendor Security Management Process



KLC CONSULTING

Vendor Security Management Program

- How many reviews can you do a year with the assigned resources?
- How to classify vendor security risk based on data handled?
- What vendor gets onsite and phone assessments?
- What is the baseline framework (ISO 27002, GLBA, HIPAA, …)?
- What baseline questions to include in the questionnaire?
- How will the vendor responses get 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?

KLC CONSULTING

Tools to Help Manage Vendor Risk

Evolution of Tools in Medium to Large Organizations:

→

Vendor Security Risk Management System (**Data Collection**)

→

Vendor Security Risk Management System (**Automation**)

KLC CONSULTING

Dealing with Vendors

- Define roles and responsibilities
  - What should Vendor Relationship Manager do?
- When should Assessment Analyst engage the vendor?
- What is the process to schedule an assessment?
- How much lead time should you give to the vendor to fill out the questionnaire?
- How much time do you spend assessing the vendor - onsite and over the phone?
- **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 issue?
- **What is the Risk Acceptance Process???**

KLC CONSULTING

Other Items to Consider

- What Management Reports to generate?
- What about 4th parties?
- How to assess data center providers?
- How to assess **Cloud Service Providers**?
- How to assess application development vendors?
- How do you assess vendors that are **outside of USA**? What regulations to consider?
- How about assessing vendors that **no longer doing business with you** but have the obligation to store your data for 7 years?

KLC CONSULTING

Some Common Vendor Issues

- Lack of Mobile Device Security (Bring Your Own Device - **BYOD**)
- Lack of Cloud Computing Usage Policy and Standards
- Lack of USB Lockdown and/or Encryption
- Lack of Local Administrator Privilege Lockdown

- Upcoming – Lack of **IPv6** networking and security knowledge (Increasing IPv6 based attacks).

KLC CONSULTING

KLC Consulting, Inc.

- KLC is developing a Turn-Key Third Party Security Risk Management System on Process Unity platform, releasing in July, 2012.
- We are looking for a Pilot Testing firm
- Contact:
  - Kyle Lai, CIPP/G/US, CISSP, CSSLP, CISA
    President & CTO
    klai@klcconsulting.net
    617-314-9721 x168
  - Tarek El Heneidy
    Director of Operations
    tarek@klcconsulting.net
    617-314-9721 x138

KLC CONSULTING

Questions and Discussion

KLC CONSULTING