Third Party Due Diligence

SIFMA Technology Management Conference
June 2008

Jennifer L. Bayuk

jennifer@bayuk.com

www.bayuk.com

Privacy Scope Requirements

- GLBA
  - Reg S-P
- Franchise and Litigation Risk
  - State Breach Reporting
  - Settlement cases

- Holdings
- Order flow-pre-trade
- Executed and reported trades
- Unannounced M & A IB deal info, Other Investment Banking info
- Customer name, Customer email address, Customer mailing address
- Customer telephone number, Customer account number
- Customer SSN, TAX ID, or other government ID
- Customer authentication information (user name, password)

Integrity Scope Requirements

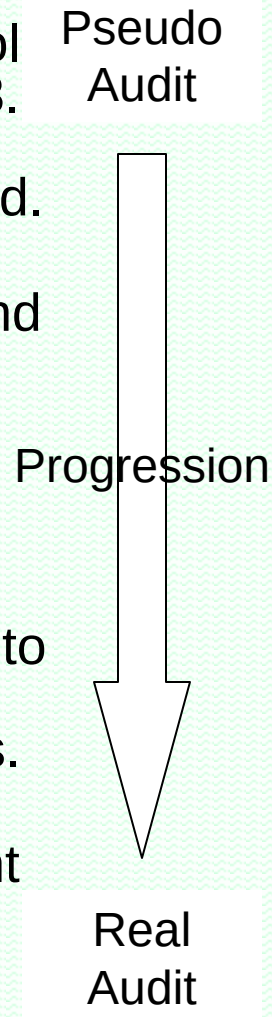
- Sarbanes Oxley
  - Data Integrity Requirements
- Vendor services commonly considered part of financial reporting are those that affect or include:
  - business transaction initiation, processing and reporting in accounting records, supporting information, and specific financial statement accounts.
  - methods for including the financial statement accounts in financial statements.
  - the financial reporting process used to prepare a firm's financial statements.
  - application functionality with respect to entitlement or financial statement calculation (e.g., applications service providers (ASPs)
  - technology hosting services for systems that develop, maintain, and/or operate management information systems activities that are associated with the above criteria.

Due Diligence Steps

1. Identify minimum amount of sensitive data which must be released to the vendor in order for the vendor to supply services.
2. Implement internal controls that ensure vendors do not receive any data other than that required to supply services and that data transfer process is secure.
3. Specify confidentiality, integrity, and availability requirements for that data at vendor site.
4. Identify the technical and operational control measures in place at the vendor which are designed to meet confidentiality, integrity, and availability requirements.
5. Map the technical measures identified in (4) to the requirements identified in (3).
6. Assess whether the vendor is capable of meeting requirements on a go forward basis.

Example Practices

A. Firm compiles a list of questions intended to identify control activity that would support requirements gathered in step 3. The vendor is asked to fill out the questionnaire. Where vendor answers do not match requirements, this is reported.
B. Same as Strategy A, but in addition, vendor is interviewed via telephone or email to explain questionnaire answers and provide evidence of alternative controls.
C. Same as Strategy A, but in addition, where vendors are considered high risk, firm performs visits to vendor site to verify answers to questions and clarify responses.
D. Firm reviews vendor data processing environment by charting path taken by data in scope. Vendor is requested to provide documented evidence of controls. Firms confirm understanding of vendor environment via phone interviews.
E. Same as Strategy D, but in addition, where vendors are considered high risk, firm performs or requires independent verification of controls, to include Internet scans, onsite audits, and/or reports of independent auditors.



Cost Comparison

Review Type		Hours	same* 100%	low - 80%	high 20%	Labor 100 revs	Tech	Travel	Total
A	Questionnaire	4	$700			$70,000	$50,000		$120,000
B	Questionnaire plus Documentation Review	20	$3,500			$350,000	$50,000		$400,000
C	Questionnaire plus Documentation Review Plus Onsite verification	4 - low risk 80- high risk		$700	$14,000	$336,000	$50,000	$40,000	$426,000
D	Data flow analysis plus Documentation Review	20	$3,500			$350,000	$60,000		$410,000
E	Data flow analysis plus Documentation Review plus verification options	20 - verify avail		$3,500	$3,500	$385,000	$60,000		$465,000
		40 – verify not avail for 50% of high risk			$7,000			$20,000	

*Assumes fully-loaded reviewer cost assumed at $175. **Assumes requirement to review 100 vendors annually

Vendor Self-Reviews

- BITS FISAP, a Financial Services Roundtable technology committee Financial Industry Shared Assessment Program, which defines a set of controls and encourages vendors to have themselves audited by them.
- ISO 27001 Certification, an evaluation with respect to the management practices in place at the vendor in comparison with the ISO security management standards.
- Moody's Vendor Risk Rating (VRR), the ratings agency's attempt to quantify risks with respect to a vendor operation based on a standard set of general IT controls.
- PCIS DSS reviews, wherein the vendor handling of credit card specific data is compared to the Payment Card Industry data security standards.
- SAS70s, an AICPA statement of accounting standard which is targeted at ensuring firm financial statements are not adversely impacted by vendor operations.

Evidence of Independence

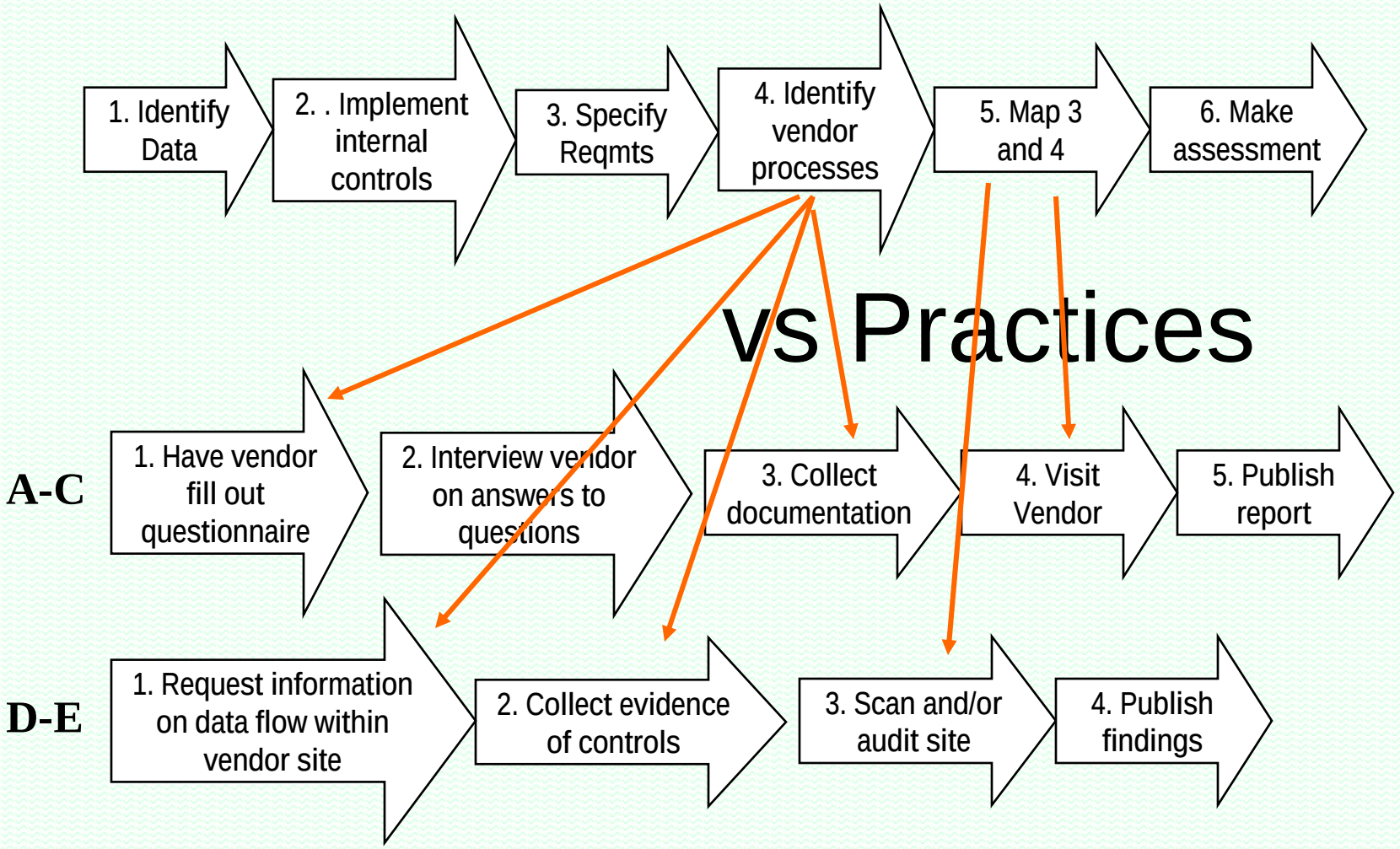
- Assessor faces material reputational risk or loss of certification for inaccurate results
- Assessor must keep technology control assessment workpapers
- Workpapers are available for authoritative review
- Assessor is paid by source other than vendor under review

Evidence: / Standard:	Assessor Risk	Workpapers Kept	Workpapers Available for review by	Assessor compensation model
BITS FISAP				
ISO 27001	X		ISO	
PCIS DSS	X	X	PCIS	
Moody's VRR	X	X		
SAS70	X	X	AICPA	

Scope Adequacy Measures

- A self-assessment report is just one piece of evidence
- Each firm must evaluate whether self-review covers scope of service and due diligence requirements

Requirements



(from slides 4 and 5)

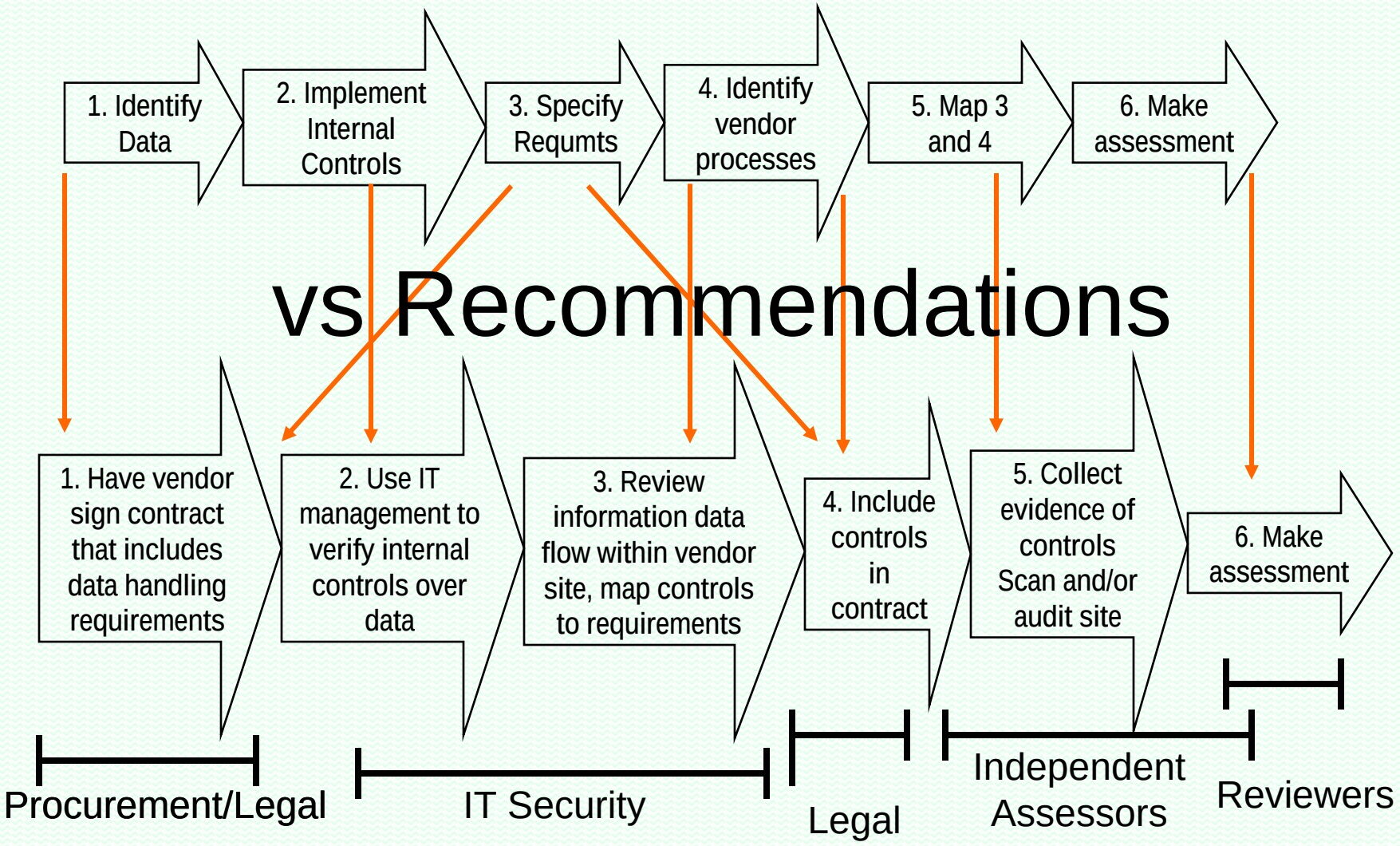
Root Cause Observations

- Security reviewers are ordering business managers to pay attention to risk reports rather than Business Managers ordering security reviews.
- Review team activities are dictated by consortiums of other industry review teams, not by firm management or consortiums of firm management.
- Due diligence requirements are rarely integrated with business
- Both vendors and large internal review organizations have a vested interest in having industry standard reviewer not subject to standards of independence.

Recommendations

- Business managers should control the vendor security review process via existing points of integration:
  - Procurement process should set vendor expectations. Use operations and compliance to validate requirements during contract review process.
  - IT management should verify that the vendor gets only the data they require and only gets it if control functions can be technically verified.
  - Legal should determine if IT Controls are required, and if so, put them in the contract. Audit clauses should also be included.
- Where requirements are contractual, *internal review teams should be enlisted to verify contractual requirements* are met. As a cost-saving effort, management may also set standards for reliance on independent audit services and document the reliance. This places management in the position of ordering security reviews and not visa versa.

Requirements



In Summary: Motivate Vendors

Rely on reasonably independent review if provided.

This will motivate vendors to get their own independent assessment in order to avoid customer audits.

When you need to review a vendor, use your best talent, *real auditors*, not checklists.

Discussion

jennifer@bayuk.com

www.bayuk.com