Feature

Vendor Due Diligence

Jennifer Bayuk, CISA, CISM, CGEIT, is an independent consultant on topics including information security policy, process, management and metrics. For 10 years she managed information security at a major Wall Street firm. She was the chief information security officer for the last six years of that tenure. Bayuk was also a manager of information systems internal audit at a different financial industry firm, a Big Four security principal consultant and auditor, and security software engineer at AT&T Bell Laboratories. Bayuk frequently publishes on information security and audit. She can be reached at *www.bayuk.com.*

First, consider the following scenario.

Last year at about this time, I was on a site evaluation team visiting a data center at a hosting service provider. Upon arrival, the members of the team stood in a conference room with the vendor sales executive, the head of operations at the center, and some of his high-level managers. They told us what we would be seeing on our tour. They described a state-of-the-art network, enormous storage capacity, caged servers with biometric security devices and service levels that were supported by highly skilled technicians.

At the end of this impressive overview, triumphant music filled the air and a previously inconspicuous curtain on the wall parted to reveal a balcony view of the network operations center. There were wall-to-wall screens with graphics depicting network routes, utilization statistics and red/yellow/green alerts. There were clusters of workstations in tiered semicircles facing the big screens, each with a sign hanging from the ceiling to identify its purpose. Included were server operations, network operations, data administration, performance monitoring, job control and others. The team stared quietly as the vendor staff beamed at the display.

My stare was in disbelief, first at the scene, then at the beaming staff, and then back. The cluster of workstations labeled "security operations" was empty. The screens showed red alarms and there was no one sitting in front of them. No one else noticed.

I had to mention it. "Why is there no one at the security station?" I asked.

The sales executive looked at the head of operations, who looked at his staff, who looked at each other. One of them finally stepped forward. "Administrators play multiple roles," he said, "and they stand up and walk around to man different workstations as tasks are necessary to be done in other areas."

Well, this did not ease my concern. "So then," I pressed, "who is logged in to each workstation? How do you maintain accountability for administrative activities where people are sharing terminals?"

The staff again exchanged looks before one answered the question. "They cannot really do much from these workstations; they are used mostly for monitoring." He said it with a finality that considered the subject closed. He smiled and led the gathering to the other side of the room to discuss the day's schedule. His attitude had quickly shifted from "see how great our operations center looks," to "pay no attention to the men behind the curtain."[1]

I was not doing an audit, or presumably the operation staff might have been concerned. The staff was not concerned, because they considered the event a sales call. Yet, I was there because of a requirement to perform due diligence on how vendors handle data.

REQUIREMENTS OF VENDOR DUE DILIGENCE

Where firms participate in any outsourcing arrangement whereby a third party is exposed to information that personally identifies individual customers, firms in the US are explicitly required under the Gramm-Leach-Bliley Act (GLBA) and the various regulations implementing GLBA to verify that personally identifiable information (PII) is safeguarded as a matter of due diligence before commencing the arrangement. Firms are also required to periodically (commonly construed to mean annually) repeat due diligence thereafter.

Where firms participate in outsourcing arrangements that do not include the handling of PII, but are known to expose other kinds of information that are required to be handled

confidentially, it would be prudent, and it is a growing industry practice, to apply the same due diligence. This is because a plethora of state privacy laws, as well as settlement cases, leave firms subject to franchise and litigation risk if other kinds of confidential information are compromised.

Examples of PII and other confidential information that typically create due diligence obligations if exposed to third parties are:

- Customer order flow
- Executed transactions
- Unannounced merger and acquisition information
- Customer name, customer e-mail address and customer mailing address
- Customer telephone number and customer account number
- Customer Social Security Number, tax ID or other government ID
- Customer authentication information (e.g., username, password)

There are requirements for due diligence information handling based on confidentiality or avoiding disclosure. In addition, firms may have requirements to perform due diligence with respect to vendor information handling for the purpose of financial reporting. Sarbanes-Oxley Act section 302 requires management to assess whether processes for generating financial statements are adequately controlled, i.e., are capable of consistently producing accurate information. Section 404 requires an external audit to report on the reliability of that management assessment. If vendor services are critical components of financial statement reporting, those services are also subject to management oversight, also known as due diligence. 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

Such are the requirements for performing something called due diligence, but what are the requirements for due diligence itself? Information systems audit and control practice standards vary widely from organization to organization, but vendor oversight of data handling due diligence requirements at a very high level are not too controversial. They are:

1. Identify the minimum amount of sensitive data that must be released to the vendor for the vendor to supply services.
2. Implement internal controls to ensure that vendors receive only data required to supply services and the data transfer process is secure.
3. Specify confidentiality, integrity and availability requirements for data at the vendor site.
4. Identify the technical and operational control measures in place at the vendor that are designed to meet confidentiality, integrity and availability requirements.
5. Map the technical measures identified in step 4 to the requirements identified in step 3.
6. Assess whether the vendor is capable of meeting requirements going forward.

VENDOR DUE DILIGENCE REVIEWS

These logistical requirements for due diligence have led to a wide variety of firm-specific third-party data-handling review processes. Many are motivated by GLBA and, therefore, concentrate on confidentiality as opposed to availability. Those motivated by Sarbanes-Oxley focus on integrity over confidentiality and availability. However the criteria for requirements are weighed, they generally follow an IT controls audit or a pseudo IT controls audit process.

Steps 1 and 2 are straightforward, but involve scrutiny of a firm's own controls rather than the vendor's. Step 3 is not as straightforward, but still may be done in isolation, as it involves interpretation of requirements. Actual scrutiny of vendors starts with step 4.

Having experience both in scrutinizing vendors and being scrutinized as a vendor, the author has seen a variety of methods by which firms conduct due diligence, and those basically conform to one of these scenarios:

A. The firm compiles a list of questions intended to identify control activity that would support requirements gathered in step 3. The vendor fills out the questionnaire. Where vendor answers do not match requirements, this is reported.

B. Same as strategy A, but in addition, the vendor is interviewed via telephone or e-mail to explain questionnaire answers and provide evidence of alternative controls.
C. Same as strategy A, but in addition, where vendors are considered high risk, the firm visits the vendor site to verify answers and clarify responses.
D. The firm reviews the vendor data processing environment by charting the path taken by data in scope. The vendor is requested to provide documented evidence of controls. The firm confirms its understanding of the vendor environment via phone interviews.
E. Same as strategy D, but in addition, where vendors are considered high risk, the firm performs or requires independent verification of controls, to include Internet scans, onsite audits and/or reports of independent auditors.

Scenarios A-D can be seen as a sequential flow from what was previously referred to as a "pseudo audit," which is scenario A, just asking questions and documenting the answers, through actual audit, where scope is considered, starting with scenario D, and maturing with scenario E. Every firm has its own comfort zone as to what level of due diligence is actually required.

However, what the firms have in common is redundancy. Where each vendor is audited separately by many clients, the cost of services increases uniformly for all. **Figure 1** considers what scenarios A-E cost for a firm that must perform due diligence on a set of 100 vendors annually. One could argue with the numbers, but no matter how the costs are estimated, it is obvious that, if each firm maintains its own program to review vendors, using any of the approaches in this table industrywide creates redundant work effort with respect to the overall goal of performing due diligence on securities industry vendors. Each vendor interview or visit requires the vendor to spend time on the due diligence activity and raises the cost of the vendor services for all customers.

In recognition of this excessive cost, several efforts have been undertaken by information systems control professionals over the years to come up with industry standards for vendor due diligence reviews, for example:

- Financial Institution Shared Assessment Program (FISAP), from BITS, a division of the Financial Services Roundtable, which defines a set of controls and encourages vendors to have themselves audited by them
- ISO 27001 attestation, an evaluation with respect to the management practices in place at the vendor in comparison with the International Organization for Standardization (ISO)'s security management standards
- Payment Card Industry (PCI) Data Security Standard (DSS) reviews, wherein the vendor handling of credit-card-specific data is compared to PCI DSS

Figure 1—Cost Comparison

Review Type		Hours	Same* 100%	Low 80%	High 20%	Labor 100 Reviews**	Technology	Travel	Total
A	Questionnaire	4	US $700			US $70,000	US $50,000		US $120,000
B	Questionnaire plus documentation review	20	US $3,500			US $350,000	US $50,000		US $400,000
C	Questionnaire plus documentation review plus onsite verification	4—low risk 80—high risk		US $700	US $14,000	US $336,000	US $50,000	US $40,000	US $426,000
D	Data flow analysis plus documentation review	20	US $3,500			US $350,000	US $60,000		US $410,000
E	Data flow analysis plus documentation review plus verification options	20—verify availability		US $3,500	US $3,500	US $385,000	US $60,000		US $465,000
		40—verify not available for 50% of high risk			US $7,000			US $20,000	

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

- Statement of Accounting Standard (SAS) 70 reports, targeted at ensuring firm financial statements, based on the standard from the American Institute of Certified Public Accountants (AICPA)

For any given firm to rely on the results of these or any other types of reviews, the firm must have some evidence that the review results accurately reflect the vendor control environment. Where the reviewer or assessment team is the firm itself, the independence comes from the firm's own criteria. However, in many cases, the reviewers are third-party consulting companies that are paid directly by the vendors undergoing review. If the reviews really were audits, a comparison with ISACA Standards for Information Systems Control Professionals would show that the auditor was not entirely independent.[2] Evidence of independence comes in a variety of forms, including:

- Assessor faces material risk of reputation or loss of certification for inaccurate results
- Assessor keeps technology control assessment work papers[3]
- Work papers are available for authoritative review
- Assessor is paid by a source other than the vendor under review

Given these commonly accepted industry independence evidences, the currently available vendor assessment standards do not fare well, as demonstrated in **figure 2**. Given that none of these approaches actually meet the due diligence requirements outlined previously, the path that has been taken by those seeking industry consensus does not yet provide assurance that data are properly handled. Even if vendor assessment standards were completely independent, each company still has to perform due diligence to the extent that the assessment report must cover the scope of the vendor handling of that firm's data.

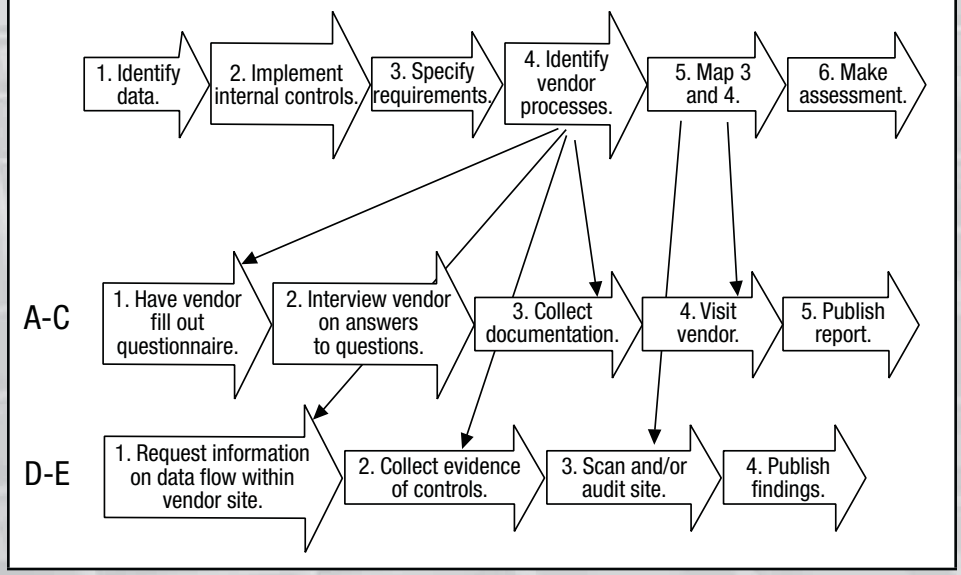
Figure 3 illustrates this point. The approaches taken by some firms to audit their vendors are laid side by side with the regulatory requirements for due diligence (steps 1 through 6). They are not isomorphic. At most, a passed audit means the vendor is cognizant of security measures, not that the data actually handled by the vendor on behalf of any given firm are covered in the review. There are several reasons why this situation has been allowed to reach the current fairly stable state. In the current situation:

- 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 consortia of other industry review teams, not by firm management or consortia 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 reviewers not subject to standards of independence

Figure 2—Evidence of Independence

Standard	Evidence			
	Assessor Risk	Work Papers Kept	Work Papers Available for Review By	Assessor Compensation Model
BITS FISAP				
ISO 27001	X		ISO	
PCI DSS	X	X	PPCIS	
SAS 70	X	X	AICPA	

Figure 3—Requirements vs. Practices



However, following a few recommendations should put due diligence back on track:

- Business managers should control the vendor security review process via existing points of integration:
  - The procurement process should set vendor expectations. Operations and compliance should be used to validate requirements during the contract review process.
  - IT management should verify that the vendor gets only the data it requires and gets the data only 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 that 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 *vice versa*.

Figure 4 illustrates the effect that following these recommendations would have on the mapping from requirements to due diligence process. A firm reviewer is still required, but the setup provided by the other areas in the organization makes their verification job a much shorter task.

CONCLUSION

There is no stigma in relying on a reasonably independent review if a vendor is able to provide one. However, it may be done only in the context of a full understanding of the data in scope. Even so, there will be times when a firm has no choice but to review a vendor. In such cases, it should use the best possible talent—real auditors, not checklists. This should motivate vendors to get their own independent assessment in order to avoid customer audits.

ENDNOTES

[1] Reference to *The Wizard of Oz*

[2] ISACA, Standards for Information Systems Control Professionals, 520, "Independence," *www.isaca.org/standards*

[3] Work papers are required by the AICPA to provide audit evidence and are the basis for the Public Company Accounting Oversight Board (PCAOB) assessment of auditors as required by the Sarbanes-Oxley Act.

Figure 4—Requirements vs. Recommendations