

Incorporating SAS No. 70 and Other Third-Party Reports into a Vendor Management Program



by Joel Lanz

The SAS No. 70 report is a helpful tool for operational risk managers in their management of vendor risk, but it has its limitations. This article explains the problems and suggests a way to use SAS No. 70 as one tool in a comprehensive vendor management program.

If a financial institution (FI) offers any of the services in the box at right, there is a good chance that it contracts with an outsourced third party (vendor) to assist with various elements of the service's delivery. In the never-ending challenge to deliver increasing value to various stakeholders in the face of economic realities, FIs have increasingly turned to vendors to deliver services in a more effective and efficient fashion. And this reliance is no longer limited to back-office, non-customer-facing activities.

Core Processing Systems. . . Valuation Services. . . Internet Banking. . . Cash Management Systems. . . Phone Switches and Voice Response Units . . . Infrastructure Management. . . Telecommunications. . . Application Development or Maintenance. . . Call Center. . . Offsite Storage and Record Systems. . . Loan Underwriting. . . Loan Servicing. . . Payment Systems. . . Trading Systems. . . Managed Security Services. . . ATM, Debit, and Credit Card Processing. . . Trust and Custodial Services

Software Engineering Institute, Information Technology Governance Institute, and the Institute of Internal

Auditors—have

As with most opportunities, reliance on vendors creates risk that must be managed. In some cases, regulatory agencies drive the demand for managing vendor risk. In other cases, business common sense and fiduciary responsibilities, including potential legal liability, generate the demand. Well-respected organizations—including the Bank Information Technology Secretariat (BITS), Federal Financial Institution Examination Council (FFIEC),

issued guidance on establishing a program to manage vendor risk. Meanwhile, vendors and other consultancies have issued their own perspective on vendor management due diligence and monitoring. Frequently, this latter perspective espouses the need to leverage the vendor's or consultant's particular area of expertise.

In both cases, however, the discussion of monitoring vendor activity—especially for processing

© 2004 by RMA. Joel Lanz leads a technology assurance and advisory CPA practice; he is the executive member for Professional Standards of the New York State Society of CPAs' Technology Assurance Committee; and he is an adjunct professor at the School of Professional Accountancy at the C.W. Post campus of Long Island University. The author wishes to acknowledge the assistance provided by Gordon Huszagh, CFO, Suffolk Bancorp.

activities related to information technology—includes the Statement on Auditing Standards No. 70 (SAS No. 70). Standards issued by the American Institute of Certified Public Accountants constitute the body of Generally Accepted Auditing Standards.¹

The basic precept of a SAS No. 70 report is for the vendor to engage a single independent auditor to audit its control environment and produce a report that can be distributed to the vendor's clients (that is, one audit) rather than have each client send its own auditor to audit the vendor individually (that is, multiple audits).

Vendors are quick to proclaim the success of their SAS No. 70 efforts as shown in the following press releases:²

- *...it has successfully issued its SAS No. 70 Type 1 report.... The self-initiated audit demonstrates...commitment to its customers as a reliable, transparent, secure ASP that is focused upon minimizing risk, increasing value, maintaining service availability, and preserving client privacy and data security.*
- *...is built on a foundation of values, and two of our most important values are integrity and "customer first." Earning a SAS No. 70 Type 1 certification [demonstrates our] acting on both of these values.*
- *Protecting customer data is the cornerstone of...success. Our SAS No. 70 audit is an important way to independently validate how well we manage...security.*
- *...passing the SAS No. 70...Type I audit is a key requirement for companies who wish to perform data-center and Web-hosting*

BECAUSE MANAGERS AND THEIR AUDITORS MAY NOT FULLY UNDERSTAND SAS NO. 70, THEY MAY RELY ON IT ALONE FOR ASSURANCE NEVER INTENDED TO BE GIVEN.

functions for financial...or other security-sensitive or regulated organizations. Such institutions can't use...firms that haven't passed the SAS No. 70 audit.

The mounting responsibilities of operational risk managers and the mandate for FIs to comply with evolving corporate governance initiatives can lead them to rely on their vendor's SAS No. 70 and associated proclamations to manage their vendor risk. Unfortunately, neither the managers nor their auditors may fully understand SAS No. 70 and so may rely on it alone for assurance that was never intended to be given. And if an auditor may not fully appreciate the true scope of SAS No. 70, then it should come as no surprise that an individual regulatory field examiner may also not be applying it correctly in insisting that financial institutions pay significant attention to its contents. Then again, maybe regulators understand all too well how financial institutions are using SAS No. 70, and perhaps that is why many FIs now are encouraged to implement a program to satisfy increasing regulatory expectations for vendor management.

Vendor Management and the Regulatory Environment

Auditors and regulators have long expressed degrees of concern over how financial institutions managed vendors. For example,

the 1996 *FFIEC IS* [Information Systems] *Examination Handbook* provided significant guidance in provisions that would protect financial institutions and their customers from weak vendors. Yet, pre-2000, many of these professionals experienced significant frustration when they would query FI representatives on their responsibilities for outsourced processing. Examples of typical responses follow:

- *We received a SAS No. 70 (and no, we didn't read it) as performed by a large accounting firm. Why do we need to do anything else?*
- *We would not have outsourced if we knew how to manage technology. Who are we to evaluate the contents of the SAS No. 70?*
- *Our lawyers read the contract...what possible additional things could the regulators ask for?*

Leveraging their lessons learned from managing Year 2000 risk, regulators began to increase their expectations for what financial institutions needed to do to manage their vendors. *Outsourcing Financial Services Activities: Industry Practices to Mitigate Risk*, published in October 1999 by the Federal Reserve Bank of New York, identified 13 industry practices for mitigating outsourcing risk. The top item on the list: "The board of directors and senior management must retain

IT WAS BECOMING CLEAR THAT FINANCIAL INSTITUTIONS COULD NO LONGER “OUTSOURCE” RESPONSIBILITY AND FIDUCIARY CARE FOR THEIR CUSTOMERS’ CONFIDENTIAL INFORMATION.

accountability for any outsourced activity. They determine the strategic role and objectives for the outsourcing arrangement, and provide necessary approvals.” Although basic, given the progress made in this area since 1999, the publication made it quite clear that senior financial institution management could no longer abdicate their responsibilities for managing vendors.

A second major regulatory thrust relating to vendor management came with the publication of the IT-related procedures within the Gramm-Leach-Bliley Act (GLBA), more commonly known as the “501(b) examination guidance” or “GLBA 501(b).” These procedures leverage regulatory concern over safeguarding customer information to focus bank managements’ attention on managing technology risk in general and, specifically, on considering the need to oversee service providers (vendors) as shown from the following guidance considerations (some of which were communicated to financial institutions for the first time):³

- Performing appropriate due diligence (including protecting customer information) in selecting service providers.
- Identifying data shared with service providers.
- Including contract provisions for service providers to comply with 501(b) guidance (as

indicated above, this would include technology risk in general, i.e., security, business continuity planning, and general controls).

- Considering whether service providers provide adequate periodic reports to enable financial institutions to evaluate providers’ performance and compliance with key risk management strategies, especially information security.
- Developing vendor management policies and procedures, including reviewing provider audits, test results, or equivalent examinations.

Although the guidelines do not specifically mention SAS No. 70 and do give FIs the opportunity to consider other types of evaluations, many risk executives, consultants, and some individual field examiners continued to believe that obtaining and reviewing a SAS No. 70 was a mandatory requirement in satisfying the reviewing vendor evaluation expectation. However, it also was becoming clear that financial institutions could no longer “outsource” responsibility and fiduciary care for their customers’ confidential information.

In late 2002, the FFIEC issued its first *Information Technology Handbook*. Each handbook is devoted to a major technology function. With knowledge that a handbook on outsourcing is

planned, risk managers can review handbooks already released to obtain an appreciation of heightened regulatory expectations for vendor management in the future. For example, the *eBanking IT Examination Handbook* identifies the following items to consider when an examiner is determining the quality of the institution’s risk management over outsourced technology services:⁴

- Due diligence prior to acquisition, including consideration of strategic plans, vendor reputation, financial condition, and ability to provide monitoring reports.
- Written contracts with clear responsibilities relating to the description of work, pricing considerations, security program, audit rights, contingency plans, data backup and protection, compliance with 501(b) provisions, upgrading of hardware and software, availability of vendor’s financial information, penalty and cancellation provisions, limitations over subcontracting, termination rights, institution ownership of data, and rights of federal regulators to examine services provided.
- Ongoing vendor oversight, including designation of an accountable executive for monitoring activities, control over remote vendor access, periodic reviews of continuity plans and coordination with the institution’s plans, review and monitoring of performance reports, and review of service provider audits (e.g., SAS No. 70 reports) and regulatory exam reports.

Around the time *eBanking IT Examination Handbook* was issued, BITS released its updated *Framework for Managing Technology Risk for IT Service Provider Relationships*.⁵ The framework provides an exhaustive guide of best practices in managing vendors. Although the framework suggests the review of a SAS No. 70 to determine compliance with control objectives, it also demonstrates vendor management practices beyond the scope of the traditional SAS No. 70. In some situations, executives began to question the contents and usefulness of the SAS No. 70 in fulfilling their regulatory and fiduciary responsibilities. With the new publications, it was apparent that vendor management meant that executives had to *consider their vendor's control environment to the same degree they would if they had not outsourced the service*. It also became very apparent that control objectives specified by vendors in the SAS No. 70 were woefully inadequate in helping executives determine that their information was being processed and maintained with the same degree of care as if it had never left the financial institution.

AICPA Perspective on SAS No. 70

The Auditing Standards Board (part of the AICPA) issued SAS No. 70 in 1993 to replace an earlier SAS (No. 44) that described similar control concerns over the processing by service providers.⁶ To provide guidance to auditors on the preparation and use of SAS No. 70, the AICPA issued an Audit Guide.⁷ It is quite interesting to compare the intent

of SAS No. 70 reports *identified by the issuers* with the proclamations of the press releases previously mentioned. As stated in the Audit Guide, “The guidance in SAS No. 70, Service Organizations, as amended, is applicable to the audit of the financial statements of an entity that obtains services from another organization that are part of the user organization’s information system.”⁸ The Audit Guide further identifies five service criteria provided by service organizations that would be considered part of an entity’s information system for financial statement purposes:

1. Transactions that are significant to the financial statement.
2. Procedures by which transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements.
3. Related accounting records, supporting information, and specific accounts in the financial statements.
4. How the information system captures other events and conditions that are significant to the financial statements.
5. The financial reporting process used to prepare the entity’s financial statements.

As can be seen, the SAS No. 70 was never intended to be used as a management tool for due diligence or for monitoring activity or quality of the service organization (vendor). It was not meant to be used to discharge fiduciary responsibilities, nor was it meant to demonstrate compliance with GLBA, customer privacy, adequacy of security programs, or any of the other proclamations made in the press releases identified above. It was never intended to be part of a process to demonstrate regulatory compliance. In identifying—and in some situations, testing—controls, SAS No. 70’s focus was solely on those processes that could impact the financial statement of the organization using the vendor to process financial transactions, and it was to be used by professional auditors in designing their audit approach. However, because of the ease of substituting the work of the auditor performing the SAS No. 70, rather than the financial institution performing the “honest work” of managing the vendor as provided in evolving regulatory and BITS guidance, many financial institutions fell into the trap of misusing the report as part of their vendor management programs.

IT ALSO BECAME VERY APPARENT THAT CONTROL OBJECTIVES SPECIFIED BY VENDORS IN THE SAS No. 70 WERE WOEFULLY INADEQUATE IN HELPING EXECUTIVES DETERMINE THAT THEIR INFORMATION WAS BEING PROCESSED AND MAINTAINED WITH THE SAME DEGREE OF CARE AS IF IT HAD NEVER LEFT THE FINANCIAL INSTITUTION.

A VENDOR MANAGEMENT POLICY DESCRIBING THE ASSOCIATED RISKS OF VENDOR MANAGEMENT AND THE NEED, IF ANY, FOR VARIOUS DEPARTMENTS TO REVIEW THE SAS No. 70 IS AN INTEGRAL ELEMENT IN DEMONSTRATING DUE DILIGENCE TO REGULATORS OR OTHER INTERESTED PARTIES.

How Should an Operational Risk Manager Use the SAS No. 70?

Despite the intended audience, the operational risk manager can use the SAS No. 70 to supplement and, at times, facilitate a comprehensive vendor risk management program. This section will suggest how the manager should make a cost-investment use of time in leveraging the SAS No. 70 report.

Managers and their auditors (both internal and external) should discuss the need to actually review the report. At a minimum, the report could provide risk managers with a good source of background information on the vendor. However, prior to investing significant time in reviewing the report, the risk manager should avoid duplicating audit efforts or needlessly spending time on sections with minimal value to the risk manager. A vendor management policy describing the associated risks of vendor management and the need, if any, for various departments to review the SAS No. 70 is an integral element in demonstrating due diligence to regulators or other interested parties.

The opinion within the SAS No. 70 report will clarify whether it is a Type I or Type II report. The main difference between the

two is that the auditor issuing the SAS No. 70 report is testing the effectiveness of controls to determine if the controls indeed function as intended. Generally, few if any of the control objectives identified have actually been tested for a Type I report. The reputation of the auditor issuing the report also is important. Bigger is not necessarily better, but the manager may want to consider the overall reputation and qualifications of the firm performing the work.⁹

The report section entitled “The Service Organization’s Description of Controls” enables the vendor to provide background information that it deems to be important to readers. This section is generally not audited by the auditor and should be treated as such. For the vast majority of financial institutions that already have a comprehensive vendor management program, most of this information should have already been considered as part of due diligence prior to engaging the vendor and ongoing monitoring program.

The next section, “Information Provided by the Service Auditor,” provides additional details about the suitability of controls identified to support the control objectives. In a Type

II report, the auditor tests the effectiveness of these controls. Because the *vendor* and not the *auditor* specifies the control objectives being reported on, potential weaknesses can be identified by noting the types of control objectives normally associated with the given process that are *not* included. This latter review requires some degree of audit background and is potentially time-consuming and frustrating when performed solely by operation managers. Institutional policy should clearly specify the need, if any, to perform this detailed review.

Finally, “User Control Considerations,” normally a one-to two-page section of the report, is a must-read for all. This section identifies those controls identified by the service auditor that are the responsibility of the customer (i.e., FI). Regardless of the FI’s reliance on the SAS No. 70 report, the FI should ensure that it has implemented these controls and that they function properly.

AICPA Introduces New Services to Better Satisfy Industry Needs

Responding to the industry demand for a different level of assurance—one that would incorporate evolving and regulatory requirements, especially as they relate to safeguarding customer privacy and maintaining availability and security levels—the AICPA, together with its Canadian counterpart, has introduced a series of new assurance services.¹⁰ Two of these services, Trust Services and Privacy Framework, are of significant value to operational risk managers. Perhaps the greatest differ-

ence between the new services and the previous SAS No. 70 is that, instead of having the vendor identify which control objectives should be tested, the objectives are tested against predetermined criteria and illustrations that have been subject to due process procedures, including exposure of the proposed criteria for public comments. This results in an expressed opinion as to whether the vendor complies with the criteria. The result would bring the FI closer to demonstrating the level of vendor management expected by the regulators.

However, since these new services set a higher standard, the vendor is not likely to volunteer for the additional scrutiny. Alternatively, other forms of assurance could be developed to ensure vendor compliance with other standards, such as those published by the FFIEC or BITS.

Conclusion

The SAS No. 70 report is a helpful tool for operational risk managers, but it has its limits. Because it is intended for financial statement auditors, its review should not be automatic or expected by internal auditors or examiners. Each FI must identify the applicable risk of using a vendor and what types of risk management techniques need to be employed. Depending on the

SINCE NEW SERVICES SET A HIGHER STANDARD, THE VENDOR IS NOT LIKELY TO VOLUNTEER FOR THE ADDITIONAL SCRUTINY. ALTERNATIVELY, OTHER FORMS OF ASSURANCE COULD BE DEVELOPED TO ENSURE VENDOR COMPLIANCE WITH OTHER STANDARDS, SUCH AS THOSE PUBLISHED BY THE FFIEC OR BITS.

vendor, alternative assurance reports, such as penetration tests, may be more appropriate. However, the latter causes some risk in that when performed by a non-CPA, testing standards may differ depending on the provider.¹¹ The BITS framework provides an excellent set of tools to develop a vendor management program. The new AICPA services provide a cost-effective standard for providing a true generally acceptable standard that risk managers can rely on in performing selected aspects of their program. Yet, regardless of the standards, nothing substitutes for the institution taking accountability for the work performed by its vendors. □

Contact Lanz by e-mail at jlanz@bankingcpa.com.

Notes

¹ As a result of the Sarbanes-Oxley Act, standards relating to the audit of public companies will now be issued by the Public Company Accounting Oversight Board (PCAOB).

² Organization names have been omitted to avoid

embarrassment.

³ See Attachment for FIL-68-2001, *Examination Procedures to Evaluate Customer Information Safeguards*, Section IV—Assess the Measures Taken To Oversee Service Providers, FDIC, August 24, 2001.

⁴ *FFIEC eBanking IT Examination Handbook*, August 2003, p. A-8.

⁵ "BITS Framework for Managing Technology Risk for IT Service Provider Relationships," Version II, November 2003.

⁶ The codification of SAS No. 70 itself, along with SASs that subsequently have been issued to provide further clarification, is contained in the *Codification of Statements on Auditing Standards*, AICPA, AU 324.

⁷ Although descriptions of auditing standards, procedures, and practices in Audit Guides are not as authoritative as pronouncements of the Auditing Standards Board, AICPA members may have to justify a departure from such descriptions if the quality of their work is questioned.

⁸ *Service Organizations: Applying SAS No. 79*, as amended, AICPA Audit Guide, AICPA, 2002, p. 2.

⁹ In addition to the obvious word of mouth or industry reputation, the manager may wish to consult with the state board of accountancy or state CPA society.

¹⁰ Visit www.aicpa.org/assurance/index.htm for further information and copies of the criteria.

¹¹ See "Practical Aspects of Vulnerability Assessment and Penetration Testing," *The RMA Journal*, February 2003, pp. 52-57.