IT Attestation Services: What You Need to Know

Jennifer Bayuk

The rapid growth in outsourcing information technology (IT)—and increased reliance on software application service providers—are fueling a demand for IT attestation services. The author explains what you need to know about them.

Information technology (IT) service providers permit a pay-as-you-go model for information system processing. Business leaders find the model attractive because it alleviates the need for up-front investment and reduces lead time to production dates. Technology leaders find the model attractive because it reduces the amount of work required on their part to deliver technology services.

A VISION OF THE FUTURE

At a recent Securities Industry Association conference, Jonathan Schwartz, president and chief operating officer of Sun Microsystems, presented a vision of the future where most data and business applications would be hosted by technology services firms;[1] the payoff to the business customer would be that the only thing businesses would be required to purchase and deploy would be a PC. In this vision, there is no need for computer rooms, disk drives, or HVAC[2] systems—and there is no cost unless the customer uses the service.

But before one starts revising IT cost allocations to debit by transaction, it is of course prudent to investigate whether the service provider is a reliable business partner. In a legal and regulatory context, such investigations are referred to as "due diligence." Broadly speaking, due diligence is a requirement to review evidence and make assessments based on objective criteria. With respect to contracting for IT services, due diligence is a good-faith effort on the part of a business to ascertain that the service provider is reputable and capable of fulfilling its contract obligations, which ordinarily would include requirements to protect and safeguard information entrusted to the service provider.

There is a fundamental quandary for a business that must evaluate an IT service provider. By the act of outsourcing the service, a corporation loses the ability to directly specify the processes by which the technology will be managed. Even if the ability were to continue, actually doing so would cut considerably into the benefit side of the cost-benefit calculations that led to the decision to outsource. The due diligence effort must gather enough information about service provider management as possible without having to directly supervise it. Hence, there is a growing reliance on IT attestation services.

The first IT attestation services were performed in the 1970s. Companies that marketed accounting software began to contract electronic data processing (EDP) audits from reputable accounting firms. The accounting firms performed "data in/data out" audits on the contracting company's software. An auditor would collect batch data-entry sheets ("data in"), manually compute financial statements, and then compare his/her

Published online in Wiley InterScience (www.interscience.wiley.com).
DOI 10.1002/jcaf.20341

version of the financial statements with those produced by the computer ("data out"). This saved customers the expense of an individual information systems (IS) audit. Moreover, if the software passed the audit, the company could use the accountant's seal of approval in its advertising.

Rapid growth in IT outsourcing and increased reliance on software application service providers (ASPs) are fueling the fire for attestation services. Today, IT attestation services take for granted that software calculations meet business requirements. Checking the math has become a business operations function. Instead, a typical IT due diligence review will evaluate whether the service provider is capable of:

- handling the business volume,
- meeting quality-of-service requirements,
- securing business-sensitive data,
- recovering within a reasonable amount of time from unforeseen calamities, and
- responding to changing IT requirements.

Today's IT outsourcers and ASPs,[3] like the accounting software firms of the late 1970s, contract independent technology audits of themselves. A successful assessment is a positive advertising statement. It also saves the time that the company's own staff members would have to spend if all of its customers sent separate teams of auditors to the site to perform their own due diligence.

However, unlike the calculations of the 1970s EDP auditors, it is not possible for a corporation to check the work of today's IT assessment teams. At one end of the spectrum of IT attestation services are independent control testing of complex environments, or full-blown audits; at the other is pure marketing. Moreover, the two-pronged motivation for attestation services, assurance and advertisement, has led not only to a wide variety of attestation services, but also to confusion between attestation services and marketing tools. This confusion is sometimes on the side of the corporation performing due diligence, but it also manifests itself on the part of the outsourcers and service providers seeking to satisfy the due diligence requirement.

The due diligence effort must gather enough information about service provider management as possible without having to directly supervise it.

This article differentiates the different types of IT attestation reports that are offered as evidence that IT controls are in place and describes the attestation service process that produced them. As a corporation devises a program for performing IT service provider due diligence, it must set a stake in the ground on the type and amount of evidence it will need to be assured that the service provider can meet requirements. This article should enable its readers to make informed decisions on whether a given IT attestation report can be relied upon as evidence in support of a due diligence program.

SCOPE

The level of due diligence in examining information technology controls should be commensurate with the risk of uncontrolled systems operations. A typical objective in a due diligence review is to establish that a third party has adequate safeguards in place to secure and process data with integrity on an ongoing basis. The scope of the review is the systems operations required to fulfill the statement of work or other information services description.

However, the scope of work for an attestation report offered to a due diligence reviewer is rarely as broad as the business customer's requirement for due diligence. The level delivered from a given attestation service will be set by the assessor's objective. Service providers may have conducted external audits, internal security reviews, and/or consulting engagements that overlap in scope with a given customer's due diligence efforts.[4] However, the objective of the assessment may not be the same as the objective of the due diligence at all. Nevertheless, when asked for evidence in support of a due diligence review, the service provider is well within the realm of reasonableness in offering the customer a copy of any available attestation report. Whether or not the proffered documents fully cover the scope of customer needs for service provider due diligence is within the realm of *caveat emptor*.

TYPES OF ATTESTATION

The following is a list of typical attestation services that service providers offer customers

DOI 10.1002/jcaf

as proof that IT services are controlled. They are presented in order from most comprehensive in due diligence to least.

External Audit

External audit is the gold standard in due diligence activity. In these engagements, the external audit firm's charter is to attest that financial statements are accurate and in compliance with generally accepted accounting principles (GAAP). The external audit firm will assign a statutory auditor[5] to accept responsibility for the overall audit engagement. Once that responsibility is accepted, the scope of that statutory auditor's assignment is to detect material misstatements in the financial statements. He/she is called the *lead* and will, at the end of the review, affix his/her signature to the report that attests that the financial statements are correct. Generally accepted auditing standards (GAAS) require the lead to allocate sufficient staff members and resources to achieve assurance that the judgment of a reasonable person would not be influenced by any financial misstatement not caught in the course of the audit.[6] To accomplish this staff allocation for a large corporation, the lead must break the audit down into a series of smaller projects and provide each with its own scope. It is through this process that IS audits are conducted in support of financial statement audits. On the basis of the completeness of audit evidence and perhaps an independent peer review by other qualified technical experts, the lead statutory auditor may be confident enough in the assessment work done by the IS audit team to sign the consolidated audit report.

SAS 70 Services

The scope in a normal external IS audit must be flexible enough to serve the combined goal of financial statement and control practice verification. But in the context of a typical service provider assessment, the service provider is often not using the software provided to its customers for its own business. In addition, the service provider is often not subject to the same regulatory and legal requirements as its customers. In this case, even a successful financial statement external audit provides no assurance that controls over IT services provided by the entity to others are the same caliber as those used to produce the entity's own financial statements. That is why the American Institute of Certified Public Accountants (AICPA) introduced Statement on Auditing Standards No. 70 (SAS 70).[7] Again, the focus is on financial statements, but in this case, the financial statement of the customer.

This article should enable its readers to make informed decisions on whether a given IT attestation report can be relied upon as evidence in support of a due diligence program.

SAS 70 guidelines were specifically developed to provide guidance to auditors of companies that outsource transaction processing to IT service providers. SAS 70 clearly defines the differences between IT control objectives themselves, their implementation by management, and the auditor's testing of them. Two types of audits are described in the SAS 70 guideline: an audit of the financial statements of the user of the service and an audit of the services provided. The SAS 70 service provider attestations are directed at the second type—that is, the activities of the service organization and the service auditor. Within this second type of audit, the service organization audit, there are two subtypes: an assessment of management-identified controls and an assessment of management-identified controls plus tests of these controls. The two subtypes of an SAS 70 service organization audit are colloquially referred to by information service auditors as SAS 70 Type 1 or SAS 70 Type 2 audits.

In both types of SAS 70 service organization audits, the service auditor is presented with a document describing management's control objectives and associated control practices. This is not necessarily the entire company internal control structure but the subset of it that provides the specific service under review. The auditor will review controls with respect to the control objectives. In a SAS 70 Type 1 audit, the audit report will reflect whether the controls are adequate to achieve the control objectives and whether they have been implemented. In a SAS 70 Type 2 audit, the audit report will also identify weaknesses in control implementation.

Certifications Assessments

IT assessment teams are often hired as consultants to determine whether IT

DOI 10.1002/jcaf

management has actually implemented the control structure as described in some document. The document may be written by management, a "best practice" published by the consulting firm, or a "standards" document published by a third party. Depending on the agreement between the consultant and the service provider, the report produced by the assessor may or may not include all control weaknesses uncovered in the course of the review.

Where assessments are aimed at showing compliance with published standards, it is sometimes possible to rely on the standards organizations to enforce some measure of due diligence in claiming certification compliance with standards.[8] However, not all certification assessments have the endorsement of the associated standards bodies. For example, the International Organization for Standardization (ISO) develops standards but does not operate any schemes for assessing conformity with them.[9]

The extent to which nonstatutory assessment reports can be relied upon is the extent to which those performing the work are objective in its performance. Questions one may ask to determine the extent of an assessor's objectivity are:

- Reporting hierarchy—Does the auditor report to a person who is responsible for maintaining the controls being audited?
- Financial independence—Does the auditor's salary or fee in any way depend on the favorable opinion of a person who is responsible for maintaining the controls being audited?
- Participation in system design—Does the auditor work for an organization that helped design or implement controls that are under review, or did the auditor participate in these activities?

Where these questions are answered negatively, the work is not covered by the standards of professional practice that apply to auditors.[10] Therefore, the due diligence reviewer should have some alternative source of evidence with respect to the independence on the part of the assessor in order to rely on the assessment results.

SAS 70 guidelines were specifically developed to provide guidance to auditors of companies that outsource transaction processing to IT service providers.

Generally, certification assessments fall into two categories: technical and process. In compliance assessments of both types, best practices in IT controls are regularly published by respected organizations, and consulting organizations offer attestation services that will certify a given service provider to be in compliance with the best practice.[11]

Penetration Studies

In the domain of IT security, several IT consulting services provide "penetration studies." These are attempts to break security controls that IT management has put in place. Penetration study reports are often offered as attestations that control objectives are met. Many application service providers hand them out in lieu of audits or certification assessments. These services are entirely consulting-oriented and often marketing-oriented. Due diligence reviewers should be wary of the claims that systems cannot be penetrated when the reports neither identify the controls that management has put in place nor the methodology used to maintain the control environment. The scope of the review will often have been limited to a set of systems that management is confident it protects, and the scope may have been changed in mid-review.

Documentation Reviews

Where there is no attestation report available from any kind of external assessor, due diligence reviewers rely on a service provider's own documentation with respect to their IT control environment. A service provider that has given thought and planning to IT controls will invariably have published an internal policy and/or set of procedures that describes how customer data are protected and how systems are designed and operated for resiliency. However, it is sometimes the case that even though these documents exist, the service provider will not allow them to be taken out of house. This forces the due diligence reviewer to visit the service provider offices to read the documentation. It also indicates a lack of confidence on the part of the service provider to securely deliver documents and maintain its security when the cloak of obscurity is lifted.

DOI 10.1002/jcaf

Questionnaires and Surveys

Service providers offer such a wide variety of attestation materials as proof of internal controls that many large corporations have developed their own control requirements for service providers and send them out as questionnaires. Though it is cumbersome to the service provider and not always independently verified, it has become a fairly common method of reviewing third-party data handling.[12] Potential IT service providers are requested to answer as many as 100 or more questions about systems security, operations monitoring, resiliency, and disaster recovery processes. The level of detail required in the answers varies.

CONCLUSION

Note that a report that is most comprehensive from a due diligence standpoint may still fail to meet a due diligence objective. For example, though an external audit is most comprehensive from a due diligence standpoint, it is actually the least likely of all the attestation services to cover the scope of the services for which a given customer has contracted. Therefore, a corporate due diligence program usually combines reliance on a combination of attestation reports with some kind of analysis that demonstrates comprehensive coverage.

However, if the scope of the services to be rendered is covered by an attestation report, the type of report is the next consideration. An external audit will typically only be useful to the customer as evidence that the service provider is a going concern. However, there is value added from an IT control standpoint if the service provider is in the same business as the customer. The SAS 70 Type 2 audit clearly provides more valuable information than the SAS 70 Type 1, though at least a SAS 70 Type 1 demonstrates that the service provider has given some serious thought to what the IT controls should look like. Technical or process standard compliance reports may indicate that internal controls are in place. However, using them as evidence of due diligence may be problematic because the fact that a technical implementation is correct or a management process exists is no indication that data are actually safeguarded according to customer requirements. Penetration studies are similar to these compliance assessments in that they are reliable only to the extent that both the skill and independence of the assessor can be ascertained. Penetration studies are dissimilar from compliance reports in that it is more difficult to determine scope. Internal documentation shows at least that resources have been allocated for IT control tasks. Service provider answers to direct questionnaires and surveys can be relied upon a little more than marketing material.

The most important thing to remember about all IT attestation services is that none of them provide verification that the service provider's controls are appropriate for due diligence required from the customer standpoint; only the customer can make that determination.

NOTES

1. www.sia.com/tmc2005/pdf/Schwartz.pdf.
2. HVAC is a computer industry term for specialized heating, ventilating, and air conditioning systems.
3. Hereafter referred to as "service providers."
4. For an explanation of why various types of non-audit IT attestation services may have been commissioned by the service provider, see Bayuk, J. (2005, Fall). Security review alternatives. *Computer Security Journal*, Volume XXI, Number 4.
5. "Statutory auditor" is a generic term used to describe a person licensed in a given environment to perform independent audits. A more correct term for a given country may be certified public accountant (CPA), chartered accountant, or independent auditor.
6. American Institute of Certified Public Accountants (AICPA) Auditing Standards Board (ASB), *AICPA Professional Standards*, AICPA, June 2003. These standards govern the conduct of external audits conducted by CPAs.
7. See AICPA Auditing Practice Release No. 021056: Implementing SAS No. 70 Reports on the Processing of Transactions by Service Organizations. Note also that similar associations in other countries have published similar standards (e.g., Chartered Accountants of Canada).
8. For example, the PCI Security Standards Council (www.pcisecuritystandards.org) and the AICPA SysTrust standards (www.aicpa.org).
9. See http://www.iso.org/iso/en/iso9000-14000/certification/publicizing/publicizing_4.html.
10. For examples of these standards, see www.isaca.org, www.theiia.org, and www.aicpa.org.
11. Examples of best practices that are often the subject of technical certification reports are the Center for Internet Security (www.cisecurity.com), BITS (www.bitsinfo.org), the National Institute of Standards and Technology (csrc.ncsl.nist.gov), and SANS (www.sans.org). Examples of best practices that are often the subject of process certification reports are the International Organization for Standardization (www.iso.org) and the IT Infrastructure Library (www.itil.org).
12. See "BITS IT Service Providers Expectations Matrix," www.bitsinfo.org, January 2004.

DOI 10.1002/jcaf

Jennifer Bayuk, CISM, CISA, is a senior managing director and chief information security officer for Bear Stearns & Co. Inc. She is responsible for information security policy, process, management, architecture, and metrics. She has been a manager of information systems audit, a Big 4 security consultant and auditor, and security software engineer at AT&T Bell Laboratories. She has published on information security and audit topics ranging from security process management to client/server application controls, including two editions of an Information Systems Audit and Control Association (ISACA) textbook on the IS audit process. She chairs the Securities Industry and Financial Markets Association Information Security Subcommittee and the Financial Services Sector Coordinating Council Technology R&D Committee. She has lectured for organizations that include ISACA, the National Institute of Standards and Technology, the Computer Security Institute, and the Federal Deposit Insurance Corporation. She is a Certified Information Systems Auditor and Certified Information Security Manager. She has master's degrees in computer science and philosophy.

This article is based in part on Chapter 1.2.2 of *Stepping Through the IS Audit* by Jennifer Bayuk, a 2005 ISACA publication, available at www.isaca.org/bookstore.

DOI 10.1002/jcaf