



SAS⁷⁰ IS SO YESTERDAY

Move over SAS 70, there's a new standard in town and we all have to be up and ready if we're going to ensure safety and soundness.

In today's business environment of organizational connectivity and web-based networking, service organizations are increasingly required to demonstrate that they have adequate controls and safeguards as they host or process data belonging to their customers. This need is supported by both real-life cases involving breaches of data security within the mortgage industry, as well as legal protections and guidelines.

By David Green
A new standard developed by the American Institute of Certified Public Accountants (AICPA), the Standards for Attestation Engagements (SSAE) 16, is designed to help service organizations provide reporting on its internal controls and systems. Replacing its predecessor, Statement on Auditing Standards (SAS) No. 70, on June 15, this newer and more robust standard is an attest standard, not an auditing standard. As a result, SSAE 16 will now require management to provide a written

assertion to the service auditor regarding the fair presentation of the company's systems and internal controls. The implications of this are numerous for mortgage issuers that seek to hire external vendors for workflow management and quality control.

A LITTLE HISTORY

The Sarbanes-Oxley Act (SOX) was enacted in 2002 in response to major corporate accounting scandals by large corporations such as Enron and WorldCom. The Act, which applies only to publicly held companies, created a number of reforms to enhance corporate responsibility and ensure that financial institutions accurately disclosed information. To minimize future accounting fraud, the SOX Act also created the Public Company Accounting Oversight Board (PCAOB) to monitor the auditing of financial institutions. The SOX Act ensures transparency among management and employees, and also improves whistleblower protections. More specifically, Section 404 of the Sarbanes-Oxley Act requires management to test its internal controls; for example, to ensure their accounting systems are in fact meeting key functional requirements related to data transparency and access control. It is the requirements of Section 404 of the SOX act that make SSAE 16 audit reports

“Because management must report annually on its effectiveness of **internal controls**, it then has an obligation to inquire and inspect on all controls.”

even more important to the process of reporting on the effectiveness of internal control over financial reporting. It states that issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting, while also assessing the effectiveness of such internal controls and procedures. The registered accounting

firm must, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting.

DODD-FRANK MAKES AMENDS

Dodd-Frank Act Section 989G amends the Sarbanes-Oxley Act (SOX) to make permanent the exemption from its section 404(b) requirement for non-accelerated filers (those with less than \$75 million in market cap) that has temporarily been in effect by order of the SEC. The act also requires the SEC to complete a study within nine months of the act's enactment on how to reduce the burden of 404(b) compliance for companies with market caps between \$75 million and \$250 million. The study will consider whether any such methods of reducing the burden, or a complete exemption, would encourage companies to list on exchanges.

THE SOX AND SAS 70 CONNECTION

The relationship between Sarbanes-Oxley and SAS 70 begins with Section 404, which addresses assessments of internal control and requires a management report to that effect in respect to financial reporting. Because management must report annually on its effectiveness of internal controls, it then has an obligation to in-

quire and inspect on all controls considered vital to the organization as a whole. Since a large number of publicly traded companies outsource a host of critical services, these outsourcer providers, or service organizations, are considered an integral component for purposes of financial reporting. Therefore, a due-diligence process must be enacted to have their internal controls observed and certified. The

Securities and Exchange Commission's (SEC) Chief Accountant and the Division of Corporation Finance has stated that "In many situations, a registrant relies on a third party service provider to perform certain functions where the outsourced activity affects the initiation, authorization, recording, processing or reporting of transactions in the registrant's financial statement. In assessing internal controls over financial reporting, management may rely on a Type 2 SAS 70 report." As a result, SAS 70 Type II reports provide the needed assurance on service organizations that are conducting outsourcing services for publicly traded companies.

THE OLD STANDARD – SAS 70

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the AICPA. A service auditor's examination, or SAS 70 Audit, performed in accordance with this standard is widely respected because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, often including controls over information technology and related processes. The SAS 70 standard allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format.

The issuance of a service auditor's report, prepared in accordance with SAS No. 70, signifies to mortgage issuers that a service organization has had its internal controls and activities closely examined by an independent accounting and auditing firm. In accounting and auditing, internal control is defined as a process effected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives. It is a means by which an organization's resources are directed, monitored, and measured, and plays an important role in preventing and detecting fraud and protecting the organization's resources.

At the specific transaction level, internal control refers to the actions taken to achieve a specific objective (e.g., how to ensure the organization's payments to third parties are for valid services rendered.) Internal control procedures reduce process variation, leading to more predictable outcomes. Internal control is a key element of the Sarbanes-Oxley Act of 2002.

The audit report was issued to the service organization at the conclusion of a SAS 70 examination. If a service organization provides transaction processing, data hosting, IT infrastructure or other data processing services to the user organization, the user auditor may need to gain an understanding of the controls at the service organization in order to properly plan the audit and evaluate control risk.

Without question, these service organizations will see a significant increase in the number of companies requesting SSAE 16 audits, and will need to be prepared for the time and costs involved with the process.

SSAE 16 - THE NEW STANDARD

While the focus of SSAE 16 is similar in scope to the SAS 70 standard, this newer and more robust standard is an attest standard, not an auditing standard. This means that SSAE 16 will now require management to provide a written assertion to the service auditor regarding the fair presentation of the company's systems and internal controls. This is significant in that it requires senior management to "go on the record" regarding their organization's internal safeguards

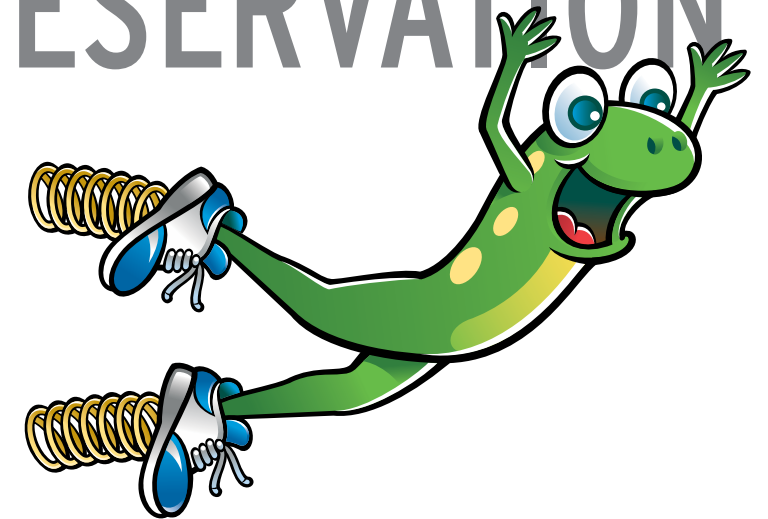
and controls were suitably designed (SSAE 16 Type 1 report) and operating effectively (SSAE 16 Type 2 report). Therefore, offering assurances to mortgage issuers that their customer data is going to be handled properly and with adequate processes and data security.

WHAT THIS MEANS

Many viable service providers and mortgage vendors have yet to go through the SAS 70 / SSAE 16 audit process. This leads one to believe that the decision makers at some financial institutions do not yet understand the value of compliance to the standard. It may be seen as just another of the endless acronyms in the mortgage and banking industry, and because mortgage bankers are not mandated to ensure their partners are in compliance by regulators,

ASSET PRESERVATION

Make the Leap to Stronger Results



Five Brothers' nationwide field services and advanced technology

take you further at every phase of the asset preservation cycle - from property preservation and inspections to REO management and valuation services. Higher asset values, lower costs. Make the leap with Five Brothers.

Experience the Five Brothers difference... **stronger results from the ground up.**



www.fivebrms.com
586.772.7600

Nationwide Field Services • Specialized Support Services • Advanced Technology Solutions

this standard may unwittingly be regarded as unimportant.

While regulations contained within SOX and the Gramm-Leach-Bliley's Safeguards Rule do not specifically mandate these accounting standards, working with vendors who have met the burden of SSAE 16 compliance surely assists organizations to ensure compliance to those regulations. For example, under the Safeguards Rule, financial institutions

“Without question, these service organizations will see a significant increase in the number of companies requesting **SSAE 16 audits**, and will need to be prepared.”

are required to secure customer records and information. As outsourcing continues to grow as a way to hedge against fluctuations in loan volume, mortgage bankers are sharing critical and confidential information with service organizations. So how can a lender ensure that the partner firm is properly caring for the information as required? One way is to ask the vendor for information on their internal controls regarding data security and privacy plans as part of their due-diligence for vendor selection. Even then, how can an organization ensure it is being properly followed? One option is to send a team of auditors to the vendor to dig through their systems, processes and internal controls to ensure that customer information is safeguarded. However, this method can be extremely costly, especially when performed on an annual basis. The SAS 70/SSAE 16 report not only encompasses the same due diligence as an internal audit to ensure that the vendor is meeting data protection standards, but also provides additional confidence that the report is affirmed by an independent and certified accounting firm. The report provided by the auditing firm will detail the processes and controls that are in place, as well as attest to their execution.

VENDORS' RESPONSIBILITY

Requiring that service organizations are in compliance with SSAE 16 is only part of the important due diligence that should be performed to ensure the security of customer data. It is important to note, that although the CPA firm performs a thorough audit as part of the SSAE 16 standard, it does not “certify” anything about the processes in place. It merely states that such processes exist,

have been reviewed, and are properly documented. To really understand how well a service organization is safeguarding customer information, mortgage issuers need to look at the details of the SSAE 16 report and understand the vendor's internal controls.

While each report will be somewhat different based on the vendor's processes and the auditing firms template, there is certainly some consistent and important information one can derive from each report. For example, how does the service organization handle physical security? How is the vendor's physical location secured? How are paper files transported throughout the office? In a world of networked and web based logistics, how are a vendors computer operations controlled? How is the computer room or data center secured? How and how often are backup files made? How are backup tapes or digital images se-

cured? How is intrusion detection handled? What data redundancy is in place?

These are just a few of the many important details organizations will be able to assess and understand by reading through a vendor's audit report.

THE MORTGAGE BANKING TRANSACTION

With an independent, outside SSAE 16 audit, financial institutions gain necessary assurances about the privacy of customer information being housed and handled by vendors. In turn, these service organizations also receive significant value from engaging in a SSAE 16 audit. An Audit Report issued by an independent auditing firm differentiates the service organization from its peers by demonstrating the establishment of control objectives and effectively designed control activities. With a trend of outsourcing services to overseas vendors, the service organization that can prove that it has the proper security controls in place domestically can gain a competitive advantage to unstable, overseas vendors that are handling customer data thousands of miles away.

Without a SSAE 16 compliance report, a financial institution may have to undergo a costly and time-consuming audit by their accounting team. In a world of increasing regulatory oversight and requirements, SSAE 16 provides lenders due diligence that ensures data security and regulatory compliance, while not incurring the expense of performing internal audits of a service organizations internal controls and safeguards. The SSAE 16 standard strengthens both the vendor and the financial institution utilizing their services, and in turn, strengthens the mortgage industry as a whole. ♦

ABOUT THE AUTHOR

David Green is founder and president of The StoneHill Group, nationwide provider of outsourcing services and consulting in the mortgage banking, banking, credit union, and financial industries since 1996. The StoneHill Group offers Quality Mortgage Outsource Solutions, including Quality Control, Fulfillment Services, Due-Diligence and Collateral Audits which allow for scalability and cost-effective services specifically tailored to meet clients' needs.

