



AuditOne Advisory

From Bud Genovese, Chairman

Your Bank Service Providers Face Important Changes to SAS 70 Requirements

Your major bank service providers --data processors, IRR and other software providers, data warehouse, etc.-- face important changes to the traditional SAS 70 Types I and II annual reporting process. The new rules, entitled Statement on Standards for Attestation Engagements #16 (SSAE16) replace the SAS 70 rules, and become effective for reports for periods ending on or after June 15, 2011. (NOTE: If this information does not apply directly to you, please consider forwarding and sharing this AuditOne Advisory with your bank colleagues who manage service provider and vendor relationships.)

As part of your vendor management requirements, your bank should receive a SAS 70 (soon to be SSAE16) report every year from your major suppliers of financial reporting data and information processing. If you do not receive this report, you should demand one. These reports attest to the technical controls implemented by vendors to ensure the integrity of data that you rely upon for your financial reports. The reliability of your financial statements and call reports are directly impacted by this information. For publicly traded companies, this becomes especially important, even if you are not an accelerated Sarbanes-Oxley filer

Likewise, if your concern is security of the information being handled by your service provider, you should request (or review) that information security controls are covered in the report. Your bank's safety and soundness is directly impacted by the information security controls implemented by these service providers, and therefore the report becomes critical for your information security risk program. Be aware though, that some of your affected service providers may have traditionally ignored engaging for these SAS 70/SSAE16 or information security reports due to the perceived high costs involved. Ignoring these requirements puts the vendors and banks at risk and invites regulatory action. But there's a lower cost way to meet the requirement.

Our sister company, AuditOne Inc., is a CPA firm whose sole business practice and focus is performing SAS 70/SSAE16 and other reviews of third party providers to the financial industry. AuditOne Inc. is dedicated to working hard to stay current on all the changes, nuances, and requirement techniques of the SSAE16 process. Our skilled audit, technical and security experts deliver the highest quality, cost-effective, responsive SAS 70/ SSAE16 services in the industry. Please feel free to recommend that your service providers contact me for further information about how to meet the new SSAE16 requirements, and reduce the potential risk to your bank.

Based on the *Statement on Standards for Attestation Engagements* issued by the Auditing Standards Board, there are three main changes to understand. Be confident that AuditOne Inc. has analyzed all the changes and is prepared to lead service providers step by step to cost-effectively meet all the requirements. Let's now take a closer look at what's new.

1) Under SSAE16, the service provider must provide a written statement of "the description of the provider's system" that will be included in Section 2 of the SSAE16 report. This is new and not previously required. This system description is to include: how the system was designed and implemented to process relevant transactions; any material changes to the system during the period

covered; statement of the system controls; etc. AuditOne Inc. can help prepare every aspect of this statement, ensuring vendors meet the requirements of new SSAE16 reporting.

2) The service provider will provide an "Assertion by Management" of a Service Organization for a Type I or II Report. While this is technically new, it is basically the same content as the "Representation Letter" now done for SAS 70s. The major difference is that this new Assertion by Management letter must now be incorporated into the SSAE16 report. Again, AuditOne Inc. can guide vendors through the process of meeting this requirement.

3) The SSAE16 can be accomplished by either the "Carve-Out Method" or the "Inclusive Method." The Inclusive Method includes a description of the nature of the services and controls provided by *subservice* organizations. The Carve-Out Method does not examine the controls of the subservice organizations' systems. AuditOne Inc. recommends the Carve-Out method because it is similar to the familiar SAS 70 process, and it saves valuable time and money.

Again, after June, 2011, ask your major service providers for annual copies of their SSAE16 reports, and have them contact me for cost-effective, industry-compliant help from AuditOne Inc.

Bud Genovese is Chairman of AuditOne LLC, a California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit and credit review services by gathering wide-ranging, extraordinary expertise within one firm. AuditOne now serves over 160 clients throughout the Western United States, and nationally. Contact Bud Genovese at 408-980-8099 or bud.genovese@audit-one.com