Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Understanding what Service Organizations are trying to SSAE

Many cloud and data center Service Organizations are transitioning from SAS 70 to SSAE 16 for yearly control audit reporting to customers. There are multiple Service Organization Control reports (SOC 1, 2, and 3) as well as types (1 and 2). Navigating which is appropriate can be confusing. This document provides guidance on how to recognize, review, and respond to this new audit standard.

Copyright SANS Institute
Author Retains Full Rights

AD

Understanding what Service Organizations are trying to SSAE

GIAC (GSNA) Gold Certification

Author: Michael Hoehl, mmhoehl@gmail.com
Advisor: Manuel Santander

Accepted: December 23, 2013

Abstract

Many cloud and data center Service Organizations are transitioning from SAS 70 to SSAE 16 for yearly control audit reporting to customers. There are multiple Service Organization Control reports (SOC 1, 2, and 3) as well as types (1 and 2). Navigating which is appropriate can be confusing. This document provides guidance on how to recognize, review, and respond to this new audit standard.

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

"*A body of men holding themselves accountable to nobody ought not to be trusted by anybody*." — Thomas Paine

1. Introduction

Today, many companies are choosing to perform common business functions like Finance, Human Resources, Legal, Sales, and Procurement with the use of information systems that reside remotely at a vendor. There are several reasons for this transition. The Internet and Cloud Computing have allowed vendors to offer a lower cost of entry and time to deploy for information systems as compared to each customer building their own independent systems in-house. Shared resources and economy of mechanism translate into lower total cost for the vendor and subsequently lower price for customers. Vendors are responsible for software lifecycle management including implementing new versions, releases, and security patches. They can offer expertise and resources that customers might not need routinely enough to justify keeping on payroll.

The vendors that offer these common on-line business functions and services are known by many different names including Software as a Service (SaaS) vendors, Managed Services Providers (MSP), Application Service Providers (ASP), Cloud Computing vendors, Virtualization and On-demand Computing Services, Data Center and Co-Location Providers. In auditor and accounting terms, these vendors are collectively identified as "Service Organizations". Customers demand some reasonable assurance that the Service Organization can fulfill their commitments in a sustainable manner. This is where the concept of "controls" is relevant. In this context, controls are simply instruments (e.g., policies, procedures, process, etc.) that guide and validate what is being done is in alignment with business objectives, values, and commitments.

Unfortunately, history reveals many examples of epic control failures. Legendary examples include the sacking of Troy (giant horse-like vehicle not properly examined for unauthorized passengers prior to entry) to the Titanic (big boat with easily broken seam rivets and staff not adequately trained for proper evacuation). Modern corporate

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

demonstrations of internal control failures include Enron, Barings Bank, and WorldCom. These examples reveal internal controls have a material impact on people and sustained success of an organization. Today, the concept of internal control is commonly associated with financial governance and reporting. However, internal control has a much broader scope in meaning and application. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of reporting; and compliance with applicable laws and regulations (COSO, 2013). This definition is intentionally broad to allow flexible application across various types of organizations, industries, and geographic locations.

As vendors are engaged to perform key business functions, the scope of internal control must grow, too. Regulators, Stockholders, Board of Directors, and Consumers generally do not care if business functions are being performed using internal or vendor technology. The requirement remains in either case for reasonable assurance that business objectives will be met. Though duties and responsibility can be assigned to vendors—accountability and assurance cannot. Therefore, the adoption of Service Organizations has driven a requirement for Service Organization internal control transparency for customers. "Transparency" is another way of saying "audit". Logistically, it might not be practical for a customer auditor to perform on-site examination of all Service Organization internal controls, and it is not feasible for Service Organizations to accommodate each and every customer on-site audit request. Therefore, an authoritative guide was needed so Service Organizations could audit and report on their internal control performance to their customer.

Service Organization system and control audit methods associated with financial governance and reporting were the first to emerge. In 1992, the American Institute of Auditing Standard Statement on Auditing Standard No. 70 (SAS 70) provided Service Organization auditors a means of demonstrating sufficient assurance for financial internal controls associated with accounts, transactions, statements, and disclosures (AICPA,

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

1992). Service Organizations soon considered SAS 70 might be of value for purposes beyond auditor communication and financial reporting. SAS 70 began to be used for examination of operations and other areas unrelated to financial reporting, and became the poster child of audit standard scope creep. For example, SAS 70 audits and reports were used by the marketing teams inappropriately to demonstrate Service Organization effectiveness for security, privacy, and availability to prospect customers. The intended scope of SAS 70 was auditor-to-auditor communication regarding internal control over financial reporting only—not general public disclosure of internal control conditions.

After a long evolution in Service Organization control assessment and reporting, the American Institute of Certified Public Accountants (AICPA) created a new framework for Service Organization Control (SOC) reporting in 2010. This framework consists of SSAE 16 SOC 1, along with SOC 2 and SOC 3. In 2011, SSAE 16 SOC 1 officially replaced the SAS 70 put forth in 1992 (AICPA, 2013b). The new framework is intended to be adaptive and extensible to address control assurance broadly across all Service Organizations. Unfortunately, this flexibility has caused some confusion as far as SOC report purpose and applicability. This paper is intended to help explain the landscape of the new SOC 1-3 and SSAE 16 reporting.

NOTE: This document is not intended to provide legal advice. The purpose of this document is general public education; it is not a substitute for legal or other professional advice. Do not rely exclusively on this document for guidance on Service Organization audit report results and risk management. Consult appropriate legal counsel, audit team, vendor management team, and supply chain management team for questions regarding business obligations and risk appetite for your organization.

2. What are the benefits of this new audit framework?

The AICPA Service Organization Control (SOC) reporting framework is a major milestone for auditors having the duty of control assurance reporting. Several parties benefit from this audit framework including the customer, vendor, and auditor.

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

2.1. Benefits to Customer

A major benefit of SSAE 16 and SOC 1 reports for customers (also known as "user entity") is eliminating the misuse of SAS 70 beyond financial reporting. SSAE 16 and SOC 1 are scoped specifically for Internal Control for Financial Reporting (ICRF), including Information Technology General Controls (ITGC). For subject matters and internal control unrelated to financial reporting, SOC 2 and SOC 3 are offered. With SOC 2, customer organization auditors have an authoritative standard for communicating with Service Organization auditors when examining internal control associated with Security, Privacy, Availability, Processing Integrity, and Confidentiality. With SOC 3, prospect customers can confirm routine control examination is taking place and the recent results of the examination.

SSAE 16 is as much an attestation standard as an audit standard. The management and those in charge of governance of a Service Organization are required to attest the scope and the examination results are appropriate. Existing and prospect customers can take comfort knowing that the vendor did not simply rely on the auditor discovery process—management at the vendor must assert that the audit scope, understanding of the systems and control performance, and findings are correct.

2.2. Benefits to Vendor

Committing to SSAE 16 helps vendors demonstrate they understand their financial control environment is relevant and impactful internally as well as externally to their customer. Providing credible evidence of adequate internal control is a growing focus for Services Organizations to meet the customer demand for assurance. When the target customer is a publically traded company in the United States, investors will demand even greater transparency into financial governance to demonstrate SOX compliance. To be eligible as a candidate for a customer Request for Proposal (RFP), these reports are frequently required. In some cases, being able to provide a recent SSAE 16 report is the only way the Service Organization will get an invite to the dance. Absence of these reports might also result in the loss of existing customers.

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

SSAE 16 aligns with international standards including the International Standard on Assurance Engagements (ISAE) 3402 *Assurance Reports on Controls at a Service Organization* and Canadian Standard on Assurance Engagements (CSAE) 3416 *Reporting on Controls at a Service Organization*. Therefore, Service Organizations have the ability to deliver reporting worldwide. This represents significant cost avoidance for Service Organizations intending to provide services globally. More information about ISAE 3402 and CSAE 3416 is provided in Section 5 SSAE 16 related audit standards.

2.3. Benefits to Auditors

Prospect customers, existing customers, regulators, and board of directors are all demanding financial reporting and other subject matters. This results in greater demands for auditing to confirm the accuracy of reporting and adequacy of controls. The primary purpose of SAS 70 and subsequently SSAE 16 is to facilitate communication between auditors when all the customer financial statement relevant systems are not run by the customer internally.

During the initial phases of a vendor audit, all parties must come to an agreement of what is relevant and in scope to be audited. For SAS 70, a comprehensive description of the controls would customarily be provided to the auditor. However, the system to which the controls applied might not be clearly elaborated. SSAE 16 and SOC reports include the requirement for description of the system and management assertion to the fairness of description. This system description assists the auditors in confirming the design and adequacy of the controls based on the specifics of the system. In addition, this description helps auditors determine if the system is presented fairly and entirely without omission or distortion of relevant information. This is a significant improvement from SAS 70 approach.

3. Navigating between SSAE 16 and SOC Reports

SSAE 16 is the new generation of AICPA Professional Standards for reporting on controls at Service Organizations in the United States. This professional standard addresses examination engagements that are relevant to the user entity internal controls

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

over financial reporting. Specifically, controls in scope for examination are those that a Service Organization implements to prevent, or detect and correct, errors or omissions in the financial information it provides to customers. This includes relevant IT General Controls (ITGC). Examples of Service Organizations in scope for SSAE 16 are those that provide hosted financial management systems, web based loan processing, SAS financial close and reporting systems, on-line payment processing, and Cloud Enterprise Resource Planning (ERP) services. SSAE 16 was made effective June 15, 2011 and requires an annual commitment by Service Organizations to examination by an auditor. (AICPA, 2011b).

A Service Organization must engage an independent auditor to perform the SSAE 16 examination. Service Organization internal auditors are not permitted to conduct the SSAE examination, though the external auditor may choose to use recent internal audit findings to support conclusions. However, the external auditor is entirely and solely responsibility for the opinion expressed in the audit report.

All SSAE 16 and SOC reports must clearly describe the following (AICPA, 2013b):

- ✓ Boundaries of the system and interfaces with other systems
- ✓ System design and implementation
- ✓ Necessary controls

These three areas scope the management assertion and the auditor opinion. The reader of the SOC report is advised to confirm that this description matches their expectation including that of the master service agreement contracted obligations. This description is valuable to auditors and customers to ensure no significant omissions or misrepresentations exist.

Not all Service Organizations will offer SSAE 16 reports to customer auditors. As the variety of cloud offerings continue to grow to serve new business functions (e.g., system infrastructure, storage, video content, IT Management systems, email, social networking, non-financial business systems like Contract Management and Human Resources Information Systems, etc.), many of the solutions are not relevant to financial

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

governance and reporting. In these cases, the customer would expect a SOC 2 or SOC 3 report for subject matter not related to financial controls. In the Cloud Security Alliance (CSA) Position Paper on AICPA Service Organization Control Reports, Service Organizations are advised to consider the need to pursue both SSAE 16 (SOC1) and SOC 2. AICPA guidance is referenced to support this CSA guidance. It states, "Service Organizations will now need to request two separate SOC reports if the Service Organization would like to address control objectives relevant to user entities ICRF and control objectives (criteria) that are not relevant to the user entities' ICRF. See paragraph 1.23 of the SOC 2 guide." (AICPA, 2011d).

Many folks have the misconception that there is an official certification associated with this examination. In fact, there is no certification, validation, or seal for SSAE 16 and SOC 1 at this time. The SSAE 16 report is intended to be shared with existing user entities to facilitate auditor-to-auditor communication--not as a sales tool for prospect customers. Most likely the report contains a statement restricting the distribution and use of the report. To acquire a "seal of approval" for non-financial controls, Service Organizations must commit to additional examinations that produce a SOC 3 report.

3.1. SOC 1

With the new AICPA professional standards, an audit that is conducted under SSAE 16 will result in a Service Organization Control (SOC) 1 report. These reports are still focused on controls that have a direct and credible relationship to financial governance and transaction processing—other subject matter is out of scope. In essence, a SOC 1 report will be the deliverable once the SSAE 16 audit is complete. In practice, SSAE 16, AT 801, and SOC 1 are used synonymously.

3.2. SOC 2

Essentially, SOC 2 provides what is missing from SAS 70 and SSAE 16 – evaluation of outsourcing vendor risks beyond those associated with financial reporting (e.g., Co-location and Data Centers, IT systems management, Cloud-based Infrastructure Providers, and Managed Security Service Providers). The primary focus for SOC 2 is the

© 2014 The SANS Institute Author retains full rights.

operational domain of controls. SOC 2 reporting uses the AT Section 101 practitioner standard. The following five Trust Services Principles (and related criteria) developed by AICPA are used by practitioners to perform SOC 2 engagements (AICPA, 2009):

- Security - The system is protected against unauthorized access (both physical and logical)
- Availability - The system is available for operation and use as committed or agreed
- Processing integrity - System processing is complete, accurate, timely and authorized;
- Confidentiality - Information designated as confidential is protected as committed or agreed
- Privacy - Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants

This approach provides a benchmark by which two similar service providers can be compared using the same set of evaluation criteria.

It is important to mention that an outsourcing vendor may choose to examine all or some of the five Trust Services Principles. This is an important consideration during Requests for Proposal (RFP) and vendor evaluations. The Service organization determines which domains are relevant to their customer. However, a Service Organization must successfully complete their examination of all five Trust Service Principles and associated Criteria to claim the SOC 3 SysTrust/WebTrust) seal.

Like SOC 1, the SOC 2 report is confidential and intended for existing customer auditors. Prospect customers or consumers of customer products can review a summarized conclusion of the audit with SOC 3 report.

3.3. SOC 3

SOC 3 satisfies the demand Service Organizations have been begging for – Certification! Once the auditor is assured that the vendor has achieved requirements of the Trust Services criteria, the vendor can display the SOC 3 SysTrust (WebTrust for website) for Service Organizations seal. SOC 3 reports provide the same level of

© 2014 The SANS Institute Author retains full rights.

assurance about controls over security, availability, processing integrity, confidentiality and/or privacy as a SOC 2 report. The difference is the intended audience for the reports. Whereas the SOC 2 report is intended for auditors, the SOC 3 report is intended for general release (prospect customers). The SOC 3 report does not contain the detailed description of the testing by the audit, but rather, a summary opinion regarding the effectiveness of the controls in place at the Service Organization.

3.4. Type 1 Report

As with the old SAS 70, SOC reports are available as Type 1 or Type 2 reports. In a Type 1 report, the service auditor will express an opinion and report on the subject matter provided by the management of the Service Organization as to (1) whether the Service Organization's description of its system fairly presents the Service Organization's system that was designed and implemented as of a specific date; and (2) whether the controls stated in management's description of the Service Organization's system were suitably designed to achieve those control objectives--also as of a specified date. (AICPA, 2011a)

3.5. Type 2 Report

For Type 2 SOC reports, the Service Organization must demonstrate the controls were sustained—not just present during the period of audit examination. A Type 2 SOC report includes the Type 1 criteria as well as (3) examines the operating effectiveness of the controls throughout a declared time period, generally between six months and one year. (AICPA, 2011a)

Frankly, customers should expect to receive a Type 2 report from a Service Organization. Examining a short point in time is not generally adequate to demonstrate sustained due care and continuous regulatory compliance.

4. Navigating within a SSAE 16 SOC 1 Report

The SAS 70 and SSAE 16 reports are still substantially similar except for the addition of management assertion. There are five sections including:

© 2014 The SANS Institute Author retains full rights.

- ✓ Auditor opinion
- ✓ Management assertion
- ✓ Description of Service Organization system and controls
- ✓ Auditor's description of testing and results
- ✓ (Optional) Information provided by Management

This paper does not include a sample SSAE 16 SOC 1 report. Illustrative auditor reports are provided for reference in AICPA AT Section 801 Reporting on Controls at a Service Organization Appendix A and B (AICPA, 2013b).

4.1. Auditor Opinion

SSAE and SOC reports must be provided by an unbiased and skilled practitioner. The first item of the report to confirm is the independence of the Service Organization auditor. The firm that performs the assessment should also be reviewed for reputation in this area of audit. The auditor responsibilities are defined within the report. This helps the reader better distinguish the difference in roles between the auditor and management.

According to AICPA, SSAE 16 auditor opinion is organized into essentially four elements (AICPA, 2013b):

1. Management's description of the Service Organization's system fairly presents the Service Organization's system that was designed and implemented throughout the specified period.

2. The controls related to the control objectives stated in management's description of the Service Organization's system were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the specified period.

3. The controls the service auditor tested, which were those necessary to provide reasonable assurance that the control objectives stated in management's description of the Service Organization's system were achieved, operated effectively throughout the specified period.

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

4. If the application of complementary user entity controls is necessary to achieve the related control objectives stated in management's description of the Service Organization's system, a reference to this condition.

The auditor must clearly state their opinion on the appropriateness and condition of the service provider's system and controls by speaking to the four aforementioned elements. For SSAE 16, the scope is defined by financial domain of controls. As mentioned earlier, the Service Organization may elect for SOC 2 to assess only certain Trust Service Principles (TSP) and associated criteria—not all five. For SOC 2, the reader is advised to confirm the assessment scope includes TSP in entirety.

The report will include a date for rendering the opinion as well as the timing of assessment applicability. For Type 1 reports, there will only be a specific date. For Type 2 reports, the report will address an examination of controls for duration of time six months to one year.

4.2. Management Assertion

Of course, one of the main purposes of SSAE 16 and SOC reports is to provide valid answers for management's question, "how do we know commercially reasonable practices are in-place and controls are effective?" In performing these audits for management, the Service Organization will be able to demonstrate credible third-party evidence the system and associated controls are in place and working as intended. For example, accounting practices are inspected, IT logical access is reviewed for least privilege, and segregation of duties is confirmed. Another objective of auditing and function of the auditor is to act as a tool of management to measure and report on risk (SANS, 2010). The SOC reports formally document risk conditions that threaten fulfillment of these commitments. When the Service Organization shares these SOC reports with their customer, the customer has the opportunity to conduct informed risk management decisions.

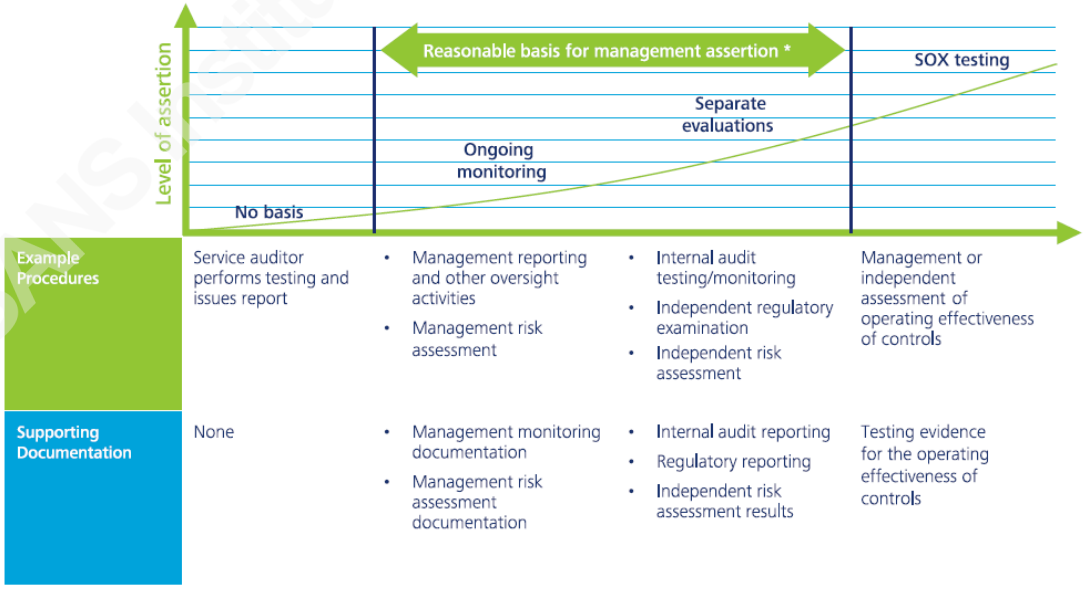
As mentioned earlier, a major difference between SAS 70 and SSAE 16 is the transition from audit to attestation. Now, management must acknowledge in writing that

© 2014 The SANS Institute Author retains full rights.

the system and control description presented for audit are fair and adequate. This is intended to ensure no information is purposely omitted or distorted simply to pass the audit. The auditor then examines the suitability of criteria to support the attestation. Criteria are the standards or benchmarks used to measure and present the subject matter against which the auditor evaluates the subject matter (AICPA, 2013b). In other words, management must have a credible basis for providing their assertion. They must explain why they have reason to believe the controls are appropriately designed and operating effectively. Lastly, management must reveal any significant changes to the system and controls. Management acknowledgement and commitment to this responsibility is a key component of the SOC report. Collectively, these changes improve audit performance and ensure management has more "skin in the game".

The following picture from Deloitte relates internal controls procedures to level of assertion for establishing a reasonable basis for management assertion (Deloitte, 2013):

Figure 1: *ISAE 3402 and SSAE 16 (replacing SAS 70) Reinforcing confidence through demonstration of effective controls* page 5



Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

4.3. Description of Service Organization System

A core requirement of SSAE 16 is comprehensive description of the Service Organization "system" in scope. This is a new concept that was not present in SAS 70. With SAS 70, the auditor provided a description of the controls, but not the Service Organization framework used to deliver services. The description of the system provides a detailed narrative of the services provided as well as supporting processes, policies, standards, procedures, technology, resources, and operational aspects relevant to service to customer. According to TSP Section 100, a system consists of 5 key components (AICPA, 2009):

- Infrastructure - The physical and hardware components of a system (facilities, equipment, and networks)
- Software -The programs and operating software of a system (systems, applications, and utilities)
- People -The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- Procedures - The programmed and manual procedures involved in the operation of a system (automated and manual)
- Data - The information used and supported by a system (transaction streams, files, databases, and tables)

The system description identifies the boundaries and scope of examination. Also note that the system and associated controls described are expected to be in-place during examination—not in-plan. The auditor is required to confirm these have been implemented entirely.

In some cases, the customer (user entity) might be obligated to perform duties as part of the system and control effectiveness. These user entity complementary controls must be described as part of the report. Administration of Logical Access Controls including creation of accounts, authorization of access, and routine entitlement review of customer staff is a common example of user entity complementary controls. The Service

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

Organization depends on their customer to perform this function because only the customer can qualify individual employee need to know.

Lastly, the vendor might elect to sub-contract some of the services. The SOC report reader is advised to determine if there are any sub-Service Organizations in use and if their role is material and necessitates additional risk evaluation. In some instances, the Service Organization may elect to separate system description and management assertion associated with the sub-service provider. When this "carve out" method is identified, the customer might elect to require a copy of the SOC report from the sub-service provider(s). This is common for application Service Organizations using a third-party data center hosting provider.

4.4. Auditor testing and results

Testing might be performed using sampling approach. The approach used is typically determined by the size of the Service Organization and number of customers. The auditor will typically use an authoritative standard for guidance on sampling approach (e.g., AU section 350, Audit Sampling) and will typically make a reference to this standard in the SOC report.

The SOC report reader is advised to read through the test procedure and results for each control to confirm the risk evaluation is substantially similar to their internal standard. Further, if any deficiencies or deviations have been identified, the test results might provide some insight into cause. This information can also be useful for risk evaluation by report reader.

4.5. (Optional) Information provided by Management

This section might contain future-oriented statements. The expectation is these statements are regarding system aspects or controls in-plan that will improve or enhance performance. The improvements might not be completely in-place during the time of examination, therefore not eligible for audit examination yet. However, the project planning or execution might be relevant to the next audit or customer demand. Examples of these near horizon statements include plans to build a redundant data center, upgrading

© 2014 The SANS Institute Author retains full rights.

to a new release of software, new safeguards, changing vendor partners, and improved business continuity management.

5. SSAE 16 related audit standards

5.1. ISAE 3402 – International version of SSAE 16

Globalization has opened doors for Service Organizations. Technically, SSAE 16 is a United States only standard. However, SSAE 16 provides better alignment than SAS 70 with the international audit standard ISAE 3402. ISAE 3402 is for Service Organizations located or delivering services outside United States. There are strong similarities between SSAE 16 and ISAE 3402. Therefore, services organizations must make only an incremental investment in examination when intending to maintain both audit standards.

5.2. CSAE 3416 – Canadian version of SSAE 16 SOC 1

The Canadian Institute of Chartered Accounts, Section 5970, *Auditor's Report on Controls at a Services Organization*, has been the authoritative standard to be applied by auditors in performing Service Organization assurance reports in Canada since 2006. The Canadian Auditing and Assurance Standards Board issued a new standard, Canadian Standard on Assurance Engagements (CSAE) 3416 *Reporting on Controls at a Service Organization*. As with SSAE 16, this standard takes effect for Service Organization assurance reports issued for reporting periods after December 2011.

This new standard aligns with the purpose and approach of ISAE 3402. They share a common scope for controls relevant to situations when the service impacts a customer financial reporting processes (including associated IT General Controls). Only minor variances exist between the Canadian and International standard. These differences were deemed necessary to avoid inconsistency with other Canadian Standards and to provide Canadian specific guidance. Canadian standards for examination of controls not relevant to financial reporting are performed using Section 5025, *Standards*

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

for Assurance Engagements Other than Audits of Financial Statements and other historical financial information.

6. Report Selection and Review

Report selection starts with determining if the report request is pre or post sale. For prospect customers, requesting a recent SOC 3 report is most appropriate. This report is intended for public disclosure (i.e., marketing) and demonstrates the Service Organization commitment to protecting customer information and systems. If the Service Organization would be in scope for SOX or financial reporting, then a request for SSAE 16 (SOC 1) report would be appropriate. For services delivered internationally, the ISAE 3402 would be more appropriate.

When conducting a Request for Proposal (RFP) or negotiating contracts with Service Organizations, consider including terms that require yearly audits by a credible audit firm and timely presentation of reports. Depending on the customer risk appetite, it might be appropriate to include the contract option for early contract termination if the SOC reports are not presented in a timely manner or a serious deficiency is reported by the Service Organization auditor.

Remember requesting both SOC 1 and SOC 2 reports might be appropriate depending on the Service Organization. A cloud Enterprise Resource Planning (ERP) vendor is an example of when both reports are of value. Further, Type 2 reports (also identified as Type II reports to avoid confusion with SOC 2) are ideal as they demonstrate that the controls are effective and sustained. Appendix B provides more guidance on report selection.

When reviewing the reports, there are several components to look for. Appendix A provides a review checklist for a SSAE 16 SOC 1 report. Generally, the auditor opinion is the report component requiring the most customer attention. If the opinion is qualified because control objectives failed, the customer must determine if the failed control objectives are relevant and material to them. Results of testing can be insightful

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

when this condition is reported. The customer may want to exercise the right for further examination of system and internal controls to clarify how directly impactful the discovered deficiencies are. If sampling was used during the audit, the customer might elect to have additional auditing performed (possibly at their expense) to evaluate relevant controls not included in the initial audit sample. If there is a carve-out because of the use of sub-service providers, then the customer might need to ask for the sub-service provider SOC report to understand the entire risk picture. Lastly, understanding obligations associated with complimentary user entity controls is important. User entity controls are not examined by the Service Organization auditor. This is the obligation of the customer.

7. Conclusion

The SSAE and SOC 1 reporting framework are an evolution of the SAS 70 reporting from 1992. Now, Service Organizations have the ability to offer customer auditors assurance reports regarding controls relevant to financial reporting. With the introduction of SOC 2 and SOC 3, a broader scope of subject matter and controls can be examined using a credible authoritative standard of Trust Service Principles. Service Organizations can now offer existing and prospect customers assurance regarding the condition of operations and controls associated with security, availability, processing integrity, confidentiality, and privacy. Collectively, these reports promote customer trust, investor confidence, management accountability, auditor efficiency, enhanced reputation, and marketing appeal.

8. References

AICPA. (1992). *Reports on the processing of transactions by service organizations.* Retrieved from http://umiss.lib.olemiss.edu:82/articles/1038093.6671/1.PDF

AICPA. (2001). *Attest Engagements, AT Section 101.* Retrieved from http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00101.pdf

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 The SANS Institute Author retains full rights.

AICPA. (2009). *TSP Section 100: Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Durham, NC: AICPA.

AICPA. (2011a). *FAQs – New Service Organization Standards and Implementation Guidance.* New York, NY: AICPA

AICPA. (2011b). *Service Organizations: New Reporting Options Alert, Strengthening Engagement Integrity Safeguarding Reporting*. New York, NY: AICPA.

AICPA. (2011c). *Service Organizations: Applying SSAE No. 16, Reporting on Controls at a Service Organization (SOC1).* New York, NY: AICPA.

AICPA. (2011d). *Technical Practice Aid TIS Section 9530: Service Organization Control Reports.* Retrieved from http://www.aicpa.org/InterestAreas/FRC/DownloadableDocuments/TIS_Sections/TIS_Section_9530.pdf

AICPA. (2013a). *Assessing and Responding to Audit Risk; International Auditing Standards.* New York, NY: AICPA.

AICPA. (2013b). *Reporting on Controls at a Service Organization, SSAE No. 16.* New York, NY: AICPA.

AICPA. (2013c). *Service Organization Control Reports; Considerations for User and Service Auditors*. New York, NY: AICPA.

AICPA. (2013d). *Service Organization Controls; Managing Risk by Obtaining a Service Auditor's Report.* New York, NY: AICPA.

Auditwerx. (2013). *The Anatomy and Need for an SSAE 16 Audit.* Retrieved from http://www.auditwerx.com/e-books/Auditwerx_Anatomy-and-Need-for-an-SSAE-16.pdf

Crowe Horwath. (2012). *Goodbye, SAS 70! Hello, SSAE 16! Insight on the New Standard & What End-Users Need to Know*. Retrieved from http://conference.csiweb.com/goodbyesas70_hellossae16.pdf

CSA. (2013). *Cloud Security Alliance Position Paper on AICPA Service Organization Control Reports.* Retrieved from https://cloudsecurityalliance.org/download/csa-position-paper-on-aicpa-service-organization-control-reports/

COSO. (2013). *Integrated Framework – Internal Control*. Durham, NC: AICPA

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

Deloitte. (2013). *ISAE 3402 and SSAE 16 (replacing SAS 70) Reinforcing confidence through demonstration of effective controls.* Retrieved from http://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/RA_ISAE_3402_and_SSAE_16.pdf

Deloitte. (2011). *Making the move from SAS 70 to SSAE 16*. Retrieved from http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_FOCT_SAS%2070_%20to_%20SSAE%20_16.pdf

IFAC. (2013). *2013 Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements.* New York, NY: International Federation of Accountants

Klein, M. (2011). *SAS 70, SSAE 16, SOC and Data Center Standards*. Retrieved from http://resource.onlinetech.com/sas-70-ssae-16-soc-2-and-soc-3-data-center-standards

KPMG. (2012). *Effectively using SOC1, SOC 2, and SOC 3 reports for increased assurance over outsourced operations.* Retrieved from http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/SOCWhitepaper.pdf

PWC. (2011). *Navigating the transition to CSAE 3416.* Retrieved from http://www.pwc.com/ca/en/controls/business-process-controls/navigating-transition-csae-3416.jhtml

SANS. (2010). *SANS 507.1 Audit Principles, Risk Assessment, and Effective Reporting.* SANS Institute.

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

APPENDIX A: Review Checklist for SSAE 16 Report

Auditor Opinion

- Auditor is independent and reputable?
- Auditor's responsibilities stated?
- Opinion qualified or unqualified and impact of deficiencies?
- Fairness of management's description of service confirmed?
- Controls suitably designed to achieve objectives?
- Controls tested demonstrated operating effectiveness during single point in time (Type I) or entire reporting period (Type II)?
- Date of audit opinion timely?
- Opinion inclusive of subService Organizations or carve out used?
- Modified auditor opinion present?

Management Assertion

- Date range for audit applicability appropriate?
- Service organization's responsibilities stated?
- Commitment that description of the System presented fairly?
- Any relevant changes to System and controls?

Description of System and Controls

- Description of System comprehensive and adequate?
- System boundaries and interfaces described clearly?
- Description of controls comprehensive and adequate?
- Control objectives met?
- System and Control design match internal standards?
- System reflects services contracted?
- Is there a requirement for complementary user entity controls?
- Description of System and Control match contract SOW?

Testing and Results

- Are specific control tests and associated results listed?
- Was sampling used for testing and what authoritative sampling standard was used?
- Were complementary user entity controls tested?
- Any test exemptions or errors?

(Optional) Information provided by Management

- Any in-plan system or control changes?
- Any DR or BCP plans?
- Any new services planned?
- Any new software versions planned?
- Any planned infrastructure changes?
- Any new sub-organizations planned?

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

APPENDIX B: Comparison of SSAE and SOC Reports

	SSAE 16 / SOC 1	SOC 2	SOC 3
Guidance	AICPA Attest Engagements AT 801	AICPA Attest Engagements AT 101	AICPA Attest Engagements AT 101
Audience	Service Management, Auditor, Customer Controller and CFO	Service Management, Auditor, Customer CIO, CSO, or CPO	Customer Business Management Or CIO
Author	Service Auditor	Service Auditor	Service Auditor
Purpose	ICFR	GRC	Marketing
Content	Auditor Opinion, System Description Control Description Management Assertion Testing and Results	Auditor Opinion, System Description Control Description Management Assertion Testing and Results	Auditor Opinion, System Description Management Assertion
System Scope	Classes of transactions Procedures and Policies Accounting records Report preparation	Infrastructure Software Procedures People Data	Infrastructure Software Procedures People Data
Control Domains	Transaction processing ITGC	Security Availability Confidentiality Processing Integrity Privacy	Security Availability Confidentiality Processing Integrity Privacy
Frequency	Yearly	Yearly	Yearly
Vendors	Financial management systems, Loan processing, Financial close and reporting systems, Payment processing, ERP	Data Centers, Cloud Computing, Infrastructure, Storage, Virtual Servers, video content, IT Mgt systems, HRIS Non-financial applications	Data Centers, Cloud Computing, Infrastructure, Storage, Virtual Servers, video content, IT Mgt systems, HRIS Non-financial applications
International Equivalent	ISAE 3402 CSAE 3416	Section 5025	

Author: Michael Hoehl, mmhoehl@gmail.com

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced