PARAGON

AUDIT & CONSULTING, INC.

Understanding and Evaluating Service Organization Controls (SOC) Reports

OR

Agenda

1. Why are SOC reports important?
2. Understanding the new SOC-1, SOC-2, and SOC-3 Reports.
3. How to read a SOC Report.
4. What are “inclusive” and “carve out” reports for sub-service providers?
5. What is a “Gap” or “Comfort” Letter and why is important?
6. How to document the review of a SOC Report for the external auditors.

Why is a SOC Report Important?

- What risk are you mitigating by outsourcing?
  - Strategic
  - Compliance
  - Financial
  - Operational
  - Reputational
  - Technology
- Risk Management/Mitigation
  - Acceptance
  - Avoidance
  - Limitation
  - Transfer

What is a SOC Report?

- SOC reports are often prepared by service organizations in lieu of multiple clients sending teams of auditors to perform individual audits under audit clauses included in the service contract.
- A service provider engages a CPA (service auditor) to perform an examination of controls at the service provider, resulting in a SOC report with detailed information about those controls.
- The service auditor's report includes opinions on whether the description of the service provider's system is fairly presented and whether controls at the service provider that may affect user entities' financial reporting are suitably designed.

Why is a SOC Report Important?

- Good Vendor Management
  - Once the relationship with the vendor has begun, don't assume that everything will go according to plan. The vendor's performance must be monitored from the beginning.
  - Include an audit clause in the service provider contract.
  - Request a SOC report during due diligence.

Why is a SOC Report Important?

- Regulatory Context
  - **COSO 2013** Principle 16: Conducts Ongoing and/or Separate Evaluations
  - **FFIEC**
    - Outsourcing Technology Services
    - Supervision of Technology Service Providers
  - **GLBA** – Management of security for contractors and third-party service providers
  - **PCI** - Appendix A: Additional PCI-DSS Requirements for Shared Hosting Providers
  - **IRS** - The employer is ultimately responsible for the deposit and payment of federal tax liabilities.
  - **HIPAA** – Covered Entities and Business Associate

Why is a SOC Report Important?

- Many companies function more **efficiently and profitably** by outsourcing tasks or entire functions to service organizations that have the personnel, expertise, equipment, or technology to accomplish these tasks or functions.
- Although user management can delegate tasks or functions to a service organization, **user management is usually held responsible** by those charged with governance, such as the board of directors, customers, shareholders, regulators and other affected parties for establishing effective controls over those outsourced functions.
- SOC reports provide user management with the information they need about a **service organization's controls** to help user management assess and address the risks associated with the outsourced service.

What is a Service Organization?

- **Service organizations** are typically entities that provide outsourcing services that impact the control environment of their customers.

Software as a Service (SaaS)	Social Media / Content Tagging and Aggregators	Online Fulfillment
Application Service Providers (ASP)	Data Center and Co-Location Providers	Rebate Processing / Online and Mail
Credit Card Processing Platforms	Managed Services	Transportation Services
Cloud Computing / Virtualization	Third Party Administrators (TPA)	Tax Processing and Filing Services
Internet Service Providers (ISP)	Medical Billing	Payroll Services
Web Design and Development	Print and Mail Delivery	Registered Investment Advisors (RIA)
Web Hosting	Security as a Service	Financial Statement XBRL Tagging

Key Players

Service Organization
An entity that processes information
or handles business transactions on
behalf of its customers (user entities)

Service Auditor
A CPA who reports on controls at a service organization

User Entity
The company that outsources its business processes to a service organization

SOC Report Types

	Report Coverage	User Community
SOC 1	Internal controls over financial reporting	User entity auditors and service consumers
SOC 2	Security, availability, processing integrity, confidentiality, or privacy	User entities, potential customers, regulators, business associates, etc.
SOC 3	Security, availability, processing integrity, confidentiality, or privacy	Publicly available

What's the purpose of each report type?

SOC 1

- Gives the auditor of a user entity's financial statements information about controls at a service organization that may be relevant to a user entity's internal control over financial reporting.

SOC 2

- Gives management of a service organization, user entities and others a report about controls at a service organization relevant to the **security**, **availability** or **processing integrity** of the service organization's system, or the **confidentiality** and **privacy** of the data processed by that system.

SOC 3

- Gives users and interested parties a report about controls at the service organization related to security, availability, processing integrity, confidentiality or privacy. SOC 3 reports are a short-form report (i.e., no description of tests of controls and results) and may be used in a service organization's marketing efforts.

Type 1 and Type 2

- Under the new AICPA reporting standards, an audit that is conducted under SSAE 16 will result in a Service Organization Control (SOC) 1 report.
- As with the old SAS 70, SOC 1 reports will be available as Type 1 or Type 2 reports.

Type 1
Presents the auditors' opinion regarding the accuracy and completeness of management's description of the system or service as well as the suitability of the **design of controls** as of a specific date.

Type 2
Includes the Type 1 criteria AND audits the operating **effectiveness of the controls** throughout a declared time period, generally between six months and one year. Like SAS 70, there is no official SSAE 16 or SOC 1 certification.

SOC 1 Report

- Since a SOC 1 is designed to report on controls surrounding financial reporting (Sarbanes-Oxley focused), there are certain aspects of the control environment that may be excluded from testing:
  - Business Continuity Planning
  - Disaster Recovery
  - Secure Storage & Destruction of Sensitive Data/Documents
  - Private Key Infrastructure / Encryption
  - Vulnerability Assessment and Penetration Testing
  - Secure Coding

SOC 2 and SOC 3 Reports

- SOC 2 and SOC 3 have stringent audit requirements with a stronger set of controls and requirements.
- SOC 2 and SOC 3 provide a standard benchmark by which two data centers or similar service organizations can be compared against the same set of criteria.
- In contrast to an SSAE-16 engagement, where the service organization defines the scope of the service offering and the control objectives for an audit, SOC 2 and SOC 3 Report use pre-defined control frameworks (**Trust Service Principles**).
- SOC 2 and SOC 3 are AT Section 101 Attest Engagements are generally not usable for Sarbanes-Oxley purposes.

SOC 2 and SOC 3 Reports

- SOC 3 Reports provide the same level of assurance as a SOC 2 Report, but the report is intended for general release.
- SOC 3 Reports do not contain the detailed description of the testing performed by the auditor, but rather, a summary opinion regarding the effectiveness of the controls in place at the data center or service organization.
- For SOC 3, once the auditor is assured that the data center operator has achieved the trust services criteria, the company can display the SOC 3: SysTrust for Service Organizations seal.
- The AICPA and CPA Canada have jointly decided to discontinue the SysTrust and SOC 3 SysTrust for Service Organizations seal programs. Seals will continue to be issued until December 31, 2014.

SOC 2 and SOC 3 Reports

Trust Service Principle		Applicability
Security	The system is protected against unauthorized access (both physical and logical).	• Most commonly requested area of coverage • Security criteria are also incorporated into the other principles because security controls provide a foundation for the other domains. • Applicable to all outsourced environments, particularly where enterprise users require assurance regarding the service provider's security controls for any system, nonfinancial or financial.
Availability	The system is available for operation and use as committed or agreed.	• Second most commonly requested area of coverage, particularly where disaster recovery is provided as part of the standard service offering. • Most applicable where enterprise users require assurance regarding processes to achieve system availability SLAs as well as disaster recovery which cannot be covered as part of SOC 1 reports.

SOC 2 and SOC 3 Reports

Trust Service Principle		Applicability
Confidentiality	Information designated as confidential is protected as committed or agreed.	• Most applicable where the user requires additional assurance regarding the service provider's practices for protecting sensitive business information.
Processing Integrity	System processing is complete, accurate, timely, and authorized.	• Potentially applicable for a wide variety of nonfinancial, and financial scenarios wherever assurance is required as to the completeness, accuracy, timeliness, and authorization of system processing.
Privacy	Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA.	• Most applicable where the service provider interacts directly with end users and gathers their personal information. • Provides a strong mechanism for demonstrating the effectiveness of controls for a privacy program

SOC 2 and SOC 3 Reports

Sample Coverage by Trust Services Principle

Security

- IT security policy
- Security awareness, and communication
- Risk assessment
- Logical access
- Physical access
- Security monitoring
- User authentication
- Incident management
- Asset classification, and management
- Systems development, and maintenance
- Personnel security
- Configuration management
- Change management
- Monitoring, and compliance

Availability

- Availability policy
- Backup, and restoration
- Environmental controls
- Disaster recovery
- Business continuity management

Processing Integrity

- System processing integrity policies
- Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs
- Information tracing from source to disposition

Confidentiality

- Confidentiality policy
- Confidentiality of inputs
- Confidentiality of data processing
- Confidentiality of outputs
- Information disclosures (including third parties)
- Confidentiality of Information in systems development

Privacy

- Management
- Notice
- Choice and consent
- Collection, use and retention
- Access
- Disclosure to third parties
- Quality
- Monitoring and enforcement

What Does a SOC Report Look Like?

- **Contents**
  - Independent Service Auditor Report
  - Management Assertions
  - Overview of Operations
  - Relevant Aspects of the Control Environment
  - Description of the System
  - Description of Control Objectives, Control and Results of Testing
  - Complementary User Entity Controls
  - Other Information Provided by Management

Independent Service Auditors Report

- Scope
- Service Organization's Responsibilities
- Service Auditor's Responsibilities
- Inherent Limitations
- Opinion (Unqualified / Qualified)

Management Assertions

- We confirm, to the best of our knowledge and belief, that:
  - The description fairly presents the general computer controls related to [name of service].
  - Whether or not any sub-service organizations are carved-out or included in the report.
  - The description includes relevant details of changes to system during the period covered by the description when the description covers a period of time.
  - The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period.
  - Subservice organizations applied the controls contemplated in the design of service organization's controls.

Overview of Operations

- Company profile.
- Description of the services covered within the scope of the audit.

Relevant Aspects of the Control Environment

- **Control Environment**
  - Communication and Enforcement of Integrity and Ethical Values
  - Commitment to Competence
  - Participation of Those Charged With Governance
  - Management Philosophy and Operating Style
  - Organizational Structure
  - Assignment of Authority and Responsibility
  - Human Resources Policies and Procedures
- **Risk Assessment**
- **Information and Communication**

Relevant Aspects of the Control Environment

- **Monitoring**
  - Corporate Audit Services
  - Compliance
  - Subservice Organization Monitoring

Description of the System

- Detailed description of the service organization's "system".
- "System" includes policies and procedures designed, implemented and documented to provide a service to user entities.
- The "system" may include:
  - Sub-service organizations
  - Complimentary User Control Considerations

Description of Control Objectives, Control and Results of Testing

Traditional SAS 70, and SOC 1

Control Objective 1: XXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	• XXXXXX • XXXXXX	XXXXX
XXXXX	• XXXXXX • XXXXXX	XXXXX
–	• –	–

Control Objective 2: XXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	• XXXXXX • XXXXXX	XXXXX
XXXXX	• XXXXXX • XXXXXX	XXXXX
–	• –	–

Control Objective X: XXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	• XXXXXX • XXXXXX	XXXXX
XXXXX	• XXXXXX • XXXXXX	XXXXX
–	• –	–

SOC 2

Security Principle: The system is protected against authorized access (both physical, and logical).

1.0 Policies: The entity defines, and documents its policies for the security of its system.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• XXXXXX • XXXXXX	XXXXX
–	–	• –	–

2.0 Communications: The entity communicates its defined system security policies to responsible parties, and authorized users.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• XXXXXX • XXXXXX	XXXXX
–	–	• –	–

3.0 Procedures: The entity uses procedures to achieve its documented system security objectives in accordance with its defined policies.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• XXXXXX • XXXXXX	XXXXX
–	–	• –	–

4.0 Monitoring: The entity monitors the system, and takes action to maintain compliance with its defined system security policies.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• XXXXXX • XXXXXX	XXXXX
–	–	• –	–

Description of Control Objectives, Control and Results of Testing – SOC 1

Control Objective 7

Controls provide reasonable assurance that documentation for the opening and modification of client accounts is received, authenticated, and established completely, accurately, and timely on the applicable system.

	Control	Tests of Operating Effectiveness	Results of Testing
7.01	The Transition team member authenticates the client account opening request by verifying that the account opening checklist is supported by a conversion request form and client direction letter.	For a selection of new accounts, inspected conversion request forms and determined the Transition team member authenticated the requests by verifying that the account opening checklists were supported by conversion request forms and client direction letters.	No exceptions noted.
7.02	The Transition team member reviews the account set-up and determines if the account information is completely and accurately entered into the system. An account open notification email is then sent to the internal service team requesting review of coding and the account set-up.	For a selection of new accounts, inspected account open notification emails to determine if a transition team member reviewed the completeness and accuracy of the account set-up.	**Exception Noted:** Account open notification emails are sent to the internal service team requesting review of account set-up; however, the service team review is not formally documented.
	Management Response: Transition Services will implement internal processes to review and document the completeness and accuracy of account set-ups. Such processes were put in place during 4th quarter 2013 for new business and will be expanded to include changes to existing business in early 2014.		

Description of Control Objectives, Control and Results of Testing – SOC 2

Criteria	Control	Testing Performed by Service Auditor	Results of Tests
2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.			
	1. Security awareness sessions are in place and each non-Senior Executive employee is required to attend annually. During an employee's first year the training consists of reviewing the security awareness program and signing an acknowledgement. In subsequent years, [redacted] has implemented a quiz-based security awareness program where employees are required to complete a number of questions based on the security policy or other security awareness materials provided.	Selected a sample of employees and obtained the attendance sheets to ensure each employee participated in security awareness training within the previous year.	Deviations noted. For one of our ten samples selected, the employees' last security awareness training occurred more than one year ago in 2011. Although the employee did not complete the training in 2012 we validated training was completed subsequent to the audit period on January 14, 2013. In addition, we also noted that the Information System Technology Policy Manual (which is the focus of the security awareness training) is reviewed annually.
	2. Upon hire, each employee is required to sign an Information Security Policy Manual acknowledgement that they have read and will abide by the policies.	Selected a sample of employees hired during the testing period and obtained their signed information security policy acknowledgements to ensure existence.	No deviations noted.

Complementary User Entity Controls

- Controls that management of the service organization assumes, in the design of the service provided by the service organization, will be implemented by user entities, and which, if necessary to achieve the control objectives stated in management's description of the service organization's system, are identified as such in that description.

Dealing with Sub-Service Providers

Inclusive Method

- Method of addressing the services provided by a subservice organization whereby management's description of the service organization's system **includes a description of the nature of the services provided by the subservice organization as well as the subservice organization's relevant control objectives and related controls.**
- The sub-service provider is audited by the same service auditor as part of the “system” described in the report.
- The sub-service provider’s management assertions will also be included in the report along with the test of the sub-service provider’s controls.

Dealing with Sub-Service Providers

Carve-out method

- Method of addressing the services provided by a subservice organization whereby management's description of the service organization's system identifies the nature of the services performed by the subservice organization and **excludes from the description and from the scope of the service auditor's engagement**, the subservice organization's relevant control objectives and related controls.
- For Sarbanes-Oxley, if there is a carve-out, management should venture to acquire a SOC 1 for the sub-service provider. Depending on the control that the main service organization is relying upon, a SOC 2 may be acceptable.

Dealing with Sub-Service Providers

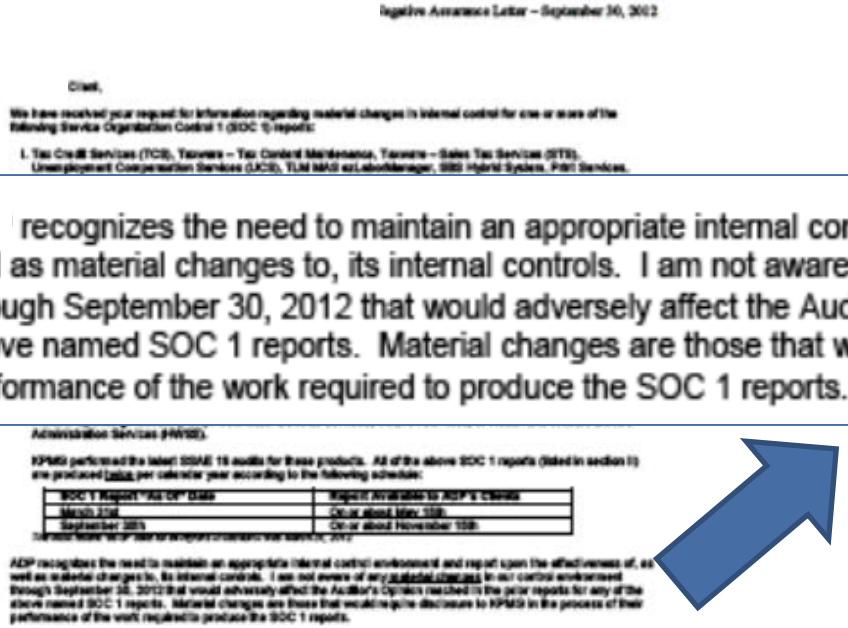
Carve-out method

- Getting a sub-service provider SOC Report
  1. Request that the primary service provider provide a copy of the report.
  2. Request a copy of a SOC 2 from the sub-service provider.
- Generally, the primary service organization has an obligation to address the services provided by the sub-service organization.
- As a downstream customer of the services provided by the sub-service organization, you are entitled to request, at a minimum, the SOC 1 or SOC 2 report that addresses the services that are being relied upon by the primary service organization.
- If you cannot get a SOC report for the sub-service organization, you need to evaluate the materiality and impact of that control on the user entity's system of internal controls.

Gap/Comfort/Bridge Letter

- Some SOC Reports cover a different time period than your fiscal year, say October 1 to September 30. If you are relying upon a SOC 1 for Sarbanes-Oxley, auditing standards require that you get assurances about the service organization's controls for your full fiscal year.
- You will need to get a "Bridge" Letter from the service organization covering the period from the end of the report through the end of your fiscal year. These are also referred to as "Gap", "Comfort", or "Negative Assurance" Letters.
- Many of the larger service organizations that have SOC reports for periods ending prior to December 31 will post these on their secure website for access by the authorized user entity representative.
- If not, the authorized user entity representative should request the letter from the service organization.

Gap/Comfort/Bridge Letter



recognizes the need to maintain an appropriate internal control environment and report upon the effectiveness of, as well as material changes to, its internal controls. I am not aware of any material changes in our control environment through September 30, 2012 that would adversely affect the Auditor's Opinion reached in the prior reports for any of the above named SOC 1 reports. Material changes are those that would require disclosure to in the process of their performance of the work required to produce the SOC 1 reports.

Documenting Your SOC Report Review

1. Perform a risk assessment to determine which service providers require review. From a vendor management perspective, you should review all SOC reports.
2. If the vendor does not provide a SOC:
   a. Request that the vendor provide a SOC if the service provided is significant.
   b. Determine if there is an audit clause. If so, is the impact significant enough to exercise the audit clause.
   c. If the vendor does not provide a SOC or there is not an audit clause, evaluate the level of risk you are assuming without sufficient visibility into the vendor's operation.
3. Determine the type of SOC Report (SOC 1, SOC 2, SOC 3 and Type 1 or Type 2)
4. Verify the scope of the report covers the services you are receiving.
5. Determine the time period covered by the report. Get Bridge Letter.
6. Verify the credentials of the service auditor.
7. Review the service auditor's opinion and management assertions.
8. Request and review SOC Reports for carved-out sub-service providers.
9. Review Service Auditor Exceptions and Management Action Plans.
10. Map User Entity Control Considerations to your internal controls.

Determine what type of report you have?

- If you are looking at a SOC 2, the scope should state which trust principles are being evaluated.

  We have examined the attached description titled Description of [Company] Hosting Services for the period July 1, 2012 through December 31, 2012"(the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the **security, availability and confidentiality** principles set forth in TSP section 100, *Trust Service Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids)* (applicable trust services criteria), throughout the period July 1, 2012 through December 31, 2012.

- There will be a section covering Trust Service Principles and Controls that are covered in the report.

Determine what type of report you have?

- If the scope states that it includes tests of operating effectiveness and covers a time period, then you are looking at a Type 2.

  > We have examined the attached description titled Description of [Company] Hosting Services for the period July 1, 2012 through December 31, 2012"(the description) and the **suitability of the design** and **operating effectiveness of controls** to meet the criteria for the security, availability and confidentiality principles set forth in TSP section 100, Trust Service Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services criteria), **throughout the period July 1, 2012 through December 31, 2012.**

- If the scope states that it only includes a review of the suitability of the design at a point in time, you are looking at a Type 1.
- Note that you will not be able to rely on a Type 1 report for Sarbanes-Oxley.

Verify the scope of the report

- Verify the scope of the report covers the services you are receiving.
- Also read the description of the system section.
- If the service(s) you are receiving is not covered by the report, ask the service organization if they have a different report covering the services that you are receiving.
- If you are using a co-location data center, make sure the report covers the data center(s) you are using.
- Be aware that some service organizations publish multiple SOC Reports. For example, many payroll service providers provide multiple reports. They may have one each for hosting, payroll tax, auto payments, withholding, flexible spending, etc.

Get a Bridge Letter

- Determine the time period covered by the report.
- Acquire a Bridge Letter if it does not cover your full fiscal year.

How to Review a SOC Report

- Determine what type of report you have (and need!).
- Verify that the services and locations match your expectations.

What kind of report is this?

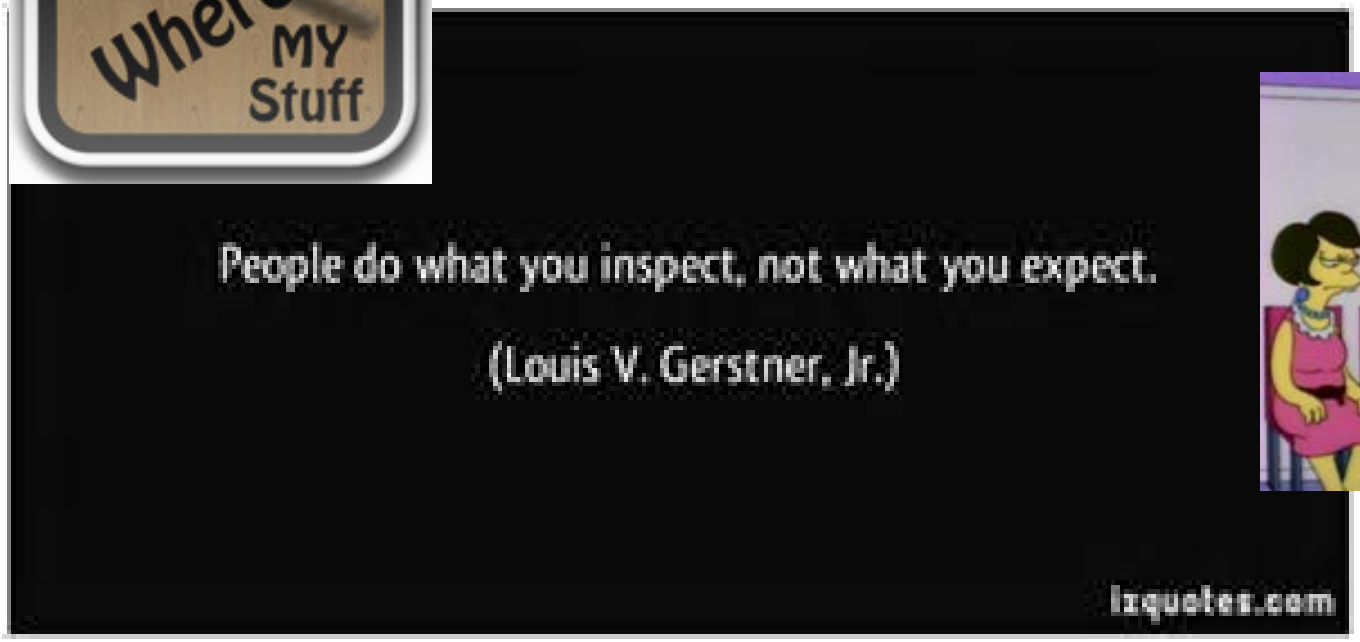
- If you are looking at a SOC 2, the scope should state which trust principles are being evaluated.

  We have examined the attached description titled Description of [Company] Hosting Services for the period July 1, 2012 through December 31, 2012"(the description) and the suitability of the design and operating effectiveness of controls **to meet the criteria for the security, availability and confidentiality principles set forth in TSP section 100, *Trust Service Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*** (AICPA, *Technical Practice Aids)* (applicable trust services criteria), throughout the period July 1, 2012 through December 31, 2012.

- There will be a section covering Trust Service Principles and Controls that are covered in the report.

Verify that services and locations match your expectations

- Read the description of the system!
- Verify that the services and locations match your expectations.

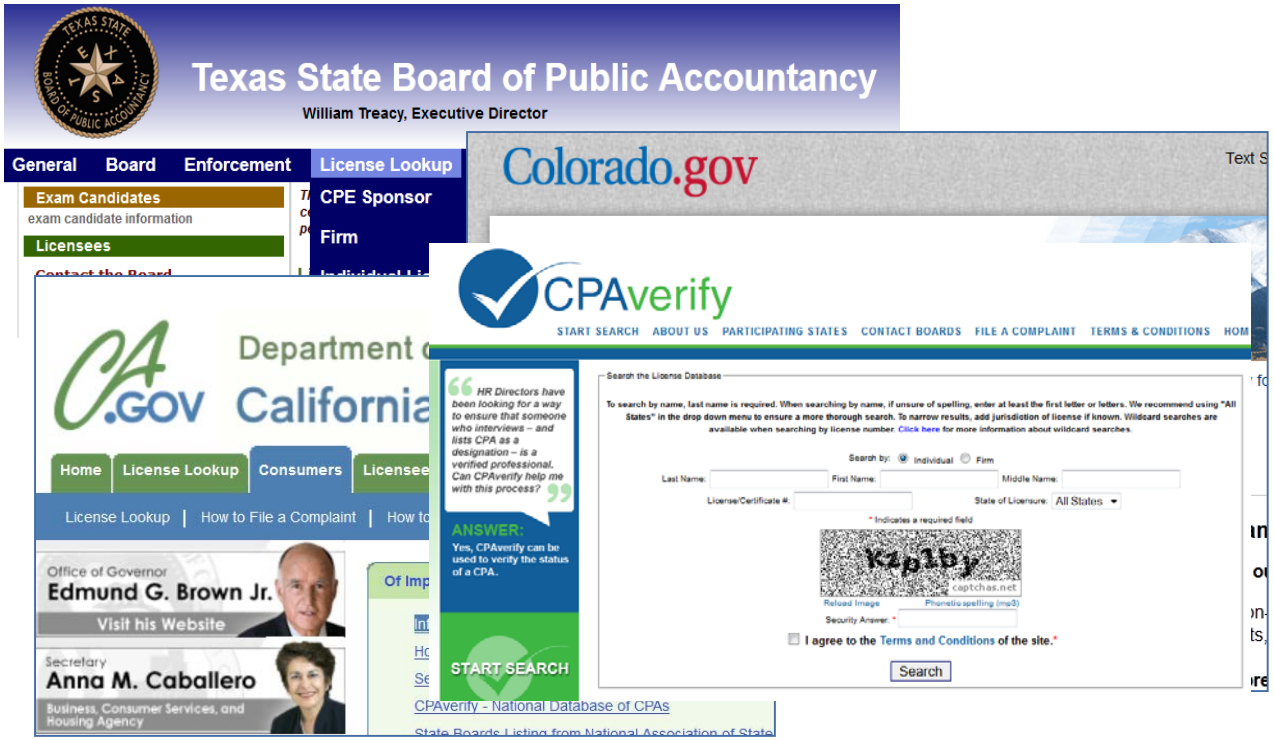


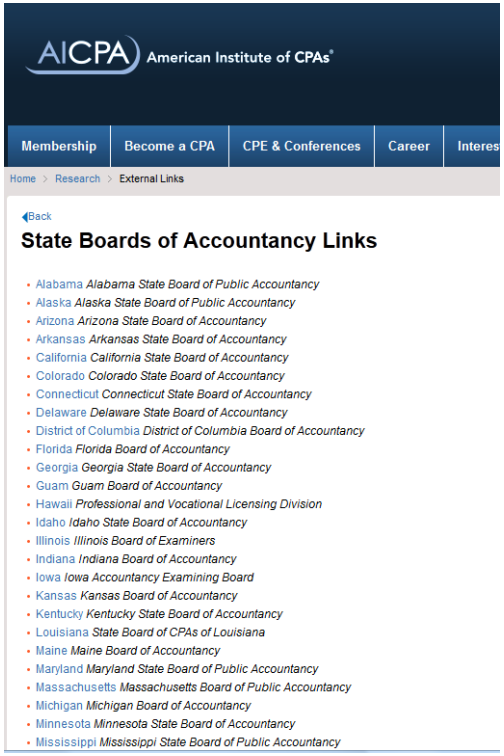
Verify the credentials of the service auditor

- If the service auditor is a well-known national firm, then a review may not be necessary.
- If the auditors issue audit reports on financial statements filed with the SEC, they must be registered with PCAOB.
- The PCAOB site shows the firm's registration, annual and special report filings, inspection reports and disciplinary actions, if any.
- http://pcaobus.org/Registration/Firms/Pages/RegisteredFirms.aspx

Verify the credentials of the service auditor

- Individual states also have sites to lookup licensees





http://www.aicpa.org/Research/ExternalLinks/Pages/StateBoardsofAccountancyLinks.aspx
http://www.cpaverify.org/

Review the Service Auditor's Opinion and Management Assertions

- Determine if the service auditor's opinion has any **qualifications**.
- If there are qualifications, determine the impact of the qualification(s) on the system described in the report and how that affects your business.
- Review management's assertions. Determine if there are any **scope limitations or unusual items** that impact the services that you are expecting.

SOC's for Sub-Service Providers

- Getting a sub-service provider SOC Report
  1. Request that the primary service provider provide a copy of the report.
  2. Request a copy of a SOC 1 or 2 from the sub-service provider.
- Generally, the primary service organization has an obligation to address the services provided by the sub-service organization.
- As a downstream customer of the services provided by the sub-service organization, you are entitled to request, at a minimum, the SOC 1 or SOC 2 report that addresses the services that are being relied upon by the primary service organization.
- If you cannot get a SOC report for the sub-service organization, you need to evaluate the materiality and impact of that control on the user entity's system of internal controls.

Service Auditor Exceptions and Management Action Plans

- Document all exceptions in the report and the service organization's action plan to remediate the issue.
- Based upon your review of the exceptions and management's action plans, determine whether or not you feel that the service organization has, or is in the process of, reinforcing and/or implementing sufficient procedures to address the exceptions and risks noted in the service auditor's report.
- Review prior years' reports.
- If the service organization is not addressing exceptions in the current period or if there are repeat exceptions from year-to-year, you may want to re-evaluate your relationship.

Map Client Control Considerations

- Service providers design applications under the assumption that certain controls would be implemented by user entities.
- For each client control consideration, identify and document (map) the control consideration to your internal control procedure that addresses the recommended control.
- This process may take time; however, client control considerations often do not change significantly from year-to-year.

Map Client Control Considerations

Client/User Control Consideration	How is this Control Implemented	Who is Responsible for Executing this Control?
Establishing controls to verify data is input and processed accurately and completely as supported by customer source documentation.	• Prior to transmission, the Payroll Department balances batch logs to the "Prepare/Edit" Report from the payroll system to ensure that all hours and dollars that have been entered manually match. • Payroll Department verifies payroll by individual for those employees that have special considerations that need to be reviewed back against time sheets or special pay adjustments or ERPAs. • If Payroll does not receive a timesheet, they will verify the employee's current status with the supervisor and/or HR. • On Tuesday of pay week, Payroll verifies that terminations processed by HR have been properly recorded/processed in the payroll system.	Bill Johnson-Payroll Mary Smith-HR
Establishing controls to verify customer process schedules are accurately updated in the payroll system Service Assistant (CSA) application.	In October of every year, the Payroll manager reviews the pay calendar for the upcoming year and makes the appropriate adjustments—if the calendar is not in the system, the payroll cannot be processed.	Bill Johnson-Payroll

Richard.Lucy@paragonaudit.com
720-245-6500