Understanding SOC 2
1) A brief perspective on where SOC 2 originated

2) SOC 2 defined and clarified

3) Important lessons from service organization controls reporting
Section 1

A BRIEF PERSPECTIVE ON WHERE SOC 2 ORIGINATED
AICPA replaced SAS 70

> Effective for audit periods ending after June 15
> Established the Statement of Control Framework (SOC Framework)

Why

> Confusion in the market – “we are SAS 70 certified”
> Frequently misused to report on controls not relevant to financial reporting – market demand for expanded scope of report

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy
Why - continued

> Growth of the service organization landscape
  - New technologies
  - Cloud computing (SAAS, PAAS, IAAS)

> Convergence of US and international standards

So what’s next?

> New attestation standard: SSAE 16 for SOC 1 reports

> AICPA issued implementation guides for SOC 1 and SOC 2
  - Service Organizations Applying Statement of Standard for Attestation No. 16 (SOC 1)
  - Reporting on Controls at a Service Organization (SOC 2)
### SOC Framework

#### SOC 1
**Service organization control 1**
- Applicable to services that are likely to be relevant to user entities' internal control over financial reporting
- Reports on controls supporting financial statement audits
- Restricted to customers during the audit period
- Example organizations: payroll processors, transaction processors

#### SOC 2
**Service organization control 2**
- Applicable to services that don’t directly impact financial reporting
- Reports on controls related to operations
- Restricted to those familiar with the subject matter
- Example organizations: Direct mailers, call centers

#### SOC 3
**Service organization control 3**
- Applicable to services that don’t directly impact financial reporting
- Reports on controls related to operations
- General use report
- Example organizations: Direct mailers, call centers
External factors

“Terrorism does remain the FBI's top priority, but in the not-too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country...”

- FBI Director Robert Mueller told a gathering of security professionals

Examples of controls breaches

> **Texas** data breach exposed 3.5 million records: Names, addresses, and social security numbers of state retirees and unemployment beneficiaries were posted, unencrypted, on a public server. (InformationWeek, April 13 2011)
  - Internal staff error

> **Bank of America** gets hit twice by internal staff: ATMs and data were compromised in separate attacks stemming from an employee theft of bank customer data and a multi-ATM heist perpetrated by a Diebold employee. (Bank Technology News – American Banker, May 2011)
  - Internal staff and vendor staff purposeful breach
Section 2

SOC 2 DEFINED AND CLARIFIED
What are trust services ("TS")?

A set of professional attestation and advisory services

> based on a core set of principles and criteria that addresses the risks and opportunities of IT-enabled systems and privacy programs.

Consists of five key components organized to achieve a specified objective.
Key components of trust services

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 (e.g. developers, operators, users, and managers)

Procedures
> The programmed and manual procedures involved in the operation of a system (automated or manual)

Data
> The information used and supported by a system (e.g. transaction streams, files, databases, and tables)
Defined criteria in five trust principle areas

> Privacy, security, availability, processing integrity, confidentiality

> Further subdivided into trust services criteria domains:
  - Policies
  - Communication
  - Procedures
  - Monitoring

A lot of overlap built into the criteria

> 51 unique criteria across security, availability, processing integrity, confidentiality

> Separate criteria specific to privacy
Principles Objectives

Security
The protection of the system from unauthorized access, both logical and physical

Availability
The accessibility to the system, products, or services as advertised or committed by contact, service-level, or other agreements

Processing integrity
The completeness, accuracy, validity, timeliness, and authorization of system processing

Confidentiality
The system’s ability to protect the information designated as confidential, as committed or agreed

Privacy
Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the privacy notice
Generally accepted privacy principles

Privacy principles

> Provides criteria and related material for protecting the privacy of personal information

> Incorporates concepts from significant domestic and international privacy laws, regulations, and guidelines

> Used to guide and assist organizations in implementing privacy programs

http://www.aicpa.org/privacy
<table>
<thead>
<tr>
<th></th>
<th>Generally accepted privacy principles (cont.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1)</td>
<td>Management</td>
</tr>
<tr>
<td>2)</td>
<td>Notice</td>
</tr>
<tr>
<td>3)</td>
<td>Choice and consent</td>
</tr>
<tr>
<td>4)</td>
<td>Collection</td>
</tr>
<tr>
<td>5)</td>
<td>Use and retention</td>
</tr>
<tr>
<td>6)</td>
<td>Access</td>
</tr>
<tr>
<td>7)</td>
<td>Disclosure to third parties</td>
</tr>
<tr>
<td>8)</td>
<td>Security for privacy</td>
</tr>
<tr>
<td>9)</td>
<td>Quality</td>
</tr>
<tr>
<td>10)</td>
<td>Monitoring and enforcement</td>
</tr>
</tbody>
</table>

http://www.aicpa.org/privacy
Generally accepted privacy principles (cont.)

Management

> The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

Notice

> The entity provides notice about its privacy policies & procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

Choice and consent

> The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
Collection

> The entity collects personal info only for the purposes identified in the notice.

Use and retention

> The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.

Access

> The entity provides individuals with access to their personal information for review and update.
Disclosure to third parties

> The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

Security for privacy

> The entity protects personal info against unauthorized access (both physical and logical).
Quality

> The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

Monitoring and enforcement

> The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.
Impacts to service organizations

> Similar structure and requirements to a SOC 1

> Trust services principles instead of control objectives

> Description is broader in a SOC 2 than you typically see in a SOC 1
  - Defined by service provided
  - Broader than SSAE 16 (e.g., privacy—includes information life cycle; processing integrity—includes the purpose of the service other than financial transaction processing)
  - May include operations

> SOC 2 report can cover additional compliance requirements outside of the trust services criteria – HIPAA, PCI, specific service level agreement requirements
  - Separate assertion, description, testing, and opinion paragraph
What’s in the report?

1. Service auditor’s report (the opinion)
2. Management’s assertion
3. System description
4. Tests of controls and results
5. Additional information provided by the service organization
Management’s assertion

> Management’s system description fairly presents the service organization’s system that was designed and implemented as of the specified date (type 1) or throughout the specified period (type 2)

> The controls stated in the description were suitably designed to meet the applicable trust services criteria as of the specified date (type 1) or throughout the specified period (type 2)

System description

> Services provided, components, system boundaries, error handling, subservice organizations, user controls and other topics
System description

> Services being provided
> Components of the system
  - Infrastructure, software, people, procedures, and data
> System boundaries
> Error handling
> Report preparation and delivery
> Subservice organizations
> Criteria and related controls including user controls
> Other aspects of the control environment
> Changes to controls during period for a type 2
> Additional details for privacy
Test of controls and results

> Do the controls identified in the description provide reasonable assurance that the trust services criteria would be met?

> Did the controls operate as designed throughout the specified period?

> If privacy is included, did the organization comply with its privacy statement commitments?

Additional information provided by service organization

> Description of the subject matter

> Criteria used to measure the subject matter

> Description of controls intended to meet the control criteria if applicable

> Assertion by management in regards to the additional information
What does it mean?

> It’s an opinion on controls, not a security audit.

> No direct security testing completed in a SOC 2 / SOC 3.

> Verifies that the company has procedures in place “to protect against”, not prevent completely.

> Requires further judgment by the auditor... and the reader.
Section 3

IMPORTANT LESSONS FROM SERVICE ORGANIZATION CONTROLS REPORTING
Important lessons learned

1. Scoping
2. The newness factor
3. Descriptions of controls
4. Testing
5. Other considerations
6. Questions to ask when looking for a SOC report service provider
Scoping

Which principles to test?

> Not all need to be tested

> If a principle is not covered in report, doesn’t mean it “failed”

Not all may be relevant to the service organization
Who’s responsibility to determine principles covered?

Appropriately performing a Type 1 vs Type 2?

> Review customer contracts
The newness factor

Minimal examples available for service organizations to use

User organizations and those in charge of governance don’t fully understand yet

> Read through the trust principles

Key resources available

> AT 101
> AICPA Technical Practice Aids: TSP 100
> Generally Accepted Privacy Principles
> AICPA Guide – Reporting on SOC 2
The newness factor (cont.)

Unfamiliarity with trust criteria

SOC 2 is not the same as a SAS 70 or SOC 1

> Companies may have both a SOC 1 and a SOC 2
It is management’s responsibility to prepare its description of its system

> Currently no examples available, AICPA looking to provide within next couple weeks

Must fairly present the system that was designed and implemented during the period

> Cannot omit or distort relevant information
Must be fact based / data driven

> Relevant to the principles identified

Must be validated

> Example - balance score card metrics don’t belong
> No marketing matters
> No subjective commentary
Testing

Communicate trust principles in advance and identify criteria being tested

> Audit team and service organization must work together to ensure engagement runs smoothly

Timing of testing

> Interim testing may be beneficial - depends on length of period

Have all applicable information and control owners available
Service organization’s controls must meet all of the criteria applicable to the principle(s)

Failed criteria

> Effect on assertions and audit report
> Has it been remediated?
> Response by management
> How significant is deviation?
  May result in qualified or adverse opinion
Other considerations

This is not just an “IT report”
> Many components relate to operations, HR, upper management

Requires appropriate entity level controls
> Risk assessment
> Control environment
> Monitoring
> Communication
Overlap

> Between security, confidentiality, availability, and processing integrity
> Privacy - GAPP

Confidentiality vs. Privacy

> Privacy is personal information
  - Information that is about, or can be related to, an identifiable person
> Confidentiality is determined by the company
Other considerations (cont.)

Changes to system during the testing period

> Requires testing of control both before and after change
> Applicable to changes material to user only
> Is description still fairly stated?

Subsequent events

> Any event after period covered, up to date of report
> If have a significant effect on management’s assertion
> Disclose in auditor’s report
Questions to ask when looking for a SOC report service provider

> How do I know if my organization is ready for a SOC report?
> Which report do you recommend for my situation and why?
> If looking at a SOC 1 or SOC 2 report, which type (1 or 2) of the SOC report do you recommend?
> What staff involvement will you need from my organization?
> What access will you need to my systems?
> What timeframe do you recommend for the SOC report?
> What deliverables will result from the engagement?
> Describe the communication process before, during, and after the engagement between you and my organization.
QUESTIONS?

Contact us: bakertilly.com
Christine Anderson, CPA, CISA
chris.anderson@bakertilly.com
608 240 2668
Pursuant to the rules of professional conduct set forth in Circular 230, as promulgated by the United States Department of the Treasury, nothing contained in this communication was intended or written to be used by any taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer by the Internal Revenue Service, and it cannot be used by any taxpayer for such purpose. No one, without our express prior written permission, may use or refer to any tax advice in this communication in promoting, marketing, or recommending a partnership or other entity, investment plan, or arrangement to any other party.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. The information provided here is of a general nature and is not intended to address specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. © 2012 Baker Tilly Virchow Krause, LLP