

# Say Goodbye to SAS 70:

What the Transition to the new SOC Reporting and SSAE16 Standards Means to my Organization

The  
Cadence  
Group





# Administration

- CPE
- Breakfast
- Bathrooms
- Cell Phones



## Upcoming Cadence Events

- **2011 Cadence Golf Tournament**
  - Tuesday, September 20<sup>th</sup> 8am at South Mountain Golf Course.
- **Cadence Training Series - GRC**
  - Thursday, October 27<sup>th</sup> at Corporate Alliance



# Introduction

## Kevin Abbott

- [kevin@thecadencegroup.com](mailto:kevin@thecadencegroup.com)
- 801-358-5748
- CISA, CISSP, PCI QSA

## The Cadence Group

- Salt Lake City based Compliance and Advisory firm, specializing in SOC Reporting, PCI, SOX, Internal Audit Services, Financial Reporting, Technical Accounting, and Enterprise Risk Management.



## Why the Change?

- SAS 70 was issued in 1992 as an AICPA standard for reporting on internal controls over financial reporting at service companies (purpose was to facilitate auditor-to-auditor communication).
- The Factors for Change to SAS No. 70
  - Need for Greater International Consistency
  - Mis-understandings, Mis-applications, and Mis-uses of SAS70
  - SAAS, Cloud Computing, Growth in Outsourcing
  - Sarbanes- Oxley Section 404
  - Service Organizations claiming “SAS Certification”



# What Happened?

**SAS 70**

**ICFR**

**SOX**

**Privacy**

**Security**

**Cloud**

**Check-box Audit  
Mentality**



# New Reporting Standards

**AICPA**

**SOC 1** - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SSAE16)

**SOC 2** - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy (AT101)

**SOC 3** - Trust Services Report (AT101)



**IAASB**

**ISAE3402** – Assurance Reports on Controls at a Service Organization (International Standard)



# Notable Changes

- Attestation standard vs. Auditing standard
- New Requirement for **Management Assertions**
- Opinion/Report Format
  - Signed Assertion page in the report
- Use of Internal Audit (disclosure)
- Use of Sub-Service Organizations (disclosure)

Effective for organizations with reporting periods ending on or after **June 15, 2011**



# SOC1 / SSAE16

## **SOC 1 Report: What is it?**

These reports, prepared in accordance with *Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization*, are specifically intended to meet the needs of the of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user' auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements. User auditors use these reports to plan and perform audits of the user entities' financial statements. There are two types of reports for these engagements (Type 1, or Type 2)

Use of these reports is restricted to the management of the service organization, user entities, and user auditors.



# SOC2

## **SOC 2 Report: What is it?**

We needed something like a SAS 70 report, but for all the other stuff. These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the **security**, **availability**, and **processing integrity** of the systems the service organization uses to process users' data and the **confidentiality** and **privacy** of the information processed by these systems . Examples of stakeholders who may need these reports are, management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

Use of these reports generally is restricted to parties that have an understanding of the criteria.



# SOC3

## **SOC 3 Report: What is it?**

*Trust Services Report for Service Organization:* SOC 3 engagements use the predefined criteria in *Trust Services Principles, Criteria and Illustrations* that also are used in SOC 2 engagements. The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor's tests of controls and results of those tests as well as the service auditor's opinion on the description of the service organization's system.

A SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system). It also permits the service organization to use the SOC 3 seal on its website. SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality and privacy).



# SOC Report Content

## SOC 1

1. Auditors report
2. Detail system description
3. Management assertion
4. Management controls
5. Auditor tests of controls and results of those tests  
– control objectives

## SOC 2

1. Auditors report
2. Detail system description
3. Management assertion
4. Management controls
5. Auditor tests of controls and results of those tests  
– criteria

## SOC 3

1. Auditors report
- ~~2. Detail system description~~
3. Management assertion
- ~~4. Management controls~~
- ~~5. Auditor tests of controls and results of those tests~~

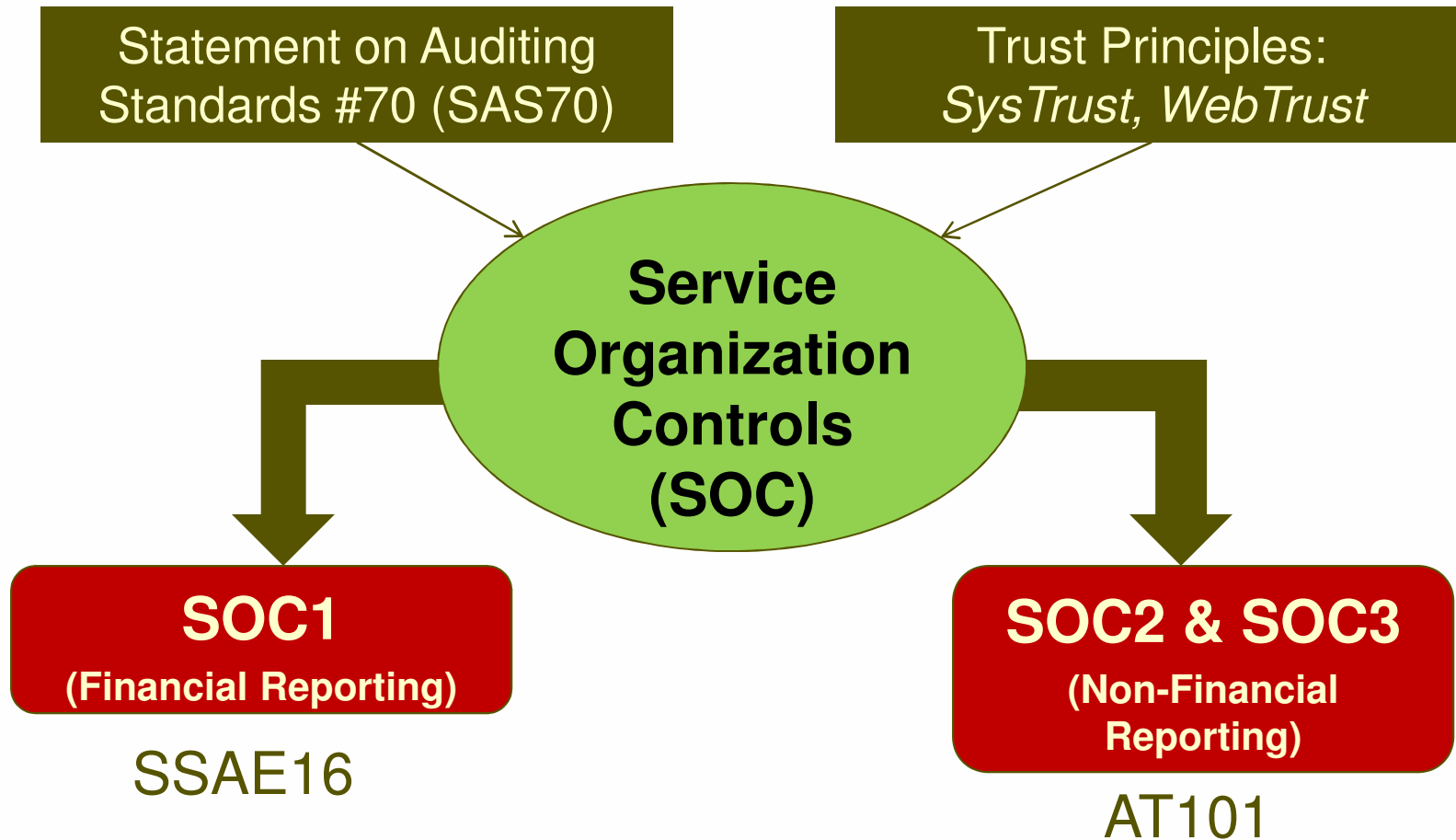


# Decisions and Next Steps

**Determine which  
SOC report is  
appropriate for  
your organization**



# Which SOC Report is Appropriate for my Service Organization?





# Which SOC Report is Appropriate for my Service Organization?

That depends on what services you perform, and who the audience is. This table summarizes the three new SOC report types.

New Standards & Options		
SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE16 – Service Auditor Guidance	AT 101	AT 101
Restricted Use Report (Type I or II report)	Generally a Restricted Use Report (Type I or II report)	General Use Report (with a public seal)
Purpose: Reports on Controls for F/S Audits	Purpose: Reports on controls related to compliance or operations	Purpose: Reports on controls related to compliance or operations
	<b>Trust Services Principles &amp; Criteria</b>	



# Which SOC Report is Appropriate for my Service Organization?

## SOC DECISION TREE

Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1 Report
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC 1 Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2 or 3 Report
Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC 2 Report
	No	SOC 3 Report
Do you need to make the report generally available or use a seal?	Yes	SOC 3 Report



# Decisions and Next Steps

Determine Which  
SOC report is  
appropriate for  
your organization

**SOC2/SOC3 Only -  
Map Controls to  
the *Trust Services  
Principles &  
Criteria***



# Trust Services Principles & Criteria

A SOC2 or SOC3 Report specifically address one or more of the following five key system attributes:

- **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 in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

SOC2 Reports may be expanded to also include PCI, HIPPA, GLBA, etc. controls.



# Decisions and Next Steps

Which SOC report  
is appropriate for  
my organization

SOC2/SOC3 Only -  
Map Controls to the  
Trust Services  
Principles & Criter

**Establish and  
document  
Management's  
Assertions**



# Management's Assertion

A written assertion about whether in all material respects, and based on suitable criteria that:

- The description fairly presents the system that was designed and implemented throughout the period
  - Controls were suitably designed throughout the period to achieve the control objectives
  - Those controls operated effectively throughout the period to achieve the control objectives
- Suitability of Criteria

**Management must have a reasonable basis for its assertion**



# Decisions and Next Steps

Which SOC report is appropriate for my organization

SOC2/SOC3 Only -  
Map Controls to the  
Trust Services  
Principles & Criteria

Establish and  
document  
Management's  
Assertions

**Establish a  
Reasonable  
Basis for the  
Assertions**



## What is Considered to be a “Reasonable Basis”

In order to have a reasonable basis for its assertion, management should understand the criteria that should be used to make the assertion:

- **Fairness** – Does the description address all of the required elements?
- **Design** – Do we understand the risks and have we identified the key controls that mitigate those risks?
- **Operating effectiveness** – Do we know that those key controls were operating with sufficient effectiveness to achieve the control objectives or Trust Principles and Criteria?
  - There is no need to assert on the design and effectiveness of individual controls, and no requirement to test every control.
  - Common approach will be to rely on monitoring controls to identify when controls are NOT working.



# What is Considered to be a “Reasonable Basis”





# What is Considered to be a “Reasonable Basis”

Sounds like SOX, right?

- Sort of. In a SOX world, there may need to be a lot of testing to gain comfort that internal controls over financial reporting are working.
- With SOC reports, the main question is: “How do we know that things are working the way they are supposed to? And that our customers are being served the way they are supposed to? This is the main part of a service organization’s business, so a lot of this is implicitly done, it may just need to be more formally documented.



# Decisions and Next Steps

Which SOC report is appropriate for my organization

SOC2/SOC3 Only -  
Map Controls to the  
Trust Services  
Principles & Criteria

Establish and  
document  
Management's  
Assertions

Establish a  
Reasonable Basis  
for the Assertions

**What can we do  
to prepare now  
for these  
changes?**



# How Service Organizations are Preparing

## 1. Establish Clear Roles & Responsibilities for Individuals Involved

- Report Owner – Responsible for overall assertion
- Risk Owner – Responsible for specific risks that threaten the achievement of control objectives (one risk owner may be responsible for multiple risks, and those risks may cross multiple objectives)
- Coordinator – Responsible for organizing risk sub-assertions, the report assertion, and maintaining supporting evidence.

## 2. Re-evaluate Scope of Report

- Overall Report Scope – Confirm the scope of the report is still appropriate and relevant in light of the services provided to user organizations
- Control Objectives – Evaluate control objectives to confirm they align with the scope of the report, keeping in mind that control objectives should correlate to processes that are likely to be relevant to a user entity's internal control over financial reporting
- Sub-service organizations – Confirm that sub-service organizations are properly reflected in the report, and that inclusive sub-service organizations understand their responsibilities for providing a management assertion.



# How Service Organizations are Preparing

## **3. Perform a Risk Assessment**

- Identify Risks that Threaten the Achievement of the Assertions
- Focus on the risks that threaten the achievement of the Assertion (and Trust Principle for SOC2 reports) rather than risks that threaten the achievement of individual controls.
- Document risks at a sufficient level of detail without getting too granular.

## **4. Identify Key Controls / Rationalize Existing Controls**

- Inquire of Risk Owners to understand what controls they utilize to inform them when the respective risks are not being mitigated
- Sub-service organizations – Confirm that sub-service organizations are properly reflected in the report, and that inclusive sub-service organizations understand their responsibilities for providing a management assertion.

## **5. Establish a Monitoring Process to Evaluate Design/Effectiveness of Key Controls**

- Leverage existing monitoring controls and control evaluations where possible
- Determine what information will be provided to Coordinator, Risk Owner, Report Owner as evidence of control operation



# How Service Organizations are Preparing



	A	B	C	D	E	F
	Control Objective Owner	Control Area	Control Objective	Risk	Key Control	Monitoring Activity
1	John Smith	Logical Access	Controls provide reasonable assurance that access to customer data and applications is restricted to appropriate personnel.	Access by unauthorized users or terminated employees due to easily guessable passwords could result in customer data theft, identity theft, and credit card data breach.	Strong password parameters must be used, including: - PW Minimum Length: 8 Chars - PW Expiration: 90 days - PW History: 10 passwords - PW Complexity: Yes	Password Parameters are validated quarterly for the KC Application, the network level, the supporting Linux OS, and the Oracle DB
2	Bill Davis	Logical Access	Controls provide reasonable assurance that access to customer data and applications is restricted to appropriate personnel.	Terminations or employee job changes result in stale accounts remaining active.	Quarterly reviews of active user listings take place for the KC Application, the network level, the supporting Linux OS, and the Oracle DB	N/A
3						
4						



## ISAE 3402

- International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization (essentially the SOC1/SSAE 16 equivalent for international entities).
- Issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), which is part of the International Federation of Accountants (IFAC).



## Appendix A – Differences between SOC1/SSAE 16 and ISAE 3402

	SOC1/SSAE 16 Requirement	ISAE 3402 Requirement
Intentional acts	If deviations result from intentional acts by service organization personnel, service auditor assess the risk that the description is not fairly presented and controls are not suitably designed.	No specific requirement
Anomalies	No such requirement.	Service auditor may conclude that a deviation is not representative of the population from which it was drawn.
Direct assistance	Permits the service auditor to use members of the work of internal audit to provide direct assistance under AU Section 322	Not addressed



## Appendix A – Differences between SOC1/SSAE 16 and ISAE 3402

	SOC1/SSAE 16 Requirement	ISAE 3402 Requirement
Subsequent events	Requires disclosure of events occurring subsequent to the period covered by the if the nature and significance of the event would prevent users from being misled.	No such requirement.
Use restriction	Statement restricting use of the service auditor's report is a prescribed format	Statement describing the intended use of the service auditor's report with more restrictive language permitted.
Documentation completion	Requires engagement documentation to be completed on a timely basis after the date of the report and no later than 60 days following the report release date.	Requires engagement documentation to be completed on a timely basis after the date of the report.



## Appendix A – Differences between SOC1/SSAE 16 and ISAE 3402

	SOC1/SSAE 16 Requirement	ISAE 3402 Requirement
Engagement acceptance and continuance	Service organization management acknowledges and accepts responsibility for providing written representations to the service auditor.	Acknowledgements is not required but written representation is required.
Disclaimer of opinion	If written representations are not provided by service organization management, the service auditor required to take appropriate action which may include disclaiming an opinion or withdrawing from the engagement.	If written representations are not provided by service organization management, the service auditor required disclaim an opinion.
Other	SSAE 16 contains certain incremental service auditors report requirements over and above the requirements of ISAE 3402.	



# Introduction

## Kevin Abbott

- [kevin@thecadencegroup.com](mailto:kevin@thecadencegroup.com)
- 801-358-5748
- CISA, CISSP, PCI QSA

## The Cadence Group

- Salt Lake City based Compliance and Advisory firm, specializing in SOC Reporting, PCI, SOX, Internal Audit Services, Financial Reporting, Technical Accounting, and Enterprise Risk Management.

# The Cadence Group



[www.thecadencegroup.com](http://www.thecadencegroup.com)