SaaS / Cloud Computing Risk Management

AICPA Attest Alternatives

Presenter: Dan Schroeder, CPA/CITP
Habif, Arogeti, & Wynne, LLP

Georgia Society of CPAs Annual Convention
June 16, 2010

About the Presenter

Dan Schroeder,
CPA/ CITP, CISA, CISM, CIA

- Partner-in-Charge, Habif, Arogeti,& Wynne LLP ("HA&W") IT Audit & Assurance Services
- SAS 70,SSAE 16, Security and Privacy Trust Services, IT Governance, and other compliance services.
- 20 years of IT advisory and audit experience - focused mainly on financial services, mfg/distribution, and technology service providers.
- Chair of AICPA's Information Technology Executive Committee ("ITEC")
- Leading author of "IT Considerations for Risk Based Auditing" whitepaper
- Lead development of AICPA IT Audit School.

Presentation Objectives

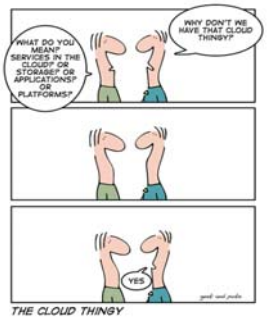
- What is SaaS and Cloud Computing?
- Implications to CPAs as service auditors/practitioners, user auditors, trusted business advisors
- Review of what SAS 70 is -- and is not
- Overview of SSAE16 and changes from SAS 70
- Overview of AICPA Trust Services Principles & Criteria as alternative approach to risk mitigation and reporting when SSAE 16 is not appropriate

WHAT IS SAAS AND CLOUD COMPUTING AND WHY DOES IT MATTER?

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

What is Cloud Computing / SaaS?

- ✓SaaS: Software as a Service
- ✓PaaS: Platform as a Service
- ✓IaaS: Infrastructure as a Service
- ✓Colocation: Private Cloud
- ✓Hosted Applications: Outsourced Cloud



Cloud Computing Trends

- 45-60% of companies using some form of cloud
- Growth rate of …….

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Implications for CPAs

- **Service Auditors / Practitioners:** many more companies providing Cloud services
- **Advisors:** more opportunities for our clients, more risks to be considered
- **User Auditors:** our clients will be more dependant on cloud providers
- No one-sized-fits-all approach to risk management

SAS 70 REVIEW: A GREAT BRAND, BUT TERRIBLY MISUNDERSTOOD

Common SAS No. 70 Myths / Misunderstandings

- The SAS 70 report from a hosting facility (co-lo, managed services) adequately addresses risks and reporting needs of customers of the solution provider (SaaS / Cloud).
- SAS 70 report can be used to report on controls related to compliance and operational matters, such as confidentiality, privacy, processing integrity, etc.
- SAS 70 report demonstrates best practices or world-class……
- A “certification”.
- SAS 70 is designed to help with sales.

SAS 70 Applicability Criteria – it was always supposed to be about ICFR

- SAS 70 is applicable to the audit of the financial statements of an entity that obtains services from another organization that are part of a user organization's information system.
- A service organization's services are part of an entity's information system if they affect any of the following:
  - The classes of transactions…..are **significant to the financial statements**.
  - The procedures, both automated and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their **inclusion in the financial statements.**
  - **The related accounting records** ……whether electronic or manual…and specific accounts in the financial statements involved in initiating, recording, processing….
  - …..information system……captures events and conditions that are **significant to the financial statements.**
  - The **financial reporting process**…….

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

SSAE 16 is replacing SAS 70

released April 2010
effective June 15, 2011
early adoption permitted.

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

SSAE 16 Reporting

Scope of Report / Opinion	Type 1	Type 2
Fairness of the presentation of management's description of the service organization's system	As of a specified date.	Through-out a specified period.
Suitability of the design of the controls to achieve the related control objectives included in the description		
Operating effectiveness of the controls to achieve the related control objectives included in the description	n/a	

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

SSAE 16 changes from SAS 70

- ICFR Relevancy
- Attest, no longer Audit
- Auditor evaluation based on suitable criteria relative to written management assertions – that are included in the report:
  - Description of the system for the entire period,
  - Suitable controls for the system, risk basis for achievement of control objectives and determining if controls suitably designed to achieve control objectives. Description of sub-service organization controls.
  - Consistent and competent application of controls.

Suitability of Criteria SSAE No. 16

System Fairly Presented

A. Description includes how the system was designed and implemented including the following:
   - Class of Transactions are significant to the financial statements.
   - Procedures by which transactions are initiated, recorded, processed, and reported from inception to inclusion in the financial statements.
   - Relevant accounting records supporting information and accounts involved in the initiation, recording, processing and reporting of transactions.
   - The capturing of other relevant events and conditions significant to the financial statements by information systems.
   - The financial reporting process used to prepare the financial statements including estimates and disclosures.

Suitability of Criteria SSAE No. 16 (Continued)

System Fairly Presented

   - The control objectives and controls designed to achieve those control objectives, if applicable, include complementary user entity controls.
   - Other aspects of the service organizations control environment, risk assessment process, information and communication systems, control activities, and monitoring controls relevant.

B. Management's description of the system includes relevant details of changes to the system during the period covered.

C. Management's description does not omit or distort information while meeting the common needs of a broad range of user entities and their user auditors.

Suitability of Criteria SSAE No. 16 (Continued)

System Fairly Presented

E. The risks that threaten the achievement of the control objectives stated in the description have been identified by management.

F. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives from being achieved.

G. Controls were consistently applied as designed throughout the specified period, including whether manual controls were applied by individuals who have the appropriate competency and authority.

SAS70 / SSAE16 Reporting

I. Service Auditor's Report

II. Description of Controls
- (Management Assertion SSAE16)

III. Control Activities and Tests of Controls

IV. Section IV (Optional)– Other Information provided by Service Organization

Reports are restricted-use reports intended for the service organization, customers of the user entity, and auditors of the user.

Role in Reducing Audit Risk

Service Auditor's Opinion:

Type I Report:
- Whether the description of the service organizations system fairly presents the system that was designed and implemented as of a specified date.
- Whether the controls were suitably designed to achieve specified control objectives as of a specified date.

Basis for Assessing Risk
- **Does not provide the user auditor with a basis for reducing the assessed level of control risk and thereby reducing substantive procedures.**
- Type I report is intended to assist user auditors in obtaining a sufficient understanding of the user organizations internal control in order to plan the financial statement audit.

Role in Reducing Audit Risk

Service Auditor's Opinion:

Type II Report:

- Type I conclusions covering the entire period (SSAE 16), and
- Whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the specified period.

Basis for Assessing Risk

- **A user auditor may be able to reduce risk below max for certain financial statement assertions**……and may therefore be able to reduce the extent of substantive testing performed for those assertions.
- A user auditor should not use only the service auditors report as a basis for assessing the control risk below max. The user auditor should read the service organization's description of controls as well as the service auditor's tests of operating and effectiveness the results of those tests, and relate this information to assertions in the user organizations' financial statements.

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Description of Controls

- Relevant aspects of the Service Organization's Internal Control Environment
  - Control Environment
  - Risk Assessment
  - Monitoring
  - Information and Communication

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Description of Controls

- Information about service organization system and controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements. The description should contain:
  - Management Assertions (and Subservice Organizations Assertions if applicable) (SSAE16).
  - Control objectives and related controls (control activities) designed to achieve them.
  - Changes to control since the later of the date of the last report or within the last twelve months.

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Control Activities and Test of Controls

- Section provided by the Service Auditor.
- Includes the control objective(s)and relevant controls identified to accomplish the objective(s).
- Includes the nature, timing and extent of control testing.
- Included the results and conclusions of the tests performed.

Section IV (Optional) Other Information Provided by the Service Organization

- Section provided by the Service Organization.
- Includes supplemental information not included in the scope of the Report. For example:
  - BCP/DRP overview
  - Planned system / control changes
- Service auditor should verify that this information does not contain any material inconsistencies with that of the description.

Service Auditor Considerations

- User Organization Needs
- Assessing the Suitability of Criteria
- Risk Based Approach
- Applicability of SSAE vs. Alternatives
- Identify Scope
- Subservice Organizations
- Timing
- Work of Internal Audit
- Peer Review

Service Organization Considerations

- Define Scope and Criteria
- Define a comprehensive Internal Control Environment
- Risk Based Design of Controls and Objectives
- Confirm the Needs of the User Organizations
- Management Assertions (SSAE 16)
- Use Section IV (Other Information) to Leverage Additional Information

User Auditor Considerations

- Report usage
- Report timing and scope
- Relevant standards
  - Audit planning (SAS No. 55)
  - Audit Considerations Relating to an Entity Using a Service Organization (Exposure Draft)

User Entity Considerations

- Scope of Service Covered
- Appropriate and Relevant Controls at the Service Organization
- Apply “User Controls”
- Identify Service Organization Control Overlap and Relevant User Controls

TRUST SERVICES PRINCIPLES & CRITERIA ("TS P&C")

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.

TS Principles

1. **Security**. The system is protected against unauthorized access (both physical and logical).
2. **Availability**. The system is available for operation and use as committed or agreed.
3. **Processing integrity**. System processing is complete, accurate, timely, and authorized.
4. **Confidentiality**. Information designated as confidential is protected as committed or agreed.
5. **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 (GAPP).

TS P&C Engagements

- Reporting on the operating effectiveness of an entity's controls over the system.
- Reporting on the operating effectiveness of an entity's controls and the entity's compliance with its commitments related to the trust services principle(s) and criteria.
- Reporting on the suitability of the design of the entity's controls over the system to achieve the trust services principle(s) and criteria, if the controls were operating effectively.

TS Criteria – four domains

1. **Policies.** The entity has defined and documented its policies relevant to the particular principle. (The term policies as used here refer to written statements that communicate management's intent, objectives, requirements, responsibilities, and standards for a particular subject.)
2. **Communications.** The entity has communicated its defined policies to responsible parties and authorized users of the system.
3. **Procedures.** The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.
4. **Monitoring**. The entity monitors the system and takes action to maintain compliance with its defined policies.

Comparison SAS 70 and Trust Services Reports

	SAS No. 70	*Trust Services*
Intended Audience for the report	SAS No. 70 reports are restricted-use reports intended for the service organization, customers of the service organization, and auditors of the user organizations (not for prospective customers).	Trust Services reports are intended to be general use reports.
Objectives of the engagement	Provide user auditor with information about controls at the service organization that may affect assertions in the user organizations' financial statements.	Provide third-party assurance as to the adherence and effectiveness of a defined system's controls against established criteria in one or more of the principles outlined above.
Types of systems and controls addressed by the engagement	For SAS No. 70, the system that produces the information included in the entity's financial statements. Coverage is for controls at the service organization that affect user organizations.	The system may be any defined financial or nonfinancial system. Coverage is for controls related to any financial or nonfinancial system by specific subject matter, namely, security, availability, confidentiality, privacy and processing integrity.
Business continuity and contingency planning reporting activities	Control objectives relating to business continuity and contingency planning are not allowable in the description of controls in the auditor's report under SAS No. 70.	Criteria relating to business continuity and contingency planning are specifically addressed by the Availability principle.

TRUST SERVICES PRINCIPLES & CRITERIA REPORTING OPTIONS

Reporting Options

- AT Section 101, *Attest Engagements* (AICPA, *Professional Standards*, vol. 1)
  - Short form – opinion letter without fuller description of controls and tests of controls.
  - Under SSAE 16 reporting framework (draft – Audit / Attest Guide in development, for release later in 2010.)

Applying TS P&C in a SSAE 16 Framework

- Management's Assertion (similar to SSAE 16 report)
- System description
- One or more Trust Services Principles
- No co-mingling / bundled reports for both ICFR and non-ICFR scenarios (ICFR is exclusive to SSAE 16)
- Control Objectives prescribed – based on Trust Services criteria:
  - Control criteria can be expanded to include guidance from other leading control references; e.g., ISO 27001, ITIL, CoBit, etc.

GENERALLY ACCEPTED PRIVACY PRINCIPLES ("GAPP")

Overview of GAPP

- Generally Accepted Privacy Principles contain **ten privacy principles and related criteria** that are essential for the proper protection and management of personal information.
- These privacy principles and criteria are **based on internationally known fair information practices** included in many privacy laws and regulations of various jurisdictions around the world and in common and leading practices.

1. Management
2. Notice
3. Choice and consent
4. Collection
5. Use, retention, and disposal
6. Access
7. Disclosure to third parties
8. Security for privacy
9. Quality
10. Monitoring and enforcement

GAPP Principles

1. **Management.** The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **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.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.

GAPP Principles

5. **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.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **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.

GAPP Principles

8. **Security for Privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and Enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Service Organizations Reporting Alternatives

- AT 101 (Attestation Report)
- Agreed Upon Procedures (AUP Report)
- AICPA/CICA Trust Service Principles and Criteria
- Trust Service in a SSAE 16 Framework (Draft Guidance)

Thank you!

Questions?

Dan Schroeder
dan.schroeder@hawcpa.com
770-353-8379

AICPA's IT Section Resources

Focus of Benefits	Examples of Current & Future Benefits
Technical content/ resources	Webcasts, podcasts, articles (ex. RBA, CAATTs, ITGCs)
Educational programs	TECH+, NAAATS Conferences
Educational Pathway	IT Audit School
Networking Opportunities	LinkedIn, CITP Champions
Communications & Updates	InfoTech Update, and more…
Other benefits	Discounts on IDEA and Active Data products

AICPA Resources

- AICPA's IT Interest Area website:
  http://www.aicpa.org/InterestAreas/InformationTechnology/Pages/InfoTech.aspx or www.aicpa.org/infotech
- June 28, 10 Webcast
  http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/Accounting/Standards/StandardsImplementationGuidance/PRDOVR~PC-WBC10065/PC-WBC10065.jsp
- AICPA's Frequently Asked Questions (FAQ)
  http://www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/AudAttest/AudAttestGuidance/DownloadableDocuments/Final%20Service%20Orgs%20FAQ.pdf
- AICPA's Statement on Standards for Attestation Engagements (SSAE) No. 16:
  http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/Standards/SSAEs/PRDOVR~PC-023035/PC-023035.jsp