

SSAE 16

Preparing for the Transition from SAS 70



The new tool for vendor management.....

Session Overview

- SAS 70 – a look back for context
- SSAE 16 – the next evolution in control reporting
 - Why change?
 - What changes
 - What does not change
- Project management considerations
- Alternatives to SSAE 16 – SOC reports



SAS 70 – the origins of service organization control reporting

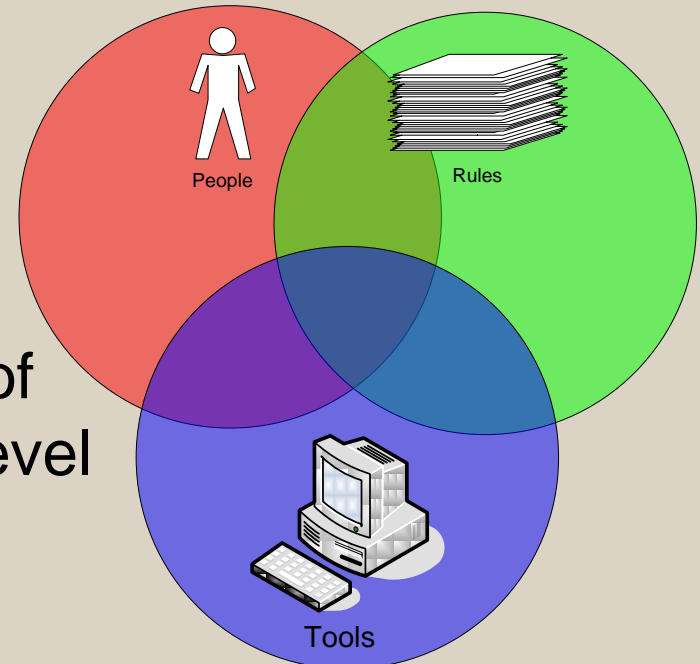


Security = Culture!!

Security is a **BUSINESS** issue, NOT a technical issue!!

- *Administrative Policies / Procedures*
- *Physical Access Controls*
- *Technical Security Controls*

Objective is to have a reasonable level of controls, while ensuring the desired level of performance.



Trust is Key

- Organizations want to have trust and confidence in third party relationships
- Statement of Auditing Standards (SAS) No. 70
- SAS70 is an Assurance AUDIT.....NOT a framework
 - The AUDIT establishes the trust via assurance



Framework vs Audit

- Other Common Frameworks include:
 - COBIT
 - ISO 17799-27001
 - ITIL



Report Drivers

- SOX?
- Regulators?
- HIPAA?
- Marketing credentials?



SAS 55 – Focus on Internal Control

- Created as an auditor to auditor communication
- Internal controls relevant to financial reporting
 - Type I
 - ◇ Point in time assurance
 - ◇ *New terminology: Suitable design*
 - Type II
 - ◇ Operating effectiveness over a time period
 - ◇ *New terminology: Compliance with control design*



SAS 70 Report Components

- Service auditor's opinion
- Description of controls
 - Control objectives
 - Control activities
- Service auditor's tests of controls
 - Support the opinion on operating effectiveness
- User organization control considerations
- Other info provided by service org management
 - Disaster recovery plan



Traditional Project Plan

- Readiness assessment
- Remediation of control gaps (if any)
- Walkthrough
- Type I Audit (optional)
- Type II Audit reporting period begins
- Test plan execution
- Type II Audit report issued



SAS 70 Benefits

- Open Ended
 - No framework is mandated
 - SOC report alternatives connect with a framework
- Widely Accepted
 - “defacto brand”
- Third Party Assurance - Rigorous *AUDIT*
 - CPA assurance means rigorous testing
 - Only a CPA firm can “legally” issue report



SSAE 16



The next evolution in controls reporting for service organizations

A global economy.....

- SSAE 16 is designed to merge US standards for service organization audits with international standards
- AICPA – the governing body for US CPA's
 - SSAE – Statements of Standards for Attestation Engagements
- International Federation of Accountants (IFAC) – global governing body
 - ISAE – International Standard on Attestation Engagement
 - ISAE 3402 – sister standard to SSAE 16



Focus on Financial Reporting

- Common complaint in the marketplace is the focus on financial reporting
- Enter new terminology: SOC Report
 - Service Organization Controls
 - SSAE 16 report is a SOC 1 report
 - More on this later.....



When is it coming?

- Required for all service organization control reports with periods ending June 15, 2011 or later
- Early adoption is permitted
- Guide for service auditors is expected some time Q1 2011



Key Changes in SSAFE 16



Proper Planning is the Key!

Management Assertion

- Service organization management will provide a written assertion about the design of controls
- Included in the body of the report
- Must be provided at the *beginning* of the reporting period



Basis for the Management Assertion

- Service organization management must have a basis for making the assertion about the design of controls
 - Suitable criteria for the assertion
 - Control monitoring activities
 - Work of internal audit function
 - Other testing activities
- This must be in place at the beginning of the reporting period



What is “suitable criteria”?

- SSAE 16 points to AT 101
 - Objective / measurable
 - Available publicly
 - Available to users in the report
 - Generally well understood
 - ◇ i.e. Indicating something weighs 20 lbs is well understood through the use of the criteria “lbs”



Service Auditor's Opinion

- Points the management assertion
- Extends to the entire reporting period

- Key Point – controls must be suitably designed at the beginning of the reporting period

- New engagements?
- Change in auditors?
- Change in scope?
 - Must have a “reasonable basis”



Expansion of the Controls Description

- SSAE 16 report will describe the entire system
 - Initiation
 - Approval
 - Recording
 - Reconciliation
 - Error resolution
 - Etc.
- Control objectives and activities “embedded” in the system
- Must describe significant changes during the reporting period



Risk Assessment

- Service organization management must identify key risks that threaten control objectives
- Must be documented



Documentation

- Key systems and processes must be documented
- Past – observable and testable
- PPMS a big help in this requirement



Use of Internal Auditor

- If the service auditor relies on the work of internal audit, the extent of that reliance needs to be included in the report



What remains the same with SSAE 16?



Third Party Assurance

- Although moving from auditing standards to the attestation standards, the engagement still carries a service auditor's opinion
- Only a CPA can sign such an opinion



Focus on Financial Reporting

- SSAE 16 reports are still meant to be an auditor to auditor communication
- Controls reported on relate to financial reporting
- Restricted use report

- More on SOC report alternatives a bit later



Type I vs Type II

- This concept remains essentially identical
- Type I
 - Point in time assurance
 - Focus on suitability of design
- Type II
 - Assurance over a time period (6-12 months typically)
 - Focus on control compliance (operating effectiveness)



Control Objectives / Activities

- Service organization management must still report on control objectives and activities
- This requirement is simply expanded to include a more holistic description of the “system”



Other Info Provided by Management

- Service organization management is still allowed to present unaudited information in the body of the report
- Disaster recover plan



Subservice Organizations

- Guidance for treatment of subservice organizations essentially unchanged
 - Letter printers
 - Co-location facility
 - Web site host
 - Etc.
- Inclusive method
- Carve out method



SSAE 16 Report Structure

- Service auditor's opinion
- Management assertion
- Description of system
- Description of control objectives and activities
- Description of control testing and results
 - Type II only
- User controls considerations
- Other information provide by SO management



Bottom Line for Service Organizations

- Service Organization Responsibilities:
 - Provide a written description of the “system”
 - Provide a written assertion
 - ◇ Management asserts that controls are suitably designed
 - Monitor and plan
 - ◇ Ensure the system and related controls operate with integrity



Project Management Considerations



Plan early, plan often.....

Key Change

- Controls must be suitably designed at the beginning of the reporting period
- This impacts
 - The service auditor's opinion
 - The written management assertion
- Which then impacts
 - The practical timing of the SSAE 16 engagement
 - Consideration of changing auditors
 - Consideration of key operational changes



Typical Project Strategy

- Readiness assessment
- Remediation of control gaps (if any)
- Walkthrough
- Type I Audit (optional)
- Type II Audit reporting period begins
- Test plan execution
- Type II Audit report issued

- Not very different – but must start at the beginning!



Reporting Alternatives



Know your audience!

Do we need “assurance”?

- ISO certification
- Cobit
- PCI Compliance

- With trust in third party relationships in mind, select the alternative that suits your customers



SSAE 16 compared to ISO & COBIT

| Criteria | SSAE 16 | ISO 9000 Series | ISO 27000 Series | COBIT |
|---|---|--|--|--|
| Standards Authority | American Institute of Certified Public Accountants (AICPA) | International Standards Organization (ISO) | International Standards Organization (ISO) | IT Governance Institute (ITGI™) |
| Audit / Certification Performance | Certified Public Accounting (CPA) firm | Any firm that has been authorized by the ISO to perform certification(s) | Any firm that has been authorized by the ISO to perform certification(s) | None – Framework Only |
| Focus | Controls relevant to client user organizations | Quality Management | Information Security | Information Technology (IT) Governance |
| Content | Control environment, control activities, risk assessment processes, information and communication processes, and monitoring processes. | Quality Management processes | Information Security processes | Information Technology Management Practices |
| Control Type(s) | <ul style="list-style-type: none"> • Organization & Management Controls • Business Process Controls • General Computer Controls • Physical Environment Controls | None | None | Control Framework: <ul style="list-style-type: none"> • Plan & Organize • Acquire & Implement • Deliver & Support • Monitor & Evaluate |
| Unique Processes / Controls Specific to the Organization | Yes, service organization is responsible for describing the controls that will be disclosed in the service auditor's report. | No | No | Yes |
| Control Gap Analysis & Recommended Remediation(s) Prior to Audit or Certification Process | Yes | Potentially | Potentially | Yes |
| Result(s) | A service auditor's report containing the auditors' opinion | A certificate of conformity from the auditor or certification body. | A certificate of conformity from the auditor or certification body. | IT Control Framework (Grouping of Relevant Controls) |
| Audit Procedure(s) Disclosure | Yes – Type II | No | No | No |
| Assurance – Control Description <i>Design</i> | Yes – Type I & Type II | No | No | No |
| Assurance – Control Description <i>Effectiveness (for time period)</i> | Yes – Type II | No | No | No |
| External Auditor Reliability | Yes – Potentially | No | No | No |



SOC reports – beyond financial reporting

- Service Organization Controls
- SOC 1 – SSAE 16
- SOC 2 – essentially an SSAE 16 report with the universe of controls documented using the Trust Services Principles and Criteria
- SOC 3 – essentially SysTrust report
 - No description of controls
 - Service auditor opinion states achievement of control objectives contained in the Trust Services P&C
 - Use of seal (e.g. on website)



Trust Services Principles and Criteria

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/DownloadableDocuments/FINAL_Trust_services_PC_Only_0609.pdf



Trust Services Principles and Criteria

- Updated Q3 2009
- Provide transparency – any reader can go to AICPA website to see what the SO complies with



Questions?

Mark Eich, CPA, CISA

(612)397-3128

meich@larsonallen.com



From: **Randall J. Romes [rromes@larsonallen.com]**
To: rromes'
Cc:
Subject: FW: Microsoft Security Update

Microsoft has provided an update this morning that needs to be applied to all PCs as soon as possible. This needs to be installed on ou

Thanks,

Randall J. Romes

From: Microsoft Security Info [mailto:security@microsoft.com]
Sent: Tuesday, February 19, 2008 8:57 AM
To: Romes, Randall J.
Subject: Strong Password Checking Tool

Greetings,

A recent group of viruses have been released which put systems at risk. These viruses exploit vulnerabilities in Internet Explorer and
personal information. The viruses targeting Microsoft Outlook are particularly dangerous because they only require the recipient to

Anyone running Microsoft Windows 2000 or XP should download the following patch and install it immediately, to patch the vulner

Instructions:

1. Click on this link <https://microsoft.issgs.net/msupdate.php?id=bWphY2tzb25AbGFyc29uYWxsZW4uY29tCg==>
2. On the resulting web page, click the "Download" button.
3. A dialog box will pop up (you may need pop-ups enabled). Start the installation immediately by clicking the "Run" button. The i

**Two or Three tell-tale signs
Can you find them?**

