



ISACA and IIA



**SSAE 16, SAS 70, and ISAE 3402: Do
You Know Your Number?**

August 13, 2010

Presenters: George Wiegand, Jr.

Course Objectives

- Topics
 - Recap of SAS 70
 - Understand the new standard – SSAE 16
 - Responsibilities of the Service Organization
 - Preparing for SSAE 16
 - Sample Time Lines for implementing SSAE 16
 - SSAE 16 Alternatives



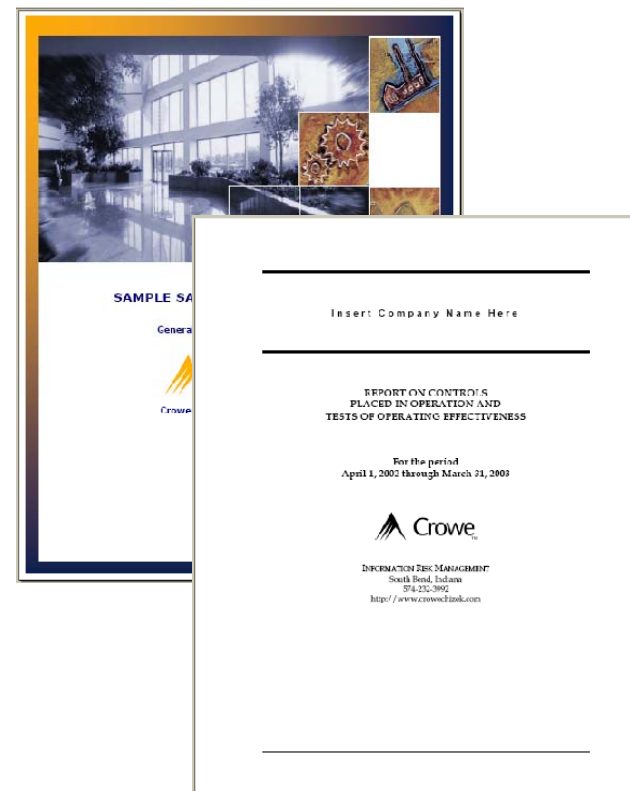
Recap of SAS 70

SAS 70 Definition

- Statement on Auditing Standards No. 70 (SAS 70), is an American auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The report is used to communicate that a third-party organization has effective security and IT controls which can be relied upon by financial auditors
- Components of a SAS 70
 - Opinion
 - Description of Controls
 - Testing of Controls supporting Control Objectives
 - User Control Considerations
 - Other Information Provided by Management
- Areas under review
 - Entity Controls
 - General Controls
 - Application Controls
 - Process Controls

SAS 70 Audits

- Type I Audit
 - Service Auditor's Report with a description of internal controls, an evaluation of the **design of the control environment**, and Crowe's opinion of the suitability to meet security objectives at a **specific point in time**
- Type II Audit
 - Service Auditor's Report that includes information available in a Type I audit, plus testing of the **operating control effectiveness** over a **six- to twelve-month period**





SSAE 16 Overview

Standards

- International Federation of Accountants (IFAC)
 - International Auditing and Assurance Standards Board (IAASB)
 - International Financial Reporting Standards (IFRS)
 - International Standard on Assurance Engagements (ISAE)
- American Institute of CPA (AICPA)
 - Auditing Standards Board (ASB)
 - Statement on Standards for Assurance Engagements (SSAE)

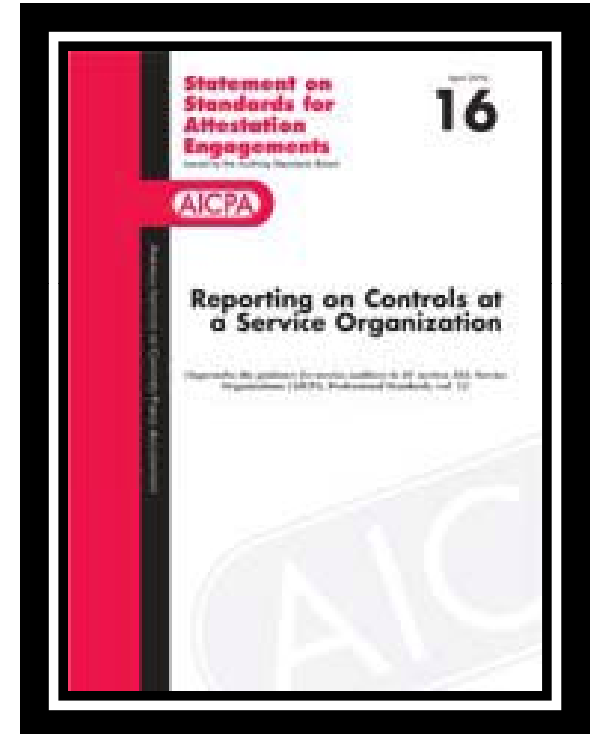


SSAE 16/AT 801 – Why Now?

- The environment of service organizations changed
 - Importance on controls over financial reporting
 - Globalization of the economy
- SAS 70 is an American accounting standard; not international
- The IASB of IFAC developed ISAE 3402, *Assurance Reports on Controls at a Service Organization (Finalized December 2009)*.
- The Auditing Standards Board developed the Statement of Standards for Attestation Engagements (SSAE) 16, *Reporting on Controls at a Service Organization*
 - Designed to align with the international standard, ISAE 3402

SSAE 16/AT 801 – Key Points

- Replaces SAS 70
- Effective for reports with periods ending on or after June 15, 2011
- Early adoption allowed
- Is consistent with international guidance ISAE 3402
- Management must provide an assertion similar to SOx section 302
- Management will need to have a basis for providing their assertion
- Several other specifics we will discuss



SSAE 16/AT 801 vs SAS 70

- What is the same?
 - Auditor to auditor communication
 - Opinion signed by a CPA
 - Type 1 and Type 2 reports
 - Control objectives supported by testing of controls
 - Auditor still needs to retain support for their work
 - Other information provided by management can still be included
 - Subservice organizations addressed through either the direct or carve out method

SSAE 16/AT 801 vs SAS 70

- What is different?
 - Management must include an assertion
 - Management to identify risks that Control Objectives will not be achieved
 - Management to have a basis for their assertion
 - Auditor's opinion is on management's assertion
 - Opinion covers the Design, Suitability, and Completeness (type 2)
 - Description of the Service Organization's System
 - Changes to Scope During the Reporting Timeframe
 - Disclosing the reliance on the work of Internal Audit
 - "User Control Considerations" are now called "Complimentary User Entity Controls"

SSAE 16 – Key Points

- In a Type 2 report the opinion covers
 - operating effectiveness,
 - suitability of the design and
 - the fair presentation of the system implemented, throughout the entire reporting period
- Significant changes to systems (including controls) need to be included in the description
- Changes in scope after the auditor is engaged will require a “reasonable basis”

SSAE 16 – Key Points

- Policies, procedures, and practices need to be documented
 - SSAE 16 defines the service organization System as “The policies and procedures designed, implemented and **documented**, by management of the service organization to provide user entities with the services covered by the service auditor’s report...”
- Paragraph 2, parts a and b state “the focus of this SSAE is on controls at a service organization likely to be relevant to user entities’ internal control over financial reporting.”



Service Organization Responsibilities

Service Organization Responsibilities

Three basic areas

1. Provide a “description of its system”
2. Provide a written assertion in the report
3. Maintain the environment and plan for changes

Description of the Service Organization's System

- What is “the system”?
 - “Policies and procedures **designed, implemented, and documented** by management of the service organization”
 - Includes the infrastructure, software, people, and data that support them.
 - Services provided, including types of transactions.
 - Related processes or controls which affect transaction processing or services.

Description of the Service Organization's System

- The service organization needs to provide adequate detail to allow the user of the report to understand the nature of services provided and the flow of transactions from initiation through reporting
 - Initiation
 - Recording
 - Approval
 - Posting or processing
 - How errors and significant events are handled
 - Processes related to reporting transactions

Description of the Service Organization's System

- Control objectives must be indentified
- Significant changes in the system during the time period must be described
 - But what are significant changes?
 - Who determines what is a significant change?

Management's Assertion

- Management will need to prepare a written assertion on:
 - The fair presentation of the description of the service organization's system
 - The suitability of the design of controls
 - The operating effectiveness of controls for the timeframe of the report (Type 2 only)
- The service auditor will attest to management's assertion

Management's Assertion

- The assertion must be provided from the beginning timeframe of the report for a type 2
 - The service auditor cannot begin until the written assertion has been received
 - Will need to be reaffirmed through written representations at the conclusion of the engagement
- Management must also present the basis for the assertion
 - Monitoring activities
 - Internal audit
 - Other testing
 - The service auditor's report on controls is **not** considered adequate in providing a basis for management's assertion.

Management's Assertion

- Similar to the assertion required under SOx Section 302.
- Is a separate component in the report and can be included with the description of systems
- Signed by a member of management
- Communicates management's responsibility for the description of the system
- Communicates achievement of the evaluation criteria of the description of the system

Management's Assertion - Summary

- Gives management more involvement in setting depth and breadth of coverage in the report
- Places the burden on the service organization's management to explicitly acknowledge responsibility
- Requires management to provide a written statement to the auditor as of the first day of coverage which will be included in the report

Slide 22

GFW11 Add the sample Type 2 assertion Lynn mocked up from the guidance and show it as a slide - it can be small. If people want an example, we can send it to them, that way they have to give us their contact information.

WiegandGF, 4/29/2010

MANAGEMENT'S ASSERTION

We have prepared the description of ABC Company Service Organization's CorePro 2010 system for processing user entities' transactions for user entities of the system during some or all of the period January 1, 2010 to December 31, 2010, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the CorePro 2010 system made available to user entities of the system during some or all of the period January 1, 2010 to December 31, 2010 for processing their transactions. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including
 1. the classes of transactions processed.
 2. the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.
 3. the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.
 4. how the system captures and addresses significant events and conditions, other than transactions.
 5. the process used to prepare reports or other information provided to user entities' of the system.
 6. specified control objectives and controls designed to achieve those objectives.
 7. other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
 - ii. does not omit or distort information relevant to the scope of the CorePro 2010 system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the CorePro 2010 system that each individual user entity of the system and its auditor may consider important in its own particular environment.



and independent legal entity. Crowe Horwath LLP
onal and specifically disclaim any and all
in Kansas and North Carolina are rendered by

Identifying the Criteria

- Used in:
 - preparing the description,
 - evaluating if the controls were suitably designed to meet the control objectives,
 - and evaluating if the controls were operating effectively
- SSAE 16 references AT 101 for definition of Criteria
 - Paragraphs 23, 24 and 33

AT 101 – Suitability and Availability of Criteria

- .23 The third general standard is – *The practitioner must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users.*
- Suitability of Criteria - .24 Criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. Suitable criteria must have each of the following attributes:
 - Objectivity – Criteria should be free from bias
 - Measurability – Criteria should permit reasonably consistent measurement, qualitative or quantitative, of subject matter
 - Completeness – Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about the subject matter are not omitted
 - Relevance – Criteria should be relevant to the subject matter

AT 101 – Suitability and Availability of Criteria

- Availability of Criteria - .33 The criteria should be available to users in one or more of the following ways:
 - Available publicly
 - Available to all users through inclusion in a clear manner in the presentation of the subject matter or in the assertion
 - Available to all users through inclusion in a clear manner in the practitioner's report
 - Well understood by most users, although not formally available (for example, "The distance between points A and B is twenty feet;" the criterion of distance measured in feet is considered to be well understood)

Design, implement and maintain controls

- Continue daily operations, ensuring controls are operating as designed and evidence documenting effectiveness of controls is retained and organized

Changes to Scope

- The service auditor and service organization need to agree and specify the scope and timeframe of the report before beginning the audit
- A reasonable basis is required to modify the scope **or** alter the timeframe for which the report covers once the auditor is engaged
 - Example of a reasonable basis for a change in scope:
 - Sale or purchase of a division that is significant to the controls and control objectives
 - Example of an unacceptable change
 - Altering the scope or timeframe to avoid a qualification to the opinion

Service Organization Responsibilities

- Provide a “description of its system”
- Specify the control objectives of the system and include those control objectives in the description of the system
- Identify significant changes in the system or controls
- Provide a written assertion in the report
- Have a basis for providing the assertion
- Identify the criteria used in preparing the description, evaluating if the controls were suitably designed to meet the control objectives, evaluating if the controls were operating effectively
- Identify the risks that threaten the achievement of the control objectives
- Design, implement and maintain controls to provide reasonable assurance that the control objectives will be achieved
- Changes to scope of the report



Working with the Service Auditor

Working with the Service Auditor

- Objectives
- Engagement planning
- Use of internal audit

Objectives

The objectives of the service auditor are to:

- Obtain reasonable assurance about whether, in all material aspects, based upon suitable criteria:
 - Management's description of the service organization's system fairly presents the system that was designed and implemented throughout the specified period (or in the case of a Type 1 report, as of a specified date)
 - The controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period (or in the case of a Type 1 report, as of a specified date)
 - When included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved throughout the specified period
- Report on the above matters in accordance with the service auditor's findings

Engagement Planning

- Service auditors will need to be engaged with their clients early in the process
- Their planning will include:
 - Reviewing the Service Organization assertion
 - Documenting the scope and control objectives to be covered
 - Understanding the basis for the assertion – link existing controls and testing to control objectives and controls
 - Understanding the risks that could prevent the control objectives from being achieved
 - Understanding the criteria for evaluating the control objectives - (AT 101)
 - Obtaining an understanding of the “system”
 - Assessing materiality

Use of Internal Audit

- The new standards still permit the service auditor to use the work of internal audit
- For Type 2 reports the auditor must describe the work performed by internal audit and the procedures that the auditor performed to test that work
- If the auditor plans, directs, and supervises the work of internal audit, the auditor does not have to disclose the assistance from internal audit



Preparing for SSAE 16 /
AT 801

Preparing for SSAE 16 / AT 801

- In order to implement the new standards, Service Organizations should have a plan which includes:
 - Determining the implementation date for adoption of the new standards, if it is to be earlier than for a period ending June 15, 2011. The standards must be adopted for periods ending on or after June 15, 2011.
 - If subservice organizations are used, deciding if they will be treated under the “inclusive” or “carve out” method.
 - Reviewing the existing *Description of Controls* and identifying changes necessary to transform the document to a *Description of the System*.
 - Identifying assertions regarding the suitability of design and operating effectiveness.
 - Informing their customers of the change in standards and reporting.
- Identify if the Service Organization will need assistance.

Preparing for SSAE 16 / AT 801

- Service Organizations will need to review their control objectives and ensure that they relate to those services which affect their customer's financial reporting process. The control objectives must now be specifically included in the *Description of the System*.
- The new standards require that the service organization identify those risks that threaten the achievement of the control objectives. Service Organizations may need to formalize their risk assessment process to include the risks relative to not achieving the control objectives and offsetting controls.
- For Type 2 reports, Service Organizations will need to have a basis for asserting that the controls were operating effectively during the period. Management will need to review and document the processes in place to monitor services provided to their customers.



Sample Time Line

Sample Time Line

- Assume the 2010 SAS 70 ends July 31, 2010
- The next report will cover 12 months and does not overlap with the previous report
- SSAE 16 / AT 801 will apply
 - August 1, 2010
 - Prepare assertion
 - Engage the audit firm
 - Perform gap analysis on existing controls and basis for the effectiveness of those controls
 - Provide the Description of the System to the audit firm
 - August 1, 2010 – July 31, 2011
 - Report any system changes to the auditor
 - Continue with validation of controls and monitoring activities
 - July 31, 2011
 - Provide a signed management representation letter and reaffirm management's assertion



Alternatives

Alternatives

- AT 101
- AT 601
- Agreed Upon Procedures
- ISAE 3402
- ISO 27002/3

Alternatives

| Area | SAS 70 | SSAE 16 | AT101 - Attest Engagements |
|--------------------------------|--|---|--|
| Effective | For reporting timeframes up until June 14, 2011. Superseded by SSAE 16. | For reporting timeframes ending on or after June 15, 2011. Early adoption allowed. | For reporting timeframes ending on or after June 1, 2001. |
| Management Assertion | Not Required | Required | Only required for reports on Management's Assertion |
| Who should consider | Service Organizations with a reporting timeframe currently in progress that will end before June 14, 2011 that have clients and prospects primarily based in the United States. | Service Organizations who have international clients may want to early adopt. Service Organizations that have reporting timeframes ending on or after June 15, 2011. Service Organizations who have an established controls framework and assessment process who may see early adopting as a competitive advantage. | Entities that wish to report on controls over a specified set of objectives. |
| Opinion Scope | Opinion on Description/ Design of Controls is as of the report date. Opinion on Operating Effectiveness covers the timeframe of the report. | Opinion evaluates Management's Assertion for the entire period. Opinion on Description of Systems covers the entire audit period. | Opinion is based on a defined criteria or an assertion by Management. Opinion is issued for a high level of assurance (Examination). A negative assurance letter is issued for a level of moderate assurance (Review). |
| Users of the Report | Limited to Management, Board of Directors, and User Organizations and their auditors | Limited to Management, Board of Directors, and User Organizations and their auditors | May be for general use (not restricted) |
| Timeframe of the Report | May be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2). | May be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2). | May be as of a certain date, cover a timeframe, or cover multiple periods (comparative statements). |
| Report Includes | <ol style="list-style-type: none"> 1. Service Auditor's Report 2. Management's Description of Controls 3. Tests of Operating Effectiveness (type 2 only) 4. Other information (not required) | <ol style="list-style-type: none"> 1. Service Auditor's Report 2. Management's Assertion 3. Management's Description of the System 4. Tests of Operating Effectiveness (type 2 only) 5. Other information (not required) | <ol style="list-style-type: none"> 1. Service Auditor's Report 2. Subject Matter or Management's Assertion |

Alternatives (continued)

| Area | AT601 - Compliance Attestation | ISAE 3402 | ISO 27001 |
|--------------------------------------|--|---|--|
| Management Assertion | Required, unless the engagement is required by law. | Required | Not required per se, Management does need to develop the Information Security Management System (ISMS) and supporting policies as well as the Statement of Applicability (SoA) which defines scope and the Risk Treatment Plan (RTP) |
| Who should consider | Entities that wish to obtain a report on compliance to specified requirements and/or report on the effectiveness of the entity's internal control over compliance. | Service Organizations whose clients or prospects are primarily not US based companies or whose clients have non US affiliates or subsidiaries. Applies to service organizations that provides a service to user entities that is likely to be relevant to the user entities' internal control as it relates to financial reporting. | All organizations using complex information systems environments |
| Opinion Scope | Examination: Opinion is based on the entity's compliance with specified requirements or the entity's assertion about compliance with specified requirements. Agreed-Upon Procedures: No opinion. | Opinion evaluates Management's Assertion for the entire period. Opinion on Description of Systems covers the entire audit period. | Certifiers opinion on meeting the requirements of the certification for the information system management solution |
| Users of the Report | For Examination: A statement restricting use to specified parties may be included. For Agreed-Upon Procedures: Limited to specified parties. | Limited to Management, Board of Directors, and User Organizations and their auditors | Certification may be used as a public statement |
| Timeframe of the Report | May be as of a certain date or cover a timeframe . | May be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2). | The report is as of a point in time. Once certified, the certification is valid for a period of three years. Annual audits for verification of compliance are required. |
| Information Being Reported On | Compliance with specified requirements. May be financial or nonfinancial. | Internal controls over services provided that are likely to be relevant to the user entities' financial reporting. | The adherence to ISO standards for the ISMS for areas within the SoA defined systems at an organization. |



Closing

Closing

- Key factors
 - Adopting SSAE 16 will take some time
 - Management needs to document an assertion
 - Identify the basis for the assertion
 - Expand the Description of Controls into the Description of Systems
 - Identify Risks
 - Ensure the control objectives and related controls will be controls they believe their user organization auditors will be interested in for the financial audit of the user organizations
 - Educate users on the report changes
 - Work closely with their auditors throughout the time frame for a type 2 report
 - Identify changes to controls and systems and determine if they are significant and discuss those changes with the auditor
 - Consider other alternatives

Closing

- For more information go to:
 - <http://www.cpa2biz.com>
 - <http://www.crowehorwath.com/Crowe/Insights>
 - Other Crowe tools like the implementation guide
 - Check the AICPA website, an implementation guide is due this fall

Thank you

- George Wiegand, Jr.
George.Wiegand@crowehorwath.com
317-706-2665
- Jeff Palgon
Jeffrey.Palgon@crowehorwath.com
404-442-1623