SAS70 Type II Reports
Use and Interpretation for SOX

November 19, 2007

Presented by:
Erin Erickson, Senior Manager
Enterprise Governance

and

Brenda Karl, Director
Technology Risk Management
Agenda

- Background
- Benefits of a SAS70 Review
- The Sarbanes-Oxley Act of 2002
- Structure of SAS70 Reports
- Interpreting a SAS70 Type II Report
- Evaluating a SAS70 Report for Sarbanes-Oxley Compliance
- User Management’s Role
Background
What is a SAS 70?

**Definition:**

Statement on Auditing Standards No. 70: Service Organizations, commonly abbreviated as **SAS 70** and also known as AU sec. 324, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), officially titled “Reports on the Processing of Transactions by Service Organizations”.

**SAS 70** defines the professional standards used by a service auditor to assess the internal controls of a service organization and issue a service auditor’s report. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers.
The AICPA issued **SAS 55** titled “Consideration of the Internal Control Structure in a Financial Statement Audit”. SAS 55 required that financial statement auditors assess the internal controls related to any process that could impact the client’s financial reporting objectives.

**SAS 55** requires auditors to perform reviews of internal controls at significant service providers.

Service providers were visited annually by numerous clients/auditors.

**SAS 70** was created to effectively allow one independent audit rather than many.

**SAS 55** was amended by **SAS 94**, titled “The Effect of Information Technology on the Auditor’s Consideration of Internal Control in a Financial Statement Audit”.

**SAS 94** affected **SAS 70** by increasing the focus on Information Technology in internal control reviews.
Common Terminology

- Common terminology associated with SAS 70 Reviews includes:
  - **Service Provider:** The organization providing services
  - **User Organization:** Clients of the service provider
  - **User Auditor:** The internal and/or external auditors of the user organization
  - **Service Auditor:** The audit firm performing the SAS 70 review
Common Terminology (cont.)

- **Service Provider Controls**: Controls at a service organization that may be a part of a user organization's information system in the context of an audit of the user's financial statements. They do not include service organization controls that are not relevant to a user organization's information system.

- **Restricted-use report**: A SAS 70 report is a "restricted-use" report intended for use by the service organization, user organizations and user auditors. SAS 70 reports are generally not appropriate for use by prospective customers.
When is a SAS 70 Applicable?

- A SAS 70 review is applicable when elements of a company’s processes are performed by a service provider and the company:
  - Needs assurance over the system of internal controls at the provider because the services/transactions affect their financial statements.
  - Needs assurance that the service provider is fulfilling contractual obligations.
  - Wants to gain a better understanding of their role in controlling the process.
When is a SAS 70 Applicable? (cont.)

There are numerous types of services that may be performed by an outsourced service provider:

- Payroll
- Investment Management
- Custody and Trust
- IT Processing
- Human Resources
- Benefit Management
- Web Hosting
- Credit Card Processing
- 401k Management
- Telecommunications
- Finance
- Accounts Payable
- Accounts Receivable
- Commodity Trading Support
Types of SAS 70 Reports

There are two types of SAS 70 reports: **Type I** and **Type II**

**Type I Report:**
- Assessment of controls over relevant systems, processes and underlying information technology environments
- Determination of whether identified controls are suitably designed and in operation at a point in time
- Service auditor gives an opinion on the effective design of controls as of a point in time
- No detailed testing of controls performed
- Provides user auditors with an understanding of the controls necessary to plan a financial statement audit
Types of SAS 70 Reports (cont.)

Type II Report:

- Includes tests of the operating effectiveness of a service organization’s controls for a period of time
- Provides highly useful information about the nature, timing, and results of tests of controls
- Provides for an opinion regarding the reasonable assurance controls are operating effectively
- User organization auditor can place reliance on the results from Type II audit procedures and report

*This is the type of report required by Sarbanes-Oxley Section 404*
Benefits of a SAS 70 Review
Benefits of a SAS 70 Review

- SAS 70 Reviews can provide numerous benefits to both user organizations and service providers:
  - **Can establish trust** – a SAS 70 Type II report with an unqualified opinion issued by an independent firm demonstrates the establishment of an effective system of internal controls.
  - **Can reduce internal costs** – without a current SAS 70 report, the burden for establishing the effectiveness of design and operation of the service providers’ system of internal controls falls to the user organization. For service providers, the costs may be significant in entertaining audits from numerous clients.
Benefits of a SAS 70 Review (cont.)

- **Provides concise, consistent information** – A SAS 70 report provides user organizations with detailed information on the services providers’ system of internal controls in a prescribed format that can be used by management, internal auditors, and external auditors.

- **Identifies opportunities for process and control improvements** – Through effective review and understanding of client control considerations, user organizations can improve their own internal system of internal controls. Service providers benefit from the identification of control deficiencies.
Benefits of a SAS 70 Review (cont.)

- **The standard is internationally recognized** – SAS 70 reporting is not only widely used in the United States, it is also recognized by auditors globally as an effective standard for obtaining assurance of controls in place at a service organization.

- **Can provide early-warning signs of potential problems** – Depending on the timing of the review, a SAS 70 review can provide user organizations information on areas where they need to strengthen their internal controls.
Benefits of a SAS 70 Review (cont.)

Key Benefit and Focus of Today’s Discussion

- Supports management’s assertion on the design and effectiveness of an entities’ system of internal control over financial reporting in compliance with Sarbanes-Oxley section 404.
The Sarbanes-Oxley Act of 2002
The **Sarbanes-Oxley Act of 2002** (“Act”) was passed by Congress and signed into law by the President on July 30, 2002. This legislation was, in part, a reaction to restore shareholder trust in the wake of high profile business failures, allegations of corporate fraud and financial statement restatements. The Act brought increased accountability for corporate governance and enhanced internal control over corporate financial reporting. Included in the Act are several sections that address internal control reporting with stiffer federal sentencing guidelines for non-compliance.

- Established the **PCAOB** as a administrative, monitoring, and rulemaking body.
Section 404(a) of the Act

**Section 404(a)** of the Act requires the SEC to adopt rules requiring annual reports to contain an assessment, as of the end of the issuer’s fiscal year, of the effectiveness of internal control over financial reporting. Section 404(b) of the Act requires the Public Company Accounting Oversight Board (“PCAOB”) to adopt standards for independent auditors to attest to management’s assessment of internal control.
On March 9, 2004, the PCAOB issued **Audit Standard 2 (AS2)** which outlines the overall rules by which SOX section 404 would be audited. This has since been replaced by Audit Standard 5 (AS5).

Given a lack of standards on how section 404 would be implemented by SEC filers, this standard also became the de-facto implementation guidance for companies.

Rules were included which address the use of service organizations and the relationship to the internal control attestation and opinion.
The use of SAS 70 reports is discussed in:

- AS 2, Appendix B, Paragraphs 18 – 29 “Use of Service Organizations”
- AS 5, Appendix B, Paragraphs 17 – 27 “Use of Service Organizations”
- PCAOB Staff Questions and Answers, Questions 24, 25, 26, 28, and 29.
The Standards reference AU sec. 324.03 as the defining criteria on whether a service organization is part of an organization’s information system:

- The service provider performs a significant class of transactions
- The procedures performed relate to transactions that impact the accounting records and financial statements
- The provider impacts how events or conditions are captured
- Processes impact the financial reporting process including estimates and disclosures
When the scope of SOX 404 dictates the service organization’s services are part of the company’s internal control over financial reporting, management’s assessment and the audit should include:

- Obtaining an understanding of the controls at the service organization that are relevant to the entity's internal control and the controls at the user organization over the activities of the service organization *(Design)*

- Obtaining evidence that the controls that are relevant to the auditor's opinion are operating effectively. *(Effectiveness – Type II)*
Procedures to perform the audit and management’s assessment include:

- **Obtaining a service auditor's report on controls placed in operation and tests of operating effectiveness**

- A report on the application of agreed upon procedures that describes relevant tests of controls.

- Performing tests of the user organization's controls over the activities of the service organization.

- Performing tests of controls at the service organization.
Management and the auditor should evaluate whether the SAS 70 report provides sufficient evidence to support the assessment and opinion, respectively. The following should be considered in this evaluation:

- The time period covered by the report
- Scope of the review and the applications covered
- The overall report opinion and results of tests of controls

AS5 – Appendix B, Paragraph 21
PCAOB Standards – AS2/AS5

- If the report contains any qualifications, management and the auditor should evaluate whether the company is applying the necessary procedures. These procedures are likely to be substantive in nature to ensure a failure of controls has not resulted in a specific issue.

- Management and the auditor should inquire as to the service auditor’s reputation, competence, and independence.

AS5 – Appendix B, Paragraphs 22 & 23
If a significant amount of time has passed between the period covered by the report and management’s assertion, additional procedure should be performed:

- A “significant amount of time” is not defined. The report should generally be with six months of management’s assertion.
- Additional procedure should include, at a minimum, a review of changes since the SAS 70 report period.
- Further procedures may be necessary based on time and changes which have occurred.
Other potential reasons for obtaining additional evidence include the following factors. As these factors increase in significance, the need to obtain additional evidence increases.

- Significance of the activities of the service organization
- Whether errors were identified in the processing of the service organization
- The nature and significance of any changes in the service organization’s controls identified by management or the auditor
If it is concluded that additional evidence about the operating effectiveness of controls at the service organization is required, this evidence may include:

- Evaluating procedures performed by management and the results of those procedures.
- Contacting the service organization, through the user organization, to obtain specific information.
- Requesting that a service auditor be engaged to perform procedures that will supply the necessary information.
- Visiting the service organization and performing such procedures.
The PCAOB has issued a series of Staff Questions and Answers to provide additional clarity on the intentions of the standards:

- What types of outsourcing activities result in a service organization arrangement addressed by Statement on Auditing Standards ("SAS") No. 70, *Service Organizations* (AU sec. 324)? What types of outsourcing activities are part of a company's internal control over financial reporting?
  - Those as described in AU sec. 324.03 (prior slide)
  - Excludes those covered by AU sec. 336 (SAS 73)
Auditing Standard No. 2 indicates that evidence about the operating effectiveness of controls at a service organization can be obtained from a Type 2 SAS No. 70 report. Is a Type 2 SAS No. 70 report issued more than six months prior to the date of management's assessment current enough to provide any such evidence?

- There are no “bright lines”
- Management and the auditor should evaluate the need for additional procedures
- Evaluation may focus on change management
Can a registered public accounting firm in the integrated audit of an issuer obtain evidence from a service auditor's report issued by a non-registered public accounting firm?

Yes. Management and the auditor should evaluate the reputation, competence, and independence of the firm as part of its evaluation.
Paragraph 79 of Auditing Standard No. 2 requires the auditor to perform at least one walkthrough for each major class of transactions…If a service organization's services involve the processing of a major class of transactions, should the company's auditor perform walkthroughs at the service organization?

- Yes, a SAS 70 can be relied upon to cover a walkthrough
- With AS5, walkthroughs are no longer a requirement
Structure of SAS70 Reports
## SAS70 Report Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Responsibility</th>
<th>Type I</th>
<th>Type II</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Independent Service Auditor’s Opinion</td>
<td>Service Auditor</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>II. Service Organization’s Description of Controls</td>
<td>Service Organization</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>III. Service Auditor’s Tests of Operating Effectiveness</td>
<td>Service Auditor</td>
<td>N/A</td>
<td>X</td>
</tr>
<tr>
<td>IV. Other Information Provided by Service Organization</td>
<td>Service Organization</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Section I – Auditor’s Opinion

- **Type I**
  - An opinion on the fairness of presentation of the description of controls and procedures provided by the service organization
  - An opinion on the appropriateness of design of the controls to meet the control objectives

- **Type II**
  - Type I opinions, plus
  - An opinion on the operating effectiveness of the controls that have been tested by the independent service auditor
Auditor’s Opinions

- **Description of Controls**
  - In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects the relevant aspects of Service Provider controls that had been placed in operation as of June 30, 2007.

- **Design of Controls**
  - Also, in our opinion, the controls as described are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and clients of Service Provider applied the controls contemplated in the design of Service Provider’s controls.
Auditor’s Opinions

- Operating Effectiveness
  - In our opinion, the controls that were tested, as described in section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives in section III were achieved during the period from January 1, 2007 to June 30, 2007.
Types of Opinions – Unqualified / “Clean”

- An **Unqualified Opinion** is issued by an auditor when the financial statements presented are free of material misstatements and are in accordance with GAAP, which in other words means that the company’s financial condition, position, and operations are fairly presented in the financial statements.

- “In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position . . . .”
Types of Opinions – Qualified

- A **Qualified Opinion** is issued when the auditor encountered one of two types of situations which do not comply with generally accepted accounting principles; however, the rest of the financial statements are fairly presented.
- The two types of situations which would cause an auditor to issue this opinion are:
  - Single deviation from GAAP
  - Scope of limitation
- “In our opinion, *except for the effects of the Company’s incorrect determination of depreciation expense, the financial statement* . . . . “
Section II – Description of Controls

Section II describes aspects of the service organization as they relate to the services provided to the user organizations, using the COSO model.

- **Control Environment** – Board of Directors, management’s philosophy, organizational structure, corporate HR policies, hiring and training practices
- **Risk Assessment** – management of risks around the financial reporting process, fraud risk
- **Information and Communication** – information is identified, captured, description of the processes and systems, communication of roles and responsibilities
- **Monitoring** – ongoing and/or separate evaluations enable management to determine whether internal control over financial reporting is present and functioning.
- **Control Activities** – actions are taken to address risks, financial and information technology controls, policies and procedures related to financial reporting are established
Client Control Considerations

- The set of controls that are *internal* to the user organization that user management should consider to achieve the control objectives identified in the SAS70 report.
- The client control considerations presented by the Service Auditor firm should not be regarded as a comprehensive list of all controls that should be employed by the client.
The Control Objectives should:

- Assist the user auditor to determine how the service organization’s controls affect the user organization’s financial statement assertions
- Be tailored to the services provided by the service organization
- Include the related general computer control objectives and specific controls
- Address financial statement assertions, including safeguarding of assets

Control Objectives dealing with compliance or non-financial statement assertions are not included in scope.
Section III – Tests of Operating Effectiveness

- A description of the tests of operating effectiveness and the results of those tests (Type II only)
  - The control objectives the controls were intended to achieve that support testing
  - The specific controls that were tested
  - An indication of the nature, timing, extent, and results of the tests applied in sufficient detail to enable user auditors to determine the effect of such tests on their assessments of control risk
- Relevant exceptions are disclosed, regardless of their impact on the audit opinion
Section IV – Other Information

- Optional and **unaudited** information the service provider may wish to share with the user organizations
  - Disaster Recovery Plans
  - Business Continuity Plans
  - Acronym Descriptions
  - Performance and Operational Statistics
  - Process Flows
  - System Enhancements
  - Segregation of Duties Enhancements
Roles & Responsibilities

- **Service Provider**
  - Identifies the services and locations in scope
  - Defines control objectives related to the services in scope

- **Service Auditor**
  - Reviews the completeness and appropriateness of the control objectives
Companies are demanding SAS 70 reports and other assurances from providers.

- Require Type II SAS 70 Report: 86%
- Visit Provider to Evaluate Controls: 26%
- Perform Audit Tests of Inputs and Outputs: 19%
- Require Type I SAS 70 Report: 1%

CFO Magazine January 2005

Accretive Solutions
Interpreting a SAS70 Type II Report
User Organizations and User Auditors should ask the following questions:

- Is it a Type I or Type II report?
- What is the scope? Does it include:
  - Sub service organizations?
  - Multiple locations?
  - Multiple computing environments?
- Is my environment included in the report?
- What is the period covered?
- Are the control objectives comprehensive?
- What are the controls and how were they tested?
  - Are the tests robust or are they inquiry only?
How to Get Started, cont.

- What are the results?
  - Design exceptions?
  - Operating effectiveness exceptions?
- What are the client control considerations?
  - Are they too extensive?
  - Are key controls in place in my organization?
  - Have I tested them and are they operating effectively?
- What additional tests should I perform given the results of the SAS70?
- If qualified, how adequate are the management responses?
Let’s Review the Client Controls

- Client Control Considerations
  - Clients are responsible for understanding which services they have contracted for from the third-party provider.
  - Third-party provider systems are designed under the assumption that clients will implement certain controls.
  - Typically, specific client control considerations are provided for certain control objectives.
Provider Process Controls – Payroll Example

- Payroll Processing
  - Payroll Data Input – Authorization
  - Payroll Data Input – Data Validation
  - Payroll Output – Pay Statements & Reports
  - Payroll Output – Distribution
  - Payroll Processing Output – Money Movement Files
Payroll Example – *Provider Controls*

- Payroll Processing
  - Payroll Data Input – Authorization
    - Clients authenticate by providing a user ID, a password and/or digital certificate to the various provider supplied input programs (*automated control*).
    - The automated input applications authenticate to the communications systems by providing a user ID and/or pass phrase (*automated control*).
  - Tele data operators enter the payroll data provided on phone / fax / road payrolls using the PayData system. They authenticate using their user ID and password (*manual control*).
Payroll Example – *Client Controls*

- Client management is responsible for:
  - establishing proper controls over the use of IDs and passwords that are used to access and transmit payroll information;
  - granting and revoking access to the client’s employees to the payroll input systems;
  - reviewing periodically the assigned login profiles of their employees for the payroll input systems;
  - the preparation and authorization of worksheets and faxes that are sent to the provider;
  - notifying the provider of changes in the authorized contacts list; and
Provider Process Controls – Investment Example

- Accounting Services Controls
  - Trades processing
  - Investment income
  - Security pricing
  - Schedule D regulatory reports
Provider Process Controls – Card Services

- Client Implementation
  - Plan Set-up
  - Administrative procedures
  - Initial Data Load

- Client Delivery
  - Member recordkeeping
  - Processing calculations and settlement
  - Reporting
General Computer Controls

- Systems Development
- Change Control / Management
- Logical Access
- Computer Operations
- Environmental Controls
- Physical Access
- File and Data Backup
- Problem Management
- Data Transmissions
General Computer Control – Example

- **Control Objective** – Controls provide reasonable assurance that logical access to programs and data is restricted to authorized individuals.

- **Description of Control**
  - **Authentication**
    - Logical access to the XYZ mainframe system is controlled through IBM’s Resource Access Control Facility (RACF). XYZ associates are authenticated by providing a unique user ID and password.
  
  - **Password & Account Policies**
    - The Corporate Mainframe Security group configures RACF password controls that establish a mandatory password change upon first login and after a specific number of days, minimum password length, password complexity, and password history.

  - **Administrator Privileges**
    - Only appropriate IT personnel have access to the administrative-level RACF functionality for the XYZ mainframe.
The fieldwork portion of the SAS70 review, as performed by the Service Auditor, is composed of several stages:

- Determining the fairness of the presentation of controls by the service provider
- Testing of the design of the controls
- Testing of the operating effectiveness of the controls – Type II review only
- Evaluation of the results
Fieldwork – Fairness of Presentation

- Obtain an understanding of the business processes and supporting IT systems
- Obtain an understanding of the controls in place supporting the control objectives
- Confirm the controls procedures as stated are in place to achieve the control objectives
  - Inquiry, inspection of documents and reports, observation of the application of specific controls, walkthroughs performed
  - Determine if the description of controls as prepared by the service organization is presented fairly
Fieldwork – Test of Design

- Evaluate to determine that the controls are designed such that if properly implemented and performed, they would achieve their desired objectives
- Consider the linkage between the controls and the specified control objectives
- Evaluate the ability of the controls to prevent or detect errors related to the control objectives
- Consider sub-service providers
- Review client control considerations
Fieldwork – Tests of Operating Effectiveness

- Testing to determine that the control procedures were in operation during the period being reported on
  - Inquiry, inspection, observation, re-performance
  - Extent of testing:
    - Nature of the control – manual vs. automated
    - Frequency of the control to determine sample size
    - Significance of the control
    - Risk of failure – past history, changes in the design, competence of individuals performing the control
- Timing of testing:
  - Adequately represent the period of the review
  - Extent of documented evidence
  - Early testing allows for remediation of deficiencies
Fieldwork – Results Evaluation

- Judgment applied in the evaluation of the results of testing to determine the overall impact to the audit:
  - Systemic problems vs. isolated exceptions
  - Potential impact on the achievement of the associated control objective
  - Cause of the deviation
- If exceptions are noted, testing is typically extended to further substantiate a conclusion
- Identify and test compensating controls
- Results of testing are described in the report
Test of a Control Activity – Example

- **Control Objective** – Controls provide reasonable assurance that logical access to programs and data is restricted to authorized individuals.

- **Description of Control** – Logical access to the XYZ mainframe system is controlled through IBM’s Resource Access Control Facility (RACF) software. XYZ associates are authenticated by providing a unique user ID and password.

- **Test of Operating Effectiveness** – Inspected a selection of RACF user IDs to determine whether the user IDs were unique.
SAS70 – Test Results

- What if control deficiencies are found in testing?
  - When exceptions are noted, the service auditor may expand sample size or identify compensating controls to achieve a level of reliability control is functioning as intended.
  - If a significant number of exceptions are noted, the auditor may conclude the control objective cannot be met and issue a qualified opinion.
  - The auditor may issue an unqualified opinion despite testing exceptions if other controls are operating effectively.
Evaluating a SAS70 Report for Sarbanes-Oxley Compliance
Using a Process Controls Framework

- Based on SEC and PCAOB guidance, the vast majority of companies are using the COSO model for their internal controls framework.
- **COSO** stands for the **Committee Of Sponsoring Organizations of the Treadway Commission**
- The COSO model is made up of five elements:
  - Control Environment
  - Risk Assessment
  - Information and Communication
  - Monitoring
  - Control Activities
Using a Process Controls Framework

- Transaction processing controls generally fall into the category of Control Activities and occur at the process level.
- Process level control objectives are dictated by the material elements of the financial statements, and can vary from company to company.
- Some SAS 70 reports may also include controls falling into the other COSO elements – these controls are generally considered entity-level controls.
- User organizations are responsible for documenting and maintaining their own control framework over most entity-level elements, especially the control environment.
COSO, as recommended by the SEC, addresses the topic of IT controls, but does not dictate requirements for such control objectives and related control activities.

The IT Governance Institute published a reference guide entitled "IT Control Objectives for Sarbanes-Oxley" which reconciles a subset of the CobIT control objectives to the COSO framework for internal control.

The control objectives contained in this document can be used as the basis or framework for evaluating a SAS 70 service auditor's examination unless a proprietary framework has been developed internally.
Creating a Scorecard Template

- Using the ITGI’s IT Control Objectives for Sarbanes-Oxley:
  - Focus on key controls
  - Tailor the control objective template to fit a company’s specific circumstances
  - Consult with your external auditors to help ensure that all attestation-critical control objectives are addressed
- Use the COSO controls model for business process/financial controls
MAPPING EXERCISE
User Management’s Role
User Management’s Role

- Management of the user organization has a number of roles and responsibilities when utilizing a service provider for significant transactions
  - Contracting / acquiring services
    - Ensure contract includes a right to audit clause
    - Include language to require an annual SAS 70 report, including timing
User Management’s Role (cont.)

- Work with service provider to ensure that significant control objectives are part of the SAS 70 review
- Work with the service provider to understand client control considerations and ensure the appropriate activities are in place
- Discuss any known or perceived issues with the provider in a timely manner
- Communicate – don’t allow a qualified opinion to be a surprise
Contact Information

Erin S. Erickson, Senior Manager
Enterprise Governance
eerickson@accretivesolutions.com

Brenda L. Karl, Director
Technology Risk Management
bkarl@accretivesolutions.com