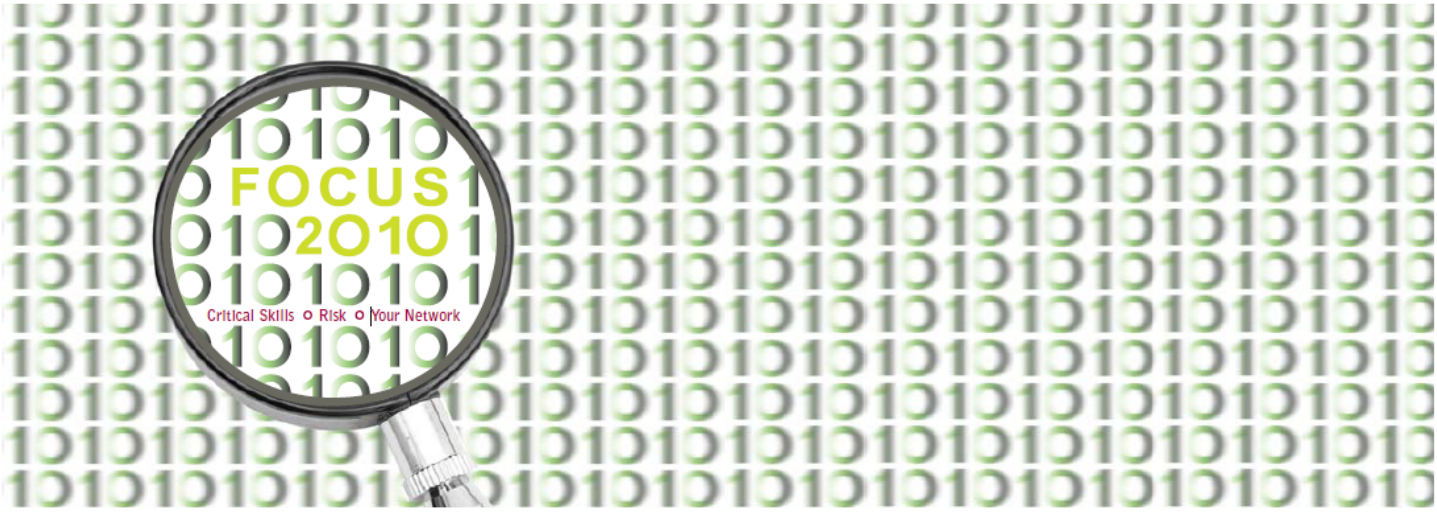
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



C22: SAS 70 Practices and Developments

Todd Bishop, PricewaterhouseCoopers

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

SAS No. 70
Practices & Developments

Todd Bishop
Director, Risk Assurance Services,
PricewaterhouseCoopers

Agenda

- SAS 70 Background Information and Overview
- SAS 70 Report Overview
- Performing a SAS 70 Audit – Key Considerations
- Using and Evaluating a SAS 70 Report
- The Use of Subservice Organizations
- Transitioning to SSAE16
- Appendix A – Common SAS 70 Terminology

ISACA
San Francisco Chapter

Background Information and Overview

Significant Outsourced Operations

- Increasingly, U.S. Companies (User Organization) outsource parts of their operations such as Payroll, Claims Processing, and Data Center Operations to other companies (Service Providers).
- Although a process has been outsourced, the user organization is responsible for the accuracy and integrity of the financial data associated with the outsourced process.
- The User Organization must understand the design and operating effectiveness of internal controls at the Service Provider and how those controls interact with their own.
- A SAS 70 report can be used to help reduce management's need to perform independent evaluation procedures of Service Provider's internal controls.

Statement on Auditing Standards (SAS) No. 70

- Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
- SAS 70 defines the professional standards used by a service auditor to assess the internal controls of a Service Provider and issue a report.
- A SAS 70 is a report prepared by an independent auditor on the internal controls at a Service Provider, for use by the customers of the Service Provider.
- The report includes the auditor's opinion issued to the Service Provider at the conclusion of the SAS 70 examination.

ISACA San Francisco Chapter

SAS 70 History

- The Statement on Auditing Standards (SAS) No. 70 is one of many periodic statements issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA).
- Periodic Statements generally involve the modification of existing auditing standards or the introduction of new auditing standards.
- Internal Controls and Service Organizations have long been an area of focus.

ISACA San Francisco Chapter

Benefits to User Organizations

- SAS 70 reports have become common because they enable a Service Provider's customers to efficiently gain an understanding of the Service Provider's internal control environment.
- As part of its assessment of controls for Sarbanes-Oxley 404, management can obtain and evaluate a Service Provider's SAS 70 report and significantly reduce the need to test the controls in place at the Service Provider (and reduce costs associated with independently testing controls).
- In addition, the User Organization's external auditors (User Auditors) can use the report to gain an understanding of, and potentially place reliance on, testing of the internal controls at the Service Provider.
- Management should consider requesting a SAS 70 from third party Service Providers that provide substantial services directly impacting financial reporting controls or internal control activities.

ISACA San Francisco Chapter

Benefits to Service Organizations

- A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities.
- A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).
- A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.
- A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

ISACA San Francisco Chapter

Examples

- Application Service Providers (ASPs)
- Payroll Processing Companies
- Data Center Hosting Companies
- Claims Processing Companies
- Collections Companies
- Benefit Plan Providers

Report Overview

SAS 70 Reports – Type I

- Type I SAS 70 Report
- Fair presentation of a Service Provider's description of its controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements.
- Were controls suitably designed to achieve specified control objectives, and were they placed in operation as of a specific date?
- Only to be used to assist in obtaining an understanding of the controls at the Service Provider.
- Provides no information on whether internal controls are operating effectively.

SAS 70 Reports – Type II

- Type II SAS 70 Report
- Includes all aspects of a Type I report and reports on whether the controls had been operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.
- A Type II report is more useful to a Company's auditors for the following reasons:
  - Provides an understanding of controls necessary to plan the audit;
  - May provide reasonable assurance that control objectives important to the User Auditor have been met;
  - Reports on controls placed in operation and tests of operating effectiveness; and
  - Provides comfort that the controls that were tested were operating with sufficient effectiveness to meet control objectives.

SAS 70 Report Format and Content

- Report of Independent Service Auditors – Contains the Service Auditor's opinion letter and states whether the opinion is qualified or unqualified (also referred to as a "clean" opinion).
- Service Provider's Description of Controls – Prepared by the Service Provider and provides a narrative description of the processes and controls covered by the scope of the report.
- Information provided by the Service Auditor – Contains the Service Auditor's procedures and results (auditor's control tests and results).
- Other Information provided by the Service Organization – Contains additional information not covered by the Service Auditor's opinion, often disaster recovery/ business continuity planning information.

Report of Independent Service Auditors

- Written solely by independent Service Auditor ("letter" format addressed to Service Organization)
- Contains standard language for:
  - Specifying the scope of the SAS 70 review performed by the independent Service Auditor, including whether subservice organizations are included in the examination ("inclusive method") or excluded ("carve-out method");
  - Indicating if internal control examination procedures extended to assessing design only (Type I) or included tests of operating effectiveness (Type II); and
  - Concluding on the description, design and operating effectiveness of internal controls
    - Qualified Opinion: One or more control objectives were not achieved.
    - Unqualified Opinion: "Clean Report. All control objectives were achieved.

Service Organization's Description of Controls

- Written by the Service Provider (with input from Service Auditor)
- "Free Format" (not standardized)
- Typically includes wording to define purpose and scope of report
- Bulk of the section is for management to describe control environment and to define control objectives (may include process flows and control narratives)
- User Control Considerations (UCCs) are typically defined within this section and define control activities that the Service Organization would expect its User Organizations to have in place in addition to the Service Organization's controls defined within the report

ISACA San Francisco Chapter

Information Provided by the Service Auditor

- "Meat and Potatoes" of report
- Typically in a matrix format and identifies the following for each specified control objective:
  - Control Activities: All in-scope control activities that, together, achieve the control objective (if designed and operating effectively);
  - Test Procedures: Validation procedures performed by the Service Auditor to determine if the control activities had operated effectively throughout the SAS 70 audit period;
  - Test Results: Results of testing (usually either "No Exceptions Noted" or "Exceptions Noted"); and
  - Management Responses: May include management's responses to test exceptions

ISACA San Francisco Chapter

Other Information Provided by the Service Auditor

- No requirements
- May contain any additional information that the Service Organization would like to disclose to its User Organizations
- Other information may include:
  - The Service Organization's Disaster Recovery Plan
  - Other Certifications (PCI, HIPAA, etc.)

ISACA San Francisco Chapter

SAS 70 Report Types - Summary

Report Characteristics	Type I SAS 70	Type II SAS 70
1. Independent Service Auditors Opinion:	Included	Included
o Whether the Service Provider's description of controls presents fairly, in all material respects, the relevant aspects of the Service Provider's controls that had been placed in operation as of a specific date.	Included	Included
o Whether the controls were suitably designed to achieve specified control objectives.	Included	Included
o 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 period specified.	Not Included	Included
2. Service Organization's Description of Controls	Included	Included
3. Information provided by the Service Auditor (Service Auditors Testing, Results of Testing)	Optional	Included
4. Other Information provided by the Service Organization (Section 4)	Optional	Optional
5. Tests of operating effectiveness for a period of time (usual minimum is 6 months)	Not Included	Included

ISACA San Francisco Chapter

Performing a SAS 70 Audit – Key Considerations

ISACA San Francisco Chapter

Performing a SAS 70 Audit

- Key Control Analysis
- "Softer" COSO Components
- Determination of Nature, Timing, & Extent of Testing
- Reliance On Subservice Organizations
- Substantive Testing
- Handling Test Exceptions

ISACA San Francisco Chapter

Key Control Analysis

- Assess which controls are truly “key” to achieving the related control objectives.
- Where possible, include only key controls.
- Assess the types of controls that support the objective, for example: automated vs. manual, and preventative vs. detective.
- Vary the nature, timing, and extent of testing for non-key controls.

“Softer” COSO Components

- Ensure the service organization provides an adequate description of their controls in section II.
- Evaluate and test the softer COSO components (control environment, risk assessment, information and communication and monitoring) in the client's description of controls.

Determination of Nature, Timing, and Extent of Testing

- Take advantage of the opportunity to drive efficiencies in your testing approach by selecting the most appropriate extent of testing when employing sampling guidance.
- Allocate sufficient time to developing test plans and outlining the appropriate nature, timing, and extent of testing within the Key Control Analysis during the planning of the audit.
- Consider the completeness of populations

ISACA San Francisco Chapter

Determination of Nature, Timing, and Extent of Testing

- As risks associated with a control increase, the more persuasive the evidence needed about its operating effectiveness.
- Evidence is increasingly more persuasive along the following continuum
  - inquiry, observation, inspection/examination and reperformance
- Many less direct controls (such as entity level controls related to the control environment) may need only inquiry/observation evidence
- Testing at the low end of a sample size range with no exceptions usually provides sufficient evidence about the effectiveness of a control, even for many higher risk controls
  - But.....we may desire even more persuasive evidence for certain higher risk controls where we might test a larger sample (e.g., 45 or 60), but also with the expectation of no exceptions

ISACA San Francisco Chapter

Reliance on Subservice Organizations

- A service organization may use the services of another service organization, e.g., a claims processing service provider may use an independent ASP to host and manage IT functions for its key claims processing system.
- In this situation, the claims processing provider is the service organization and the ASP organization is considered the subservice organization.
- A service auditor engaged to examine the controls of a service organization may need to consider functions performed by the subservice organization and the effect of the subservice organization's controls on the service organization.
- A service organization's description of controls should include a description of the functions and nature of the processing performed by the subservice organization.

Reliance on Subservice Organizations

- When a subservice organization performs services for a service organization, there are two alternative methods of presenting the description of controls:
  - Carve-out method: The subservice organization's relevant control objectives and controls are excluded from the description and scope of the service auditor's engagement.
  - Inclusive method: The subservice organization's relevant controls are included in the description and in the scope of the engagement.
- If the service organization uses a subservice organization to perform processes which relate to the scope for the SAS 70 you're performing, and the carve-out method is employed, you should obtain a SAS 70 from the subservice organization when possible.
- In order to rely on the SAS 70 of the third party organization, service providers and their auditors should perform adequate procedures to gain comfort that the client can effectively achieve the user control considerations (UCCs).

Substantive Tests

- These substantive tests of details:
  - usually entail obtaining evidence as of a point in time
  - should generally be performed only after completing a corresponding test of controls
  - may provide indirect or corroborating evidence about the operating effectiveness of related controls

While testing attributes is not testing controls, exceptions found in attributes can be indicators that controls are not designed and/or operating effectively and should be evaluated as such.

ISACA San Francisco Chapter

Handling Test Exceptions

- When auditors encounter testing exceptions, they should:
  - First evaluate and understand the nature and cause of the exceptions, even if the rate of exception is considered tolerable.
  - Consider other types of evidence of the control's operation (i.e., there are several ways to evidence an "approval").
  - If the rate of exception in the sample is greater than the auditor planned to tolerate, consider whether the results are likely to be representative of the population and, if so, reject the test or, if not, expand the test (typically by at least doubling the original sample size).

ISACA San Francisco Chapter

Handling Test Exceptions

- Concluding on Control Objectives:
  - When determining if a control objective should be qualified, auditors should consider each objective on it's own – not reviewed in total or aggregate.
  - Without other supporting evidence or considerations, exceptions identified within a key control would presumably qualify the control objective. (Key controls, by definition, are significant to the control objective.)

Handling Test Exceptions

- Describing Tests of Operating Effectiveness and the Results of Such Tests:
- In describing the results of tests of operating effectiveness, the service auditor should include exceptions and other information that in the service auditor's judgment could be relevant to user auditors. When exceptions that could be relevant to user auditors are noted, the description also should include the following information:
  - The size of the sample, when sampling has been used;
  - The number of exceptions noted; and
  - The nature of the exceptions.

Using and Evaluating a SAS 70 Audit Report

Using a SAS 70 Report

- In evaluating whether a service auditor's report provides sufficient evidence about the effectiveness of internal control at the service organization, management and the engagement team should consider the following factors:
  - The time period covered by the tests of controls and its relation to period under audit and/or the date of management's assessment on the effectiveness of internal control over financial reporting;
  - The scope of the examination and applications covered, the controls tested, and the way in which tested controls relate to the company's controls;
  - The report identifies controls over the service organizations activities that support relevant financial statement assertions at the user organization;
  - The report includes both an evaluation of the design of controls and tests of operating effectiveness (i.e., a Type II report);
  - The results of those tests of controls and the service auditor's opinion on the operating effectiveness of the controls and whether each control objective was achieved;
  - Whether significant changes that have occurred at the service organization between the SAS 70 report date and the user organization's financial year-end date have been identified and addressed;
  - The impact that the results of tests of control have on the assessment of internal control over financial reporting; and
  - The service auditor's professional reputation and competency.

Using a SAS 70 Report

- Management should also consider whether there is sufficient evidence to support comfort from controls provided by a service auditor's report.
- Because the report may be intended to satisfy the needs of several different users, management should determine whether the specific tests of controls and results in the service auditor's report are relevant to financial statement assertions that are significant to the user organization's financial statements.
- For those tests of controls and results that are relevant, management should consider whether the nature, timing, and extent of such tests of controls and results provide appropriate evidence about the effectiveness of the control to support management's assessment.
- In evaluating these factors, management should also keep in mind that, for certain assumptions, the shorter the period covered by a specific test and the longer the time elapsed since the performance of the test, the less support for comfort from controls the test may provide.

Key Components to Evaluating SAS 70 Reports

- 1. Assess Scope of Report
- 2. Evaluate Opinion and Exceptions
- 3. Map User Control Considerations
- 4. Address Gap Period
- 5. Document Management's Assessment

Assess Scope of Report

- Management should outline all of the significant operations that the Service Provider performs to help evaluate sufficiency of the SAS 70 scope.
- Management should evaluate the report to ensure all significant areas are examined.
- If significant operations performed by the Service Provider are not included in the scope of the SAS 70 report, management must assess the impact to and determine whether additional procedures are required.
- Additional procedures may include engaging Corporate Audit or another risk management function to gain an understanding of and test key controls over significant operations not covered by the SAS 70 report.

Evaluate Opinion and Exceptions

- If the SAS 70 opinion is qualified on one or more control objectives, management should evaluate the impact of the qualification and assess whether mitigating controls exist within the user organization's internal control environment to reduce the likelihood that a material error at the Service Provider would not be detected.
- Although the Service Auditor may issue an unqualified opinion, exceptions in testing may still exist and have an impact on the user organization. It is the responsibility of management to consider the nature and extent of any exceptions in the SAS 70 report.
  - Evaluate the implications of the exceptions and determine whether the exceptions relate to a key control for User Organization; and
  - Consider the effect of any complementary controls at the User Organization that might mitigate the effect of the exception.

Map User Control Considerations

- Typically included in section II of the SAS 70 Report, UCCs are controls that the Service Provider expects the User Organization to have in place.
- Management should assess its actual controls against the UCCs identified by the Service Provider and identify any gaps.
- Management should evaluate and map the UCCs to key controls documented and tested to ensure the UCCs are adequately addressed by internal controls at the Company.

Address Gap Period

- Subsequent period of “as of” date for a Type I and “period end” date for a Type II and fiscal year end for user organization is considered “Gap Period”.
- Generally, Gap period should be less than six months.
- Management should determine if additional procedures are required based on Gap period.
- Management may consider obtaining a memo from the service provider to address the gap period.

Document Management's Assessment

- Management's assessment of the significance of the operations outsourced to Service Providers and its evaluation and reliance on a SAS 70 report from a Service Provider should be formally documented.
- Key data to include in the assessment of the significance of outsourced operations should include an inventory of the Service Provider relationships, the scope of services provided and the availability and scope of a SAS 70.
- Key considerations for evaluating a specific SAS 70 include scope assessment, understanding and mapping any UCC's to key controls within the Company, and evaluation of any exceptions in the SAS 70 report related to key controls management relies upon, whether the exceptions resulted in a qualified opinion or not.

Transitioning to SSAE 16 and ISAE 3402

Transitioning to SSAE 16 and ISAE 3402

- History & background
- New standards over service organization reporting
- Perspective on overall impact on service organizations

The Need for Change

- SAS No. 70 was originally written in early 1990s and was effective for service organization audits after March 31, 1993
- Many business events have altered the landscape since the issuance of SAS No. 70
  - Increased outsourcing including usage of shared service centers
  - Continued globalization and global processing models
  - Increased regulation and enhanced risk management requiring service organization customers to obtain controls comfort related to outsourced activities impacting their financial statements, regulatory requirements and overall business risk management

The Need for Change

- SAS No. 70 has served as the de facto standard on reporting on controls at a service organization on a global basis
- Other territories have steadily sought to adopt their own service organization audit standard (e.g., Canada – Section 5970, UK – Audit and Assurance Faculty Standard (AAF))
- Absence of a global standard(s) complicates engagements that cross borders
- Potential to take advantage of differing provisions within various third party control standards

New International and US Standards

International Auditing and Assurance Standards Board (IAASB)

- Commenced a project in 2006 to develop an international standard for reports on controls at a service organization
- The proposed International Standard on Assurance Engagements (ISAE) 3402 is entitled, "Assurance Reports on Controls at a Service Organization"
- The proposed standard complements International Standards on Auditing (ISA) 402, "Audit Considerations Relating to Entities Using Service Organizations"

New International and US Standards

The Auditing Standards Board (ASB)

- Resurrected the AICPA SAS70 Task Force in 2007 to develop a successor set of standards to AU 324 (SAS No. 70)
- One proposed standard will be a Statement on Standards for Attestation Engagements (SSAE) (i.e., attest standard), "Reporting on Controls at a Service Organization"
- Second proposed standard complements the proposed Statement on Auditing Standards (SAS) (i.e., auditing standard), "Auditing Considerations Relating to an Entity Using a Service Organization"

ISACA San Francisco Chapter

Comparing SAS70 and SSAE16

Similarities	Differences
• Scope is focused on controls that are likely to be relevant to user entities' internal control over financial reporting • Type 1 and Type 2 reports may be issued by the service auditor • Inclusive and carve-out methods may be used in cases of subservice organizations • Service organization's description of controls under SAS 70 generally will provide a basis for the system description under SSAE 16 • Service auditor's report is restricted to service organization management, user entities of the service organization and the independent auditors of the user entities	• New standard is an attest standard, not an audit standard; a separate audit standard will be issued to address the requirements of the user auditor • Management's written assertion • Subservice organizations are required to provide a similar assertion when the inclusive method is used • In a Type 2 report, the service auditor opines on suitability of the design of controls related to the control objectives throughout the entire period • Service auditor is required to disclose any use of the work of Internal Audit (or other management testing functions) within the report • Format of service auditor's opinion will change

ISACA San Francisco Chapter

Differences between ISAE 3402 and SSAE 16

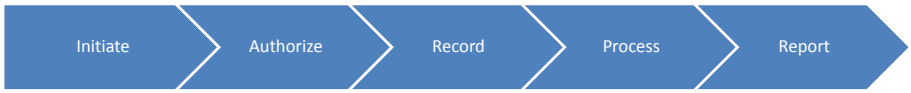
- Significant differences – none
- Minor differences:
  - Intentional acts
  - Use of internal Audit (IA)
  - Subsequent events
  - Statement on restricted use of the report

Management's Assertion

- Management is required to provide a written assertion stating that the controls are fairly presented, suitably designed and (in the case of a Type 2 report) operating effectively to achieve the specified control objectives.
  - Included in, or attached to, management's description of the system and documented within the report
  - Based on suitable criteria selected by management and stated within the assertion
  - Must have a reasonable basis for its assertion
  - Subservice organization must also provide a written assertion when using the inclusive method
  - A service auditor is precluded from issuing a report if management does not provide a complete written assertion

Management's Description of the System

- Management is responsible for preparing its description of the service organization's system
  - Policies and procedures designed, implemented, and documented by management to provide customers with the services covered by the service auditor's report.
  - Where applicable, should include: services covered, period covered, control objectives and related controls, complementary user controls, controls operated by the subservice organization(s), description of the classes of transactions processed, the process used to prepare reports provided to customers, and other aspects of the COSO internal control framework relevant to user entities
  - Generally consistent with the elements included in existing SAS 70 reports
  - Includes any relevant changes during the period covered by the report



Risk Factors

- Management's description of the system should specify control objectives and related controls
- In specifying control objectives and controls, management should identify the risks that threaten such control objectives
- A risk assessment process should be performed by management
  - At a minimum, the relevant risks should be considered through thoughtful identification of the control objectives when designing, implementing, and documenting the service organization's system
  - No requirement to explicitly include the relevant risks within the report

Communication Plan

- Service organizations should establish an effective plan for communication of the new standards and education of relevant parties, including:
  - Program offices
  - Customer service / contract teams
  - Sales teams
  - Customers
  - Subservice organizations
- Re-visit and assess the impact on customer and/or subservice contracts

ISACA San Francisco Chapter

Adoption

- Standards are effective for report periods ending on or after June 15, 2011.
  - For example, a twelve-month report period beginning July 1, 2010
  - Early adoption is permitted; however, companies should assess benefits and feasibility.
  - We do not anticipate that many companies will early adopt the new standard
  - Opportunities for single report – SSAE 16 and ISAE 3402
  - Reports issued in the US must be performed under SSAE 16 standard, at a minimum

ISACA San Francisco Chapter

Questions?

Appendix A - Common SAS70 Terminology

Common SAS 70 Terminology

- Service Organization/Service Provider: The entity (or segment of an entity) that provides services to the user organization.
- User Organization: The entity that has engaged a Service Provider and whose financial statements are being audited.
- Service Auditor: The independent auditor firm performing the SAS 70 audit services.
- User Auditor: The auditor who reports on the financial statements of the user organization.
- Service Auditor's Report: The report issued by the service auditor expressing an opinion on whether the Service Provider's internal controls are designed and operating effectively as of a specific date.

Common SAS 70 Terminology

- User Control Considerations (UCC): Controls the Service Provider expects User Organizations to be performing. It is the responsibility of the User Organization to design and implement these controls.
- Coverage Period: Applies to a Type II SAS 70 and refers to the period of time that the control objectives and related control activities were in place and tested for operational effectiveness (i.e., 10/1/05 to 9/30/06). Tests of controls are performed on a sample selected from the coverage period.
- Gap Period: The difference in the "as of" or "period end" date in the SAS 70 Report and the year end date of the User Organization financial statements. For example, if a SAS 70 Report's "as of" or "period end" date were 9/30, based on the User Organization's fiscal year end date of 12/31, the Gap Period, or period not covered by the SAS 70 Report is three months.

Common SAS 70 Terminology

- Risk Assessment: Risk assessment by company management includes: The establishment of objectives at different levels; identification and analysis of relevant risks to achievement of the objectives; forming a basis for determining how the risks should be managed; and building the mechanisms to identify and manage the specific risks.
- Control Activities: The policies, procedures and practices that are put into place to ensure that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified
- Information and Communication: Pertinent information that must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities.

Common SAS 70 Terminology

- Control Environment: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all the other components of internal control, providing discipline and structure.
- Monitoring: Assessment by appropriate personnel of the design and operation of controls on a suitably timely basis, and the taking of necessary actions (i.e., effectiveness).
- Control Deficiency: Control deficiencies fall into one of two categories:
  - Design Deficiency: necessary control is missing or existing control is not designed properly
  - Operating Deficiency: properly designed control either is not operating as designed or person performing the control does not possess necessary authority / qualifications to perform the control effectively.