

**WOLF & COMPANY, P.C.**  
Certified Public Accountants  
and Business Consultants  
*Insight and Integrity*

**SAS No. 70 Review:  
Identifying weaknesses &  
implementing best practices**  
©2010 Wolf & Company, P.C.

Victoria A. Hayes, CISA  
February 9, 2010

Boston • Springfield • Albany

---

---

---

---

---

---

---

---

**About Wolf & Company, P.C.**

- Established in 1911
- Provides Audit, Tax, and Risk Management services
- Over 170 employees
- 3 Offices: Boston and Springfield, MA, and Albany, NY
- Named one of the "Area's Largest IT Consulting Firms" by Boston Business Journal 2007, 2008, 2009

*As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and outstanding service.*

**WOLF & COMPANY, P.C.**  
Certified Public Accountants  
and Business Consultants  
*Insight and Integrity*

**WolfPAC**  
WOLF & COMPANY, P.C.

---

---

---

---

---

---

---

---

**Welcome!**

**Vicki Hayes**  
• Certified Information Systems Auditor  
• IT Assurance Senior Manager

**Wolf's IT Assurance group provides:**

IT Audit	Business Continuity Planning (BCP)
Information Privacy Review (GLBA, HIPAA, State Laws)	Incident Response Planning (IRP)
Application Security Review	Policy & Procedure Development
Network Vulnerability Assessments	Internal IT Audit Support (SOX 404)
Internet Intrusion Testing	SAS 70 & Systrust Assurance
Wardialing	
Social Engineering Assessment	

*Wolf's IT Assurance professionals have detailed knowledge of business operations and technologies.*

**WOLF & COMPANY, P.C.**  
Certified Public Accountants  
and Business Consultants  
*Insight and Integrity*

**BEST OF 2009**  
BANKER & TRADERSMAN  
**GOLD**

**WolfPAC**  
WOLF & COMPANY, P.C.

---

---

---


---

---

---



---

---



### Objectives

- Applicability of a SAS No. 70 report
- Review of the SAS No. 70 report
- SAS No. 70 Future



---

---

---


---

---

---



---

---



### What is a SAS No. 70?

- Widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
- Allows service organizations to disclose control activities and processes to its user organizations and their auditors in a uniform reporting format.
- In an audit of a user organization, the user auditor obtains an understanding of the entity's internal control sufficient to plan the financial statements audit.



---

---

---


---

---

---



---

---



### SAS No. 70 Benefits for a Service Organization

- Service organizations would have to entertain multiple audit requests from its users and their respective auditors.
- A Service Auditor's Report with an unqualified opinion 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 service organizations build trust with its users.
- The SAS No. 70 process results in the identification of opportunities for improvements in many operational areas.
- A SAS No. 70 provides a greater opportunity of retaining clients and attracting new ones.



---

---

---

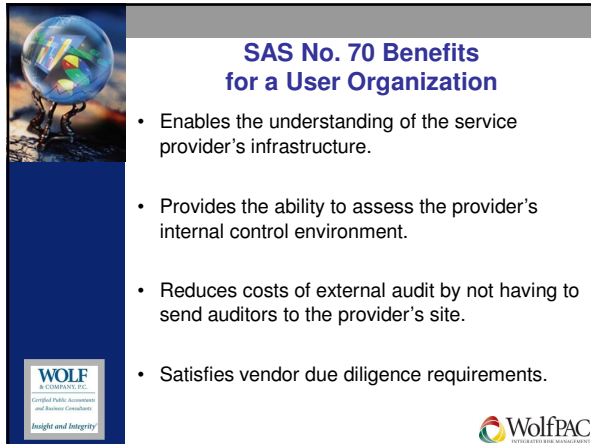
---

---

---

---

---



**SAS No. 70 Benefits  
for a User Organization**

- Enables the understanding of the service provider's infrastructure.
- Provides the ability to assess the provider's internal control environment.
- Reduces costs of external audit by not having to send auditors to the provider's site.
- Satisfies vendor due diligence requirements.

**WOLF & COMPANY, P.C.**  
Certified Public Accountants  
and Business Consultants  
*Insight and Integrity*

**WolfPAC**  
WOLF & COMPANY, P.C. A MEMBER OF THE WOLF GROUP

---

---

---


---

---

---

---

---



**SAS No. 70 Scope**

Services and Systems

**Core Data Processing**

**Payroll**

**Investment Services**

**Insurance Claims Processors**

and Non-financial Services

**Firewall and Technology Outsourcing**

**WOLF & COMPANY, P.C.**  
Certified Public Accountants  
and Business Consultants  
*Insight and Integrity*

**WolfPAC**  
WOLF & COMPANY, P.C. A MEMBER OF THE WOLF GROUP

---

---

---

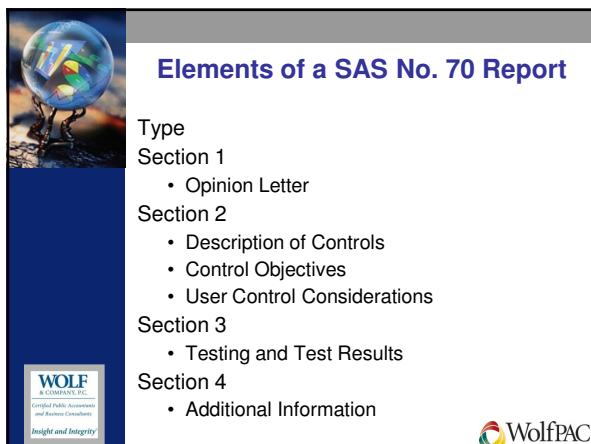
---

---

---

---

---



**Elements of a SAS No. 70 Report**

Type

Section 1

- Opinion Letter

Section 2

- Description of Controls
- Control Objectives
- User Control Considerations

Section 3

- Testing and Test Results

Section 4

- Additional Information

**WOLF & COMPANY, P.C.**  
Certified Public Accountants  
and Business Consultants  
*Insight and Integrity*

**WolfPAC**  
WOLF & COMPANY, P.C. A MEMBER OF THE WOLF GROUP

---

---

---


---

---

---

---

---





### Type I vs. Type II

**Type I**

- Report on controls placed in operation  
"walkthrough at a point in time"

**Type II**

- Report on controls placed in operation and operating effectiveness  
"sample testing over a period of time"


---

---

---


---

---

---



---

---



### Type I vs. Type II

Section Contents	Type I Report	Type II Report
1. Independent Service Auditor's Report	Included	Included
2. Service organization's description of controls	Included	Included
3. Information provided by the independent service auditor	Optional	Included
4. Other information provided by the service organization	Optional	Optional


---

---

---


---

---

---



---

---



### Section 1: The Opinion Letter

Section Contents	Type I Report	Type II Report
1. Placed in operation as of a specific date and...	Included	Included
2. Suitably designed to achieve the specified control objectives	Included	Included
3. Operating with sufficient effectiveness during the period specified	Not Included	Included


---

---

---


---

---

---



---

---



**Section 1:  
The Opinion Letter**

- Identifies systems/processes tested
- Defines period of coverage of the systems/processes tested
- Concludes whether documented controls satisfy the control objectives
- Identifies exceptions to testing of the documented controls (Type II)



---

---

---


---

---

---



---

---



**Section 2:  
Description of Controls**

- An overview of operations
- Relevant aspects of:
  - Control Environment
  - Risk Assessment
  - Monitoring
  - Information Systems
  - Communication
- Control objectives and related controls
- User control considerations



---

---

---


---

---

---



---

---



**General Control Objectives**

- Organizational Structure
- Physical Access / Environmental Controls
- Logical Access
- System Maintenance
- Backup and Recovery



---

---

---


---

---

---



---

---



### Sample Control Objectives

- Controls provide reasonable assurance that the organizational structure **adequately supports** critical functions, **segregates** incompatible duties, and **provide appropriate ownership and supervision** of key technologies and business processes.
- Controls provide reasonable assurance that physical access to the processing center and other sensitive areas is **restricted** to authorized personnel.
- Controls provide reasonable assurance that critical processing equipment is **protected** from external or environmental hazards.
- Controls provide reasonable assurance that **only authorized** users with a legitimate business need can access the statement processing applications and databases surrounding them.
- Controls provide reasonable assurance that changes to systems are **authorized, tested, approved, implemented and documented**.



---

---

---


---

---

---

---

---





### Section 3: Information Provided by the Auditor

#### Types of tests

- Inquiry
- Observation
- Inspection
- Re-performance

Testing of operating effectiveness



---

---

---


---

---

---

---



---



### Section 4: Information Provided by the Service Organization

Information the service organization would like to communicate

- Detail behind remediation exceptions
- New products or expanded services



---

---

---


---

---

---

---



---



### Reviewing the SAS No. 70 Report

#### Section 1 - The Opinion Letter

- Services and Systems – Make sure that the service or system you need controls on is listed. The service/system, location, and scope are in the first paragraph
- Date(s) of Testing – Ensure that you are comfortable with the dates that the controls are tested for. Note Type I or Type II
- Deficiencies – A qualified opinion has words in the opinion paragraphs that say "...in our opinion, except for the matter described in the preceding paragraph..."



---

---

---


---

---

---

---



---



### Reviewing the SAS No. 70 Report

#### Section 2 - The Description of Controls

- **Narrative Description** – This includes a description of the entire control environment, including the risk assessment process, monitoring, information systems descriptions, and communication within and outside the service organization.
- **Control Objectives and Related Controls** – Many times these are deferred to Section 3.
- **User Control Considerations** – The service organization relies on some controls that you put in place. This may be a secondary audit or review.



---

---

---


---

---

---

---



---



### Reviewing the SAS No. 70 Report

#### Section 3 – Testing (in a Type II only)

- Testing is the section that the independent auditors are responsible for.
- Test records are organized by control objectives. Control activities should completely support the control objective.
- Testing will include the control activity, test or tests to validate the control activity, and a result (many times, "No relevant exception noted").



---

---

---


---

---

---

---



---



### Reviewing the SAS No. 70 Report

**Section 4 – Other Information from Organization (Optional)**

- This section provides other pertinent information that the service organization feels you may need to know.
- Inclusions may be management responses to opinion qualifications, other process factors of importance (ie. Disaster recovery), other services offered, or other initiatives that are being pursued.
- This section **IS NOT AUDITED** by the firm performing the SAS No. 70 review of controls. There is no opinion on this section.



---

---

---


---

---

---

---

---





### Other Assurance Reports

**SysTrust**

- Tests and reports on the effectiveness of controls over system reliability
- Uses standard principles and criteria for all engagements
- Addresses controls over system security, availability, confidentiality, and processing integrity

**WebTrust**

- Reports on management's assertion about a Web site
- Addresses controls over online privacy and certification authorities



---

---

---


---

---

---



---

---



### Future of the SAS No. 70

- Change from SAS 70 to SSAE
- Changes to SEC Custody Rule
- Consolidation of Service Organizations
- Cloud Computing
- SOX 404



---

---

---


---

---

---



---

---



### Future of the SAS No. 70

The International Auditing and Assurance Standards Board (IAASB) and the Auditing Standards Board (ASB) in the United States have undertaken to develop new standard.



---

---

---


---

---

---



---

---



### ISAE 3402 and SSAE

- Effective for reporting periods ending on or after June 15, 2011.
- Management will be required to provide an assertion regarding the fairness of presentation of controls, their suitability of design and the effectiveness of their operations.
- In Type II; all three assertions/opinions (description, design, and operating effectiveness) will have to be for a period of time.
- Report can be extended beyond financial reporting.



---

---

---


---

---

---

---



---



### Thank You / Questions

Victoria A. Hayes, CISA  
IT Assurance Senior Manager  
Phone: 617-428-5458  
Email: [vhayes@wolfandco.com](mailto:vhayes@wolfandco.com)

**Handouts & Recording Available:**  
[www.wolfpacsolutions.com/webinars/2010](http://www.wolfpacsolutions.com/webinars/2010)



---

---

---

---

---

---

---

---





**Upcoming Webinar Topics**

ACH  
Role of Technology in Audit  
GLBA  
Cloud Computing

To inquire about our upcoming webinars, or to suggest future topics, contact:

Melissa Goodwin  
Marketing Specialist  
Phone: (617) 261-8167  
Email: [mgoodwin@wolfandco.com](mailto:mgoodwin@wolfandco.com)



---

---

---

---

---

---

---

---