

Control Essentials

Volume II, Issue VII

July 2007

Business Consulting

- Regulatory Support
 - Policies and Procedures
 - Regulatory Compliance
 - Sarbanes-Oxley
 - GLBA
 - HIPAA
 - BSA
 - PCI (Payment Card Industry) Security Audit
 - Information System Audit Outsourcing
- Enterprise Support
 - Business Continuity Planning
 - Attestation and Assurance
 - SAS-70
 - E - Discovery
 - Forensic Examinations
 - Security Remediation

Technology Consulting

- Application Security
 - Application Security Assessment
 - Application Penetration Test
 - Web Application Security Assessment
 - Web Application Penetration Test
- Network Security
 - Risk Assessment
 - Vulnerability Assessment
 - Penetration Testing
 - Internal
 - External
 - Social Engineering
 - War Dialing
 - War Driving
 - Blue Snarfing
 - Wireless Security Assessment
 - Information System Security Audit
 - Information System Control Audit
 - Network Architecture Design and Assessment
 - Physical Security Assessment
 - Log Analysis

SAS 70 Reports - What do they really tell you?

Many organizations outsource some type of information system operations to third party providers. While using the services of third party providers can offer a cost-effective alternative to obtain necessary expertise and to expand products and services, it also introduces additional risks. The risks range from having inaccurate information which could affect financial statements to serious security breaches.

It is critical that the company providing the outsourcing services have reliable controls. Organizations that outsource part of their information system operations often rely on "SAS 70" (Statement of Auditing Standards No. 70) reports to determine if the third party providers have adequate controls.

Currently, there are serious limitations in the way SAS 70 reports are being performed and used. This article examines how SAS 70 reports can be improved, and how businesses can use them more effectively.

SAS 70 reports

SAS 70 reports are provided by independent Certified Public Accountants (CPA's). SAS 70 is one of the auditing standards promulgated by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). CPAs who perform SAS 70 reviews follow the specifications of the AICPA guide "Service Organizations: Applying SAS No. 70, as Amended".

There are two types of SAS 70 reports:

- A *Type I* report provides the independent CPA's opinion of the third party provider's control structure and a description of the implemented information systems controls.
- A *Type II* report contains the same information as a "Type I" report, plus the results of testing performed by the independent CPA to validate the existence, adequacy and effectiveness of the reported controls.

The use of SAS 70 reports

Because many of the functions performed by third party providers affect user organizations' financial statements, auditors performing audits of financial statements need to obtain information about the services and controls of third party providers. Such information about third party providers is usually obtained through SAS 70 reports.

When auditors are working with publicly traded companies, their work is guided not only by the AICPA's standards, but also by standards issued by the Public Company Accounting Oversight Board (PCAOB). In May of 2007, the PCAOB issued auditing standard no. 5 which addresses audits of internal controls (and replaces standard no. 2 on this subject). Thus, when dealing with public companies, audits of internal controls need to be consistent with both the AICPA's SAS 70 and the PCAOB's auditing standard no. 5.

Although SAS 70 reports were originally intended to be used by auditors while evaluating controls that affect the reliability of financial statements, in recent years many organizations have been using the SAS 70 reports to evaluate whether their third party providers have sufficient information system controls such as security access controls to address regulatory requirements. Thus, the use and reliance on SAS 70 reports continues to grow.

Recent concerns about SAS 70 reports

Limits of Type I reports. There is a need for better understanding of the limits of different types of SAS 70 reports. Companies seeking information about their third party provider's controls need to be aware of the differences between a Type I and Type II report. SAS 70 Type I reports provide only a generalized overview of the third party provider's information system control structure. A company may request a SAS 70 report and wind up receiving a Type I report from their outsourcer which does not validate the stated control objectives through testing.

Limits of Type II reports. SAS 70 Type II reports about a service organization are often insufficient to meet the needs of the company that is receiving the outsourcing services. When a Type II SAS 70 review is conducted, certain control objectives are selected, and then testing is conducted with respect to the selected objectives. However, often the selected control objectives do not address all the essential areas necessary to provide reasonable assurance regarding critical information system controls.

Furthermore, in many SAS 70 Type II reports that appear to have addressed adequate control objectives, the level and extent of testing per control objective may not be enough to provide a reliable opinion of the status of essential information system controls. For instance, a common control objective of a third party that provides data processing services to small and medium size banks would typically state that information security mechanisms restrict system users to only the data files and application functions they are authorized to use. There are a number of ways to test this control objective. It would be insufficient to test this control objective by superficial tests related to the adequacy of password controls. However, SAS 70 reports have been issued with such limited testing. This is a critical control objective that relates to the reliability and integrity of financial and customer data. Proper testing of this control objective requires many more critical security controls in addition to basic password controls. A SAS 70 attestation report based on inadequate testing may give a false sense of controls to a recipient that is relying on the CPA's conclusions.

Limits of SAS 70 reports with respect to regulatory requirements.

There are increased regulatory requirements with respect to internal controls, including controls relating to information systems and security. Businesses have turned to SAS 70 reports to provide some assurances about internal controls. However, some regulatory requirements call for testing of a greater scope and depth than what is usually provided by SAS 70 reports.

Limited CPA training and experience. Currently, most CPAs have not been formally trained to deal with complex automated system infrastructures and their related technical controls. This is one of the reasons why some SAS 70 reviews lack the proper coverage and testing of key information systems controls like security access controls that are directly related to the reliability and integrity of financial statements.

Limited guidance and oversight. While the AICPA and the PCAOB have worked to provide auditing standards and guidance, this particular area continues to present a challenge to auditors and to the businesses that rely on the auditors. The lack of detailed guidance is one of the reasons SAS 70 reviews sometimes lack adequate testing of critical information systems controls. More detailed guidance and increased oversight would be beneficial, especially with respect to the internal controls that relate to information systems.

Organizations must evaluate the adequacy of SAS 70 reports

Organizations that outsource information system operations need to ensure that they receive SAS 70 reports that address essential control areas and provide adequate testing coverage of all relevant information system and security control aspects related to the function being outsourced. In order to accomplish this objective, outsourcers should consider the following:

- **The CPA.** Consider whether the SAS 70 was performed by professionals with integrity and the appropriate skills. CPAs providing SAS 70 reports need to have skills beyond general accounting knowledge. CPAs performing SAS 70 audits should also have skills and experience with respect to information systems and security.
- **The type of SAS 70 report.** Ensure that you have a Type II SAS 70 to ensure testing of key control areas and evaluate the type of SAS 70 opinion provided.



- **The controls selected for testing.** Evaluate if the control objectives covered by the SAS 70 properly address the needs of your business as well as the requirements of relevant laws and regulations. Ensure that the following areas of controls are covered, if they are applicable to your organization:

Application Systems
<ul style="list-style-type: none"> • System Development, Implementation and Maintenance • Application Documentation • Quality Assurance

Transactions
<ul style="list-style-type: none"> • Recording • Data Transmission • Reporting • Calculations

Security
<ul style="list-style-type: none"> • Logical Security • Physical Security • Environmental Controls • Operational Recovery • Segregation of Duties

Computer Operations
<ul style="list-style-type: none"> • System Processing • Operations Support

- **Scope and level of testing.** Evaluate the scope and level of testing to ensure it is adequate. Ensure that all relevant areas of key controls for your business are properly addressed by the SAS 70. Also, ensure that the level of testing for each control area is sufficiently detailed to support the overall opinion provided in the report. It is essential that the organization assigns a person with a strong technical, information systems control and security background to perform the evaluation of the testing performed. If the organization does not have the personnel with the skill sets to perform this review, consider using an outside consultant with the necessary background for this evaluation.
- **Sub-contractors.** If the third party provider also uses the services of other sub-service organizations that affect your business, ensure the SAS 70 covers key control aspects of the sub-service organizations.
- **Date of report.** Ensure the reporting period of the SAS 70 is current. There is a consensus that reports should not be more than one year old. Also, there is a concern that reports with respect to internal controls should cover the same time period as the financial statements.

Additional considerations

- **Other types of security testing.** Consider asking your third party provider for reports involving additional testing such as vulnerability assessments and penetration tests (“ethical hacking”).
- **Legal contracts.** Ensure that legal contracts with third party providers indicate the types and scope of audits and technical reviews that you require (e.g., SAS 70 Type II, vulnerability assessments, ethical hacking tests, etc.). The contracts should also state the frequency of the required reports. The contract must also indicate that the organization reserves the right to perform its own audits or technical reviews, if the organization is not satisfied with the audits provided by the third party.

Conclusion

Organizations that outsource some type of information system operations to third party providers need to manage the risks that outsourcing creates. These organizations usually rely on SAS 70 reports to determine if their third party providers’ internal controls are adequate to manage their risks.

It is imperative that organizations take a closer look at their SAS 70 reports in an effort to identify those reports that are not providing sufficient assurance about the effectiveness of information systems controls that are relevant to the organization’s operations and financial statements. They also must demand SAS 70 reports with more detailed testing of key information system controls when their evaluations indicate current SAS 70 reports are not providing a sufficient basis to properly evaluate the effectiveness of controls.

Additionally, CPAs performing and/or evaluating SAS 70 reviews should have formal information systems training and knowledge in addition to their accounting background. Finally, professional bodies such as the AICPA and PCAOB also need to provide more guidance and oversight to CPA’s who perform information system control evaluations and SAS 70 reviews.

In recent years, regulators, businesses, investors, and consumers have come to realize how important internal controls are. They are key to the accuracy of financial statements. Also, the reliability and security of businesses often depend on the effectiveness of internal controls. SAS 70 reports that evaluate these controls can be a helpful tool, but only if SAS 70 reports are properly performed and properly understood.



Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania
Syracuse University, Syracuse, New York
Xavier University, Cincinnati, Ohio
University of Miami, Miami, Florida
Florida International University, Miami, Florida

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.
Demotte Consulting, Ltd.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
CitiBank
Carnival Cruise Lines
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

We encourage you to visit our website, www.emrisk.com, for details on ERM's services, team profile, clientele and testimonials from some of our clients.

For further information, please contact an ERM consultant at (305) 447-6750.