

SAS 70: The Emperor Has No Clothes

Executive Insight Series

Jonathan G. Gossels

Introduction

As organizations search for a reliable benchmark by which to measure potential business partners and to distinguish their own services, SAS 70 is often mentioned. Unfortunately, security professionals are in nearly unanimous agreement that SAS 70 is neither a meaningful security metric nor worth the high cost of obtaining the SAS opinion.

This brief paper presents the key facts so you can make an informed decision about SAS 70 for yourself.

What is SAS 70?

The Statement of Auditing Standards (SAS) number 70, Service Organizations, is an auditing standard developed by the American Institute of Certified Public Accountants. Its purpose is to enable an auditor to evaluate and issue an opinion on the controls that a service organization has in place. The output, the Service Auditor's Report, contains the auditor's opinion, a description of the controls in place, and if it is a Type II report, a description of the auditor's tests of control effectiveness. A SAS 70 Type I analysis does not include testing.

What's the problem?

So far, it sounds great. What is the problem? There are three fundamental problems. Taken individually, each would call into question the validity of the opinion. Taken together, it explains why a SAS 70 opinion is held in such low regard.

No Objective Standard

SAS 70 is not a predetermined set of standards that an organization must satisfy in order to "pass" the audit. In a SAS 70 audit, the service organization is responsible for describing its control objectives and control activities that might be of interest to auditors in user organizations.

If an organization does not have a security policy covering a particular area, or has one that allows ineffective security (for example, an organization may not have a policy that prevents the deployment of production servers with default configurations and default passwords), the SAS 70 audit report would contain a favorable opinion because the control activities (none) matched the stated control objectives (none).

SystemExperts has seen examples of this time and again. On beginning a security review of a service organization that has been mandated by a prospective customer of its service, the service organization hands us a SAS 70 report that cost them \$150,000 to have done. Naturally, it has a favorable auditor's opinion. In every case, within ten minutes, we've found fundamental security flaws in the system that would have put customer private and business proprietary information at risk.

Only CPA Firms, Not Technology Experts Can Perform a SAS 70 Audit

Most people don't go to their auto mechanic for their yearly physical. Both provide important services but they are not substitutes for each other.

Properly securing today's interconnected IT infrastructures requires highly specialized skills. It is important to get both the big picture, the overall architecture, as well as the details, exactly right. Equally important is to assess what you *don't see*; potential vulnerabilities that are not covered by existing controls. The very skills and temperaments that make CPAs and auditors successful in their regular

activities work against them in playing a security role. It may be an unfair generalization, but it is not stretching to say that, as a whole, CPAs and auditors are not “out-of-the-box” thinkers. Hackers are. Your security consultants need to be as well.

The SAS 70 Audit Process is Designed to Drive Billable Hours

The SAS 70 process is transparent in its aim to create billable hours for the SAS 70 auditors. Typical SAS 70 costs range from \$100,000 to \$300,000. You may wonder why it is so expensive since the service organization provides the control objectives and control activities as inputs to the process.

Many SAS 70 audits cost even more. If an organization does not have suitable documentation of its control objectives or control activities, the actual SAS 70 audit is preceded by a period of billable consulting time during which the accounting firm works with the client to prepare the required documents.

If you find yourself in this situation, the best course of action is to *stop right there* and reassess the situation. Lack of written control objectives and control activities is a classic symptom of an underlying problem, control is not an integral part of day-to-day operations. Most organizations would be better off spending money to address the control deficiencies,

rather than spending it on documenting the fact the control objectives or control activities are deficient.

Buried in the SAS 70 details are requirements that drive up the costs and provide no benefit to the client. For example, to obtain a Type II report, detailed testing of the controls must be performed for a minimum of six months. Most organizations change something significant in the IT infrastructure over a six month period so the testing often needs to be repeated. In contrast, a thorough security review costs a fraction of that total and is usually completed in a month or two.

Don't be Afraid to Ask, “Why?”

If you are a service provider and a customer or potential customer asks you to have a SAS 70 audit performed, talk with them so you understand their concerns. Then, work with them to structure an objective assessment of your environment that will address those concerns. More than likely you will find yourself working with a security firm on a well bounded project that actually meets your business needs, not a SAS 70 audit.

For a fraction of the cost of a SAS 70 audit, most organizations can have their security thoroughly reviewed and documented in a way that is suit-

able for sharing with customers and business partners. Typically, such reviews consist of a design review to assess the overall architecture, inspection of key system configurations, penetration testing, evaluation of incident detection and response capability, and a code review of critical applications or modules.

If your organization is evaluating a service provider, SAS 70 is the wrong thing to ask for. You should be looking for proof that the security of the services provider meets or exceeds *best industry practice*. Naturally, those practices vary by industry. Find a reputable security consulting firm with a successful track record in your industry.

ISO 17799

Consumers of information services have recently become interested in ISO 17799. This standard provides the objective security standards so lacking in SAS 70. While certification with ISO 17799 in a formal way, suffers from many of the same economic drawbacks as SAS 70, many organizations will benefit substantially from the audit preparation process described in the standard.

Resources

American Institute of Certified Public Accountants (AICPA)

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Network-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

Intrusion Detection and Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento

www.SystemExperts.com

info@SystemExperts.com