

# Canaudit Perspective

---

January 2005  
Volume 6, Issue 1

## Topics of Interest:

- Auditing for Profit
- Automating Auditing for Profit
- Information Security: An Example of SOX Audit Casualties



## Auditing after SOX

Written by: Gordon Smith  
President, CEO  
Canaudit, Inc.

Sarbanes-Oxley Act (SOX) was the big event of the last year. Audit departments and external audit firms were scampering to complete the required work by the deadline. Business processes were being documented and analyzed. Control issues were documented. Timely remediation of the issues, followed by further testing, ensured that many organizations were able to comply with SOX without the dreaded disclosure of serious control weaknesses. A monumental effort was required to ensure SOX compliance. Auditors had to be diverted from other tasks, and the audit plan had to be curtailed so that the SOX objectives could be met. Now, many of us can see the light at the end of the tunnel. Now, we can begin to look beyond SOX from an Internal Audit standpoint.

Let us start with analyzing the impact of SOX. For this article I want to address two topics. The first is what I like to call *Auditing for Profit* - a method of utilizing the information we have to enhance profits. The second topic is the impact of deferring some critical audits or limiting the testing performed during the SOX review process. This is particularly obvious in the areas of information security.

### Auditing for Profit

Over 15 years ago, I put together my first *Auditing for Profit* seminar. It was one of the most successful courses our company offered, as it provided a proven methodology for enhancing profits while improving control. This course ran its lifecycle and was retired. After looking at the wealth of business process information now available to us because of the SOX effort, I have redesigned this seminar from the ground up. My new premise is to use the SOX documentation to identify unneeded or inefficient processes. It is obvious to me that we documented many inefficiencies and labor-intensive processes. Now is the time to analyze these processes, determine the cost of the inefficiencies, identify short-term improvements with low implementation costs, and create an audit report that presents these to management on a business process by business process basis.

My first target in *Auditing for Profit* is labor inefficiencies. I ask two questions to assist me in identifying the value added by a business process. The first is, "Why are we doing what we are now doing?" The second is, "What value does this add to the corporation?" If these can be identified and categorized using the existing SOX documentation, then we achieved additional benefits from the SOX process. This turns the SOX process from a necessary but expensive overhead item into a valuable business resource. Another technique I use is to gather the staff auditors into a group, and then ask them to identify the 10 most wasteful processes in the company. The auditors are then given 24 hours to think about waste in the organization. They then come back together with their ideas. I like to offer prizes for the best ideas. Be prepared to award the prize to more than one person, as several people often have the same truly brilliant idea.

It does not take very long to set up this process. Bring the auditors together, and then use an example, such as ineffective meetings. Ineffective meetings are something everyone can identify with and it serves to introduce the process. As we all know, the cost of meetings is very high. Many people who attend meetings do not want to be there, but they are there so they will not be assigned tasks in absentia. Other people attend because they always have attended. Often, topics are bandied about, consuming a great deal of time, yet these items are not resolved by the end of the meeting. Another meeting is scheduled to rehash the same conversations in the hope that a consensus can be reached. I suggest several techniques to reduce the cost of meetings. The first is to determine the importance of each agenda item. Then I calculate the salaries of the people who will be in the room and develop a cost per minute. This should be placed on an overhead display so that meeting participants can see the meeting costs on a minute-by-minute basis. This helps participants to focus on the topics and the value of the time spent discussing the issues.

Another example I like to use is the wasted time resulting from having people in meetings who do not need to be there. Some people only need to be there for certain topics. I like to have these people rotate in and out of the meeting as required. A meeting assistant can call the people when they are needed and arrange for a graceful exit when they are no longer required. It may be useful to have some people attend the meeting by teleconference. They can listen in from their desk as they do other work. If they hear something they would like to comment on, they do so. If someone has a question for them, they answer it. When their presence is no longer required, they leave the teleconference.

If participants attend via video conferencing, remember that there are communication costs as well as salary costs. Video conferencing is an excellent tool. It enables people to participate in meetings without incurring travel time and expenses. Do not forget that video conferencing can also be done from the desktop or from local or remote meeting rooms. This enables people to attend the conference on an as-required basis: coming in for a few moments, and then leaving. Others can stay for longer periods and may even attend for the entire meeting. This example helps auditors realize that there are no sacred processes and that they should look at all company processes, not just transactional processes. Obviously, I have many more examples relating to the various business processes. I am sure you can think of many of them as well.

### **Automating Auditing for Profit**

Automating the *Auditing for Profit* process is one of my pet projects. I am concerned that we are missing many cost-reductive or revenue-enhancing opportunities because we do not use audit software as frequently or as deeply as we should. One of the constant annoyances of modern e-commerce is the time wasted when trying to buy a product, solving a problem with a reservation, or seeking assistance with a web transaction that just will not work. Often I end up in automated assistance hell. When I dial, I get seven or eight options, none of which quite apply. Once I get close to what I want, I get put on hold until the ice melts in the spring or so it seems. Then I can not get an answer, as I must go through level one triage before I can get to someone who really knows the answer. Not only is this frustrating, but I often hang up. This could result in a lost sale or an unnecessary return of perfectly good merchandise. It could cost you the client's future business.

Since this happens to me, I expect it happens to other customers. To determine if it is a problem, I suggest using audit software on the Call Management System. This software can be used to identify the number of clients who hang up without making a touch tone selection, those that hang up without getting through to a human, and the number of excessively long calls (which indicate that the client is not getting a timely solution). These are just the high-level tests that indicate a problem exists. There are many more tests that we can create to enhance revenues and provide better customer service. The same software that was written for call management could possibly be adapted to identify customers who are having difficulty with Internet transactions. My objective is to identify how many customers attempt to complete an order, then quit before it is completed. While these are Information Technology *Auditing for Profit* issues, I also believe we should utilize *Auditing for Profit* software for more traditional uses, such as collecting receivables sooner, reducing bad debts, and identifying and recapturing duplicated vendor payments.

I suggest that you take another look at your SOX workpapers and documentation to identify areas for profit enhancement or labor reduction. I like to identify items with a fast recovery cycle. If your company can spend less than \$50,000 and produce a definite cash return of \$200,000 within three months, then the item should be a high priority on your list. Setting Return-on-Investment thresholds, such as items that produce a 200 percent return in less than three months, enable a speedy return on the audit effort. Obviously, these items should be researched and implemented first. This will provide an immediate result for your *Auditing for Profit* program. Then you can work on the items that require a larger capital investment, but have an even higher Return-on-Investment potential.

### **Information Security: An Example of SOX Audit Casualties**

The next item I would like to discuss is the diversion of internal audit resources from planned audits to the SOX efforts. While I understand the need for this, I think the sooner we return to our audit plans the better. I am particularly concerned with Information Technology audits that have been deferred. Our technical audits in the last six months have shown that security is not at the level required to protect essential financial and business information assets. Most of the items we identify are housekeeping issues that enable disgruntled staff and contractors, competitors or electronic espionage agents, and hackers to gain unauthorized access to your organization's environment. In my opinion, 2005 should be the year we focus on Information Security.

In 2004, we did not see any improvement in information security, as most of our clients were focusing their audit resources on SOX. This year, I believe that auditors should focus on validating basic information security. I would start with a network audit, followed by UNIX/Linux, Windows server and desktop and mainframe operating system and security audits, as well as database audits. Using our methodology, these audits can be completed in four to six weeks and will provide a high return on audit hours invested. In the next few paragraphs, I will provide a brief description of the major items we uncovered in the past year. These identified items can be used to assist in your own risk assessment.

Overall, network security remains poor. Very few organizations have implemented the intrusion prevention (IPS) and intrusion detection (IDS) software. Those that have often miss a few critical settings. When we go into a client's environment, we normally just plug into a network jack, install our own hub and go to work. Network jacks should not be active unless they are used by authorized employees and contractors. In addition, the unique computer identifiers, such as the MAC address (Media Access Control), should be checked before the software activates the jack. If an unauthorized machine plugs into the network, an alert should be sent to the security staff so that they can take immediate action.

Access to services such as GoToMyPC and tools such as netcat and cryptcat enable someone on the inside of the network to create a session to an external machine. The external machine can then control the internal machine, which can be used to attack the rest of the network. We call these inside-out outside-in attacks. Most of our clients are unaware of these types of attacks and have not taken measures to prevent them.

In the Windows environment, some of the older threats have not been remediated. Using anonymous null sessions, we nearly always identify accounts with poor passwords. In the past few audits we have performed, capturing the passwords for the entire domain has only taken an hour or two of effort. In some cases, the client has moved to Active Directory, which is more secure, yet they often leave the old domains up and running. As a result, we are able to compromise an account in the Active Directory to gain administrative rights. Another one of the older threats that we have failed to see remediated is the MS03-026 DCOM vulnerability. This vulnerability, with exploit code publicly available and in the wild, enables an unauthenticated user full access to the system, allowing an attacker to add an administrative account/backdoor to the system. A fix for this exploit was issued well over a year ago, yet in every environment, we have found a few machines that were not patched. In the Windows environment, one or two poorly secured systems can be the crack in the dike. Without Hans Brinker to put his thumb in the crack before the security dike collapses, the entire Windows environment may fall.

In the UNIX environment, there are several issues that can lead to a security domino effect. The first are missing patches. In the SUN environment, the two vulnerabilities we find most often are the Integer Overflow exploit and

the SAdmin feature. Implementing patches and configuration changes effectively negate these risks. In almost every UNIX environment we have audited, we find that unnecessary services are active. These unnecessary services vary in risks, from letting an attacker use trust relationships to gain root access to a machine to enumerating accounts or performing a denial of service attack. Services such as Telnet and FTP can also be used to sniff unencrypted passwords as they traverse the network. Clearly, the UNIX environment is worthy of an audit.

Lastly, I am concerned about poorly secured Internet connections. Many of our clients permit staff to do email from home. This is a great idea and a productivity enhancer, provided it is done securely. The most common flaw is to enable web mail users to log on using their internal network account and password. As I mentioned above, these passwords are easily compromised in a poorly secured Windows environment. The control is to use two-factored authentication. This requires the use of security tokens (RSA/SecurID), digital certificates, or biometric devices. Without this additional layer of authentication, it is very easy for a disgruntled employee or contractor with internal network access to compromise the web mail application, view email and even send email from another person's account.

As you can see, Internal Audit as a profession has a lot to accomplish in the next year. I have just scratched the surface of the workload ahead of us. Now that we have the SOX documentation, let us use it to make our organizations more profitable. Also, let us refocus on making our computer devices, business applications and networks more secure. It would be very embarrassing if your organization signs off on SOX, only to have attackers trample your controls and steal your data. By focusing on security, we can ensure that controls are in place to prevent your organization from being front page news in the Wall Street Journal.

As always, the comments in this article are mine and mine alone. I invite you to send your comments to me ([Gordon@canaudit.com](mailto:Gordon@canaudit.com)). I read and respond to every one of them. Should you need information on technical audits or Auditing for Profit please email me or call me at (805) 583-3723.



Gordon Smith  
President, CEO