

# Canaudit Perspective

April 2007  
Volume 8, Issue 2

## TOPICS OF INTEREST:

- Carefully crafting the right-to-audit clause
- Data access and audit automation
- Disaster preparedness, business continuance, backups, and offsite storage
- SAS 70's do not ensure that a third-party vendor is secure
- Surprise audits and penetration tests
- Vendor subcontracting or outsourcing of work
- Enforcing salesperson promises
- Conclusion

## DEFINING THE RIGHT-TO-AUDIT CLAUSE



GORDON SMITH  
Canaudit President

In this article I would like to address an issue that is often left out of vendor contract negotiations - the right to audit. My concern is that many of our clients fail to include right-to-audit clauses in critical contracts. Other clients have a simple clause that specifies the right to audit, but not the terms. Before I go any further, I have

to state that I am not a lawyer. I

am simply an auditor who has read and audited many contracts. All contracts regarding consulting services, software, outsourcing and other terms relating to processing your organizations transactions should be reviewed by an attorney who specializes in information technology. The items I have listed below should be used as a guideline for negotiating contracts.

### CAREFULLY CRAFT THE RIGHT-TO-AUDIT CLAUSE

The right-to-audit clause should not be a single paragraph. Rather, it should include statements that ensure that a full audit can be conducted of vendors or trading partners. A common shortfall of existing contracts is that the required notice period is not mentioned. When the auditor invokes the right to audit, the vendor may claim that 30, 60 or 90 days notice is required. This precludes the ability to perform a surprise audit, and the lengthy delay may disrupt the audit plan. Hours of work should be clearly defined. If you would like to conduct your audit in normal business hours, specify the timeframe. A vendor could claim that auditing must be

performed in the evening or overnight hours, to ensure that normal processing is not affected.

Do not forget to include the business locations that can be audited. A vendor could state that the audit can only be performed at their headquarters. Their data centers or data storage facilities could be at other locations. If you can not visit those locations, then your right to audit is severely impeded.

### DATA ACCESS AND AUDIT AUTOMATION

The right to audit may not include the right to access data or use audit software. When using an application service provider (ASP) to process your data, it is essential to ensure that the data is accurate and that it balances. This will require the use of specialized data analytic software, such as Interactive Data Extraction and Analysis (IDEA) or Audit Command Language (ACL), to interrogate the data. It would also be useful to run other audit software tests to ensure that there are no unusual data, transactions or conditions. The right to use audit software and the software products that can be used should be clearly specified, along with the right to change the audit software. I prefer this wording: "The client has the right to use general audit software and other reporting tools against the data files and / or databases." This includes the use of IDEA or ACL. It should also leave the door open to use other ad hoc reporting tools, as your audit department may switch tools over the life of the contract

It is quite possible that your organization might have a contract clause that states that your data will be segmented from other vendor client data. You may assume that it is physically separated. It is likely that this assumption is wrong. In most cases, the data is

logically separated within a database or database instance. If the data is stored in a database that is logically separated, it is doubtful that the vendor will give you direct access to the database. Before signing the contract, the data storage issues should be addressed. Determine if the data is physically segmented in different files or storage partitions, or if it is logically separated within a database. Once this is determined, you can draft the required contract clause. It is best to keep your options open in case the vendor changes their segmentation methodology. If they currently physically segment, then you should include a clause that states that you will be given direct access to data if the databases are merged and segmented logically.

If the data is logically segmented, the vendor may not want to give your organization direct access to the database. Instead, they may offer to give you an extract that contains only your organization's data. I usually frown on this, as it compromises independence. As an alternative, I believe that the extract program or code should be reviewed by your organization's internal IT auditor, then run under the supervision of your auditor. This will need to be clearly stated in the right-to-audit section of the contract.

#### **LET'S NOT FORGET DISASTER PREPAREDNESS, BUSINESS CONTINUANCE, BACKUPS AND OFFSITE STORAGE**

We are very concerned about disaster preparedness and business continuance. If the vendor has an outage and services are not available, then their disaster becomes your disaster. The right to audit the vendor's disaster and business continuance plans are necessary to ensure that your organization will be protected in the event the vendor has a prolonged outage or full-scale disaster. If your organization is a major client of the vendor, try adding in a clause that enables your auditors to attend one of the disaster-readiness tests.

The right to audit backup and recovery procedures is essential. This right to audit should extend to the offsite records management facility and data transfer procedures to and from the facility. In the last year, there have been several examples of data lost during the transfer process. Also, with summer coming, the courier van should be climate controlled to ensure that the media is not damaged by excessive heat buildup in the vehicle.

Another issue is the ability to read the backups when they are needed. Recently, an employee of the State of Alaska inadvertently destroyed the primary files. The backup files could not be read. In the past, we suggested that the backup process be modified to include a "read after write" option. This ensures that

the media can be read when it is needed. For the backup audit test, it would be a good idea to see if volumes containing your organization can be read.

#### **SAS 70'S DO NOT ENSURE THAT A THIRD-PARTY VENDOR IS SECURE**

In an outsourced environment, the auditor usually relies on the SAS 70 reports. In my opinion, a SAS 70 does not give me any assurance that the required security is in place. If you are relying on a SAS-70, then additional testing is required to ensure that the network, servers, programs and data are properly protected. In an outsourced environment, the right to audit must include the right to conduct testing above and beyond the SAS 70 testing to ensure that your organization's information assets are properly protected.

There are several levels of testing that can provide that assurance. The first is a Security Baseline. This test is performed with the knowledge and the possible participation of the outsourcer and the IT Security staff. With many of the same tools used during a Penetration Test, the audit team documents the network, then runs a battery of security tests against the machines and software to identify and document vulnerabilities. At the end of the project, the security status of the machines in the network is documented along with the specific remediation efforts required to enhance security. The baseline is re-performed in three months to quantify improvement and create metrics for measuring the remediation effort.

#### **SURPRISE AUDIT AND PENETRATION TESTS**

The ability to perform surprise audits and penetration tests is a necessity if your organization has outsourced processing and networks. Surprise audits are intended to test the controls in place during the normal business cycle. The vendor does not know when the test will be performed. Audit clients are often most careful during normal audits. Surprise tests are intended to measure how the client performs on a day-to-day basis. This technique is useful for testing physical security procedures and cash and application controls. It can include the surprise use of audit software to identify application errors or security patches on servers and workstations. We also suggest that the vendor's network be tested to ensure that your data is properly encrypted when the data is transmitted. This can be done as part of the normal audit or as part of a Penetration Test.

A Network Penetration Test should also be performed on a surprise basis. This enables the audit team to test the Intrusion Detection and Response Procedures. The Penetration Test is required for outsourced IT

operations and application outsourcing. The right to perform surprise penetration audits should be written into the contract. When we do penetration tests of our clients, they often ask us to do some testing of their outsourced vendor's site. We work closely with the client to obtain the required permission to do testing of the vendor's site. In most cases the vendor is very receptive as they get the test without paying for it. We have done Network Penetration Tests for several of our clients that have outsourced IT operations. We found that the outsourcer is generally open to the testing; however, they may have to place some limitations on the test. As an example, they would not want our team to access another client's data, or they may exclude certain systems from testing as they are shared with other clients. These are acceptable exclusions.

### **VENDOR SUBCONTRACTING OR OUTSOURCING OF WORK**

In the last three years, I have noticed an increase in vendors who outsource or offshore all or part of their operation. Our concern is that confidential information or proprietary software may be transferred to an offshore entity. There have been several published cases where confidential information has been harvested and sold to others. In one case, a contractor threatened to release confidential information if she was not paid. In my mind, it is important to know if any work is subcontracted to other vendors. In addition, it is necessary to know if any data has been off-shored.

Let's look at the subcontracting issue first. Many companies subcontract or outsource parts of their organizations. Helpdesk functions and network support are examples of functions that are outsourced. While your organization may outsource to a selected contractor, the contractor could in turn outsource their operation. It is essential to extend the Right-to-audit clause to all subcontractors. Note that the contract should also state that the contractor cannot subcontract the work out without your organization's prior written approval.

Many vendors have opened their own offices in other countries, in their continuing efforts to export North American jobs and reduce costs. The offshore employees are of high quality and industrious. My concern is not with the employees, as it is with the data and the protection of that data. I strongly urge your audit department to consider the risk of data

stored or viewable offshore. Controls must be in place in the overseas facility to ensure that the data is properly protected. When I talked to one vendor about offshore data, they insisted that the data was not offshore. It was securely located in a database in this country. They stated that the offshore employees can only view the data on their screens, that only the image is sent overseas. I suggest that the vendor did not consider screen scrapers or database queries that export the data to a printer or a file. I believe you should include in the contract the right to audit all locations where your data can be viewed or exported.

### **ENFORCING SALESPERSON PROMISES**

If a salesperson promises something or says something is "no problem", make sure you include whatever that something is in the contract. Often the sales staff truly believes that a right-to-audit clause will not be an issue. When it is time to sign the contract, they find that their own Management does not want contract modifications. When in negotiations with the salesperson and they agree to a condition, I always double-check that they are willing to put the specific issue into the contract. I keep a list of the items and present it to them at the end of the meeting. When the contract is presented, I check it carefully to ensure that all promised items are included. If anything is missing, we send it back for revisions along with copies of the salesperson's statements.

### **CONCLUSION**

The right-to-audit clause is more complicated than most auditors or even lawyers realize. If a vendor wants to restrict your ability to find issues, they can deny access to your auditors if there is no right-to-audit clause. If there is a clause, then they can restrict your ability to audit unless your organization's rights are carefully documented in the contract. I also caution you to be realistic. Each vendor is different. Some will add some or all of the above items. Others will push back. We have assisted several clients in the contract negotiations, specifically on the right-to-audit clause. In each case, we have found that the vendor was willing to deal if your firm would not sign the contract until they did. The vendor wants the contract more than you need the vendor - remember that during the negotiation phase.

*The opinions expressed in this article are mine and mine alone. I look forward to receiving your comments and question. You can email me at [Gordon@canaudit.com](mailto:Gordon@canaudit.com)*

## AUDIT & SECURITY SERVICES

Canaudit specializes in a variety of information system and technology audits, ranging from periodic network penetration testing to full network and operating system security review. Our tailored audits provide an objective, disciplined, and in-depth analysis to evaluate and improve the effectiveness of risk management, control and security within your organization's technological environment.

For interest in Canaudit to perform an IT audit for your organization, please email [Gordon@canaudit.com](mailto:Gordon@canaudit.com) or [Tamra@canaudit.com](mailto:Tamra@canaudit.com), or call (805) 583-3723.

---

## PROFESSIONAL DEVELOPMENT

Canaudit provides quality seminars to local chapters and major corporations. These seminars include technical information system audit classes aimed at everyone from an introductory level up to management. With a list of over 30 courses to choose from, we are sure to have a course that will meet your individual needs. In addition to chapter and private seminars, Canaudit also holds public courses. Upcoming public courses are posted on the website, [www.canaudit.com](http://www.canaudit.com).

### Upcoming Public Courses:

#### Philadelphia, PA

May 7 - 11, 2007

May 7 - 8, 2007

May 7 - 8, 2007

May 9 - 10, 2007

May 9 - 10, 2007

May 11, 2007

~~The Ultimate Network Penetration Class~~

Control & Security of Windows 2003

Control & Security of UNIX

Control & Security of Web Applications

~~Control & Security of Oracle~~

Control & Security of Microsoft SQL Server

**SOLD OUT!**

**SOLD OUT!**

*NEW*

#### Bloomington, MN

June 11 - 15, 2007

June 11 - 13, 2007

June 11 - 12, 2007

June 13, 2007

June 14 - 15, 2007

June 14 - 15, 2007

The Ultimate Network Penetration Class

Automating Technical Auditing

Control & Security of Windows 2003

Control & Security of Microsoft SQL Server

Control & Security of UNIX

Control & Security of PeopleSoft

*HANDS ON*

*HANDS ON*

*NEW*

#### Farmington Hills, MI

October 15-19, 2007

October 15-19, 2007

The IT Audit & Security Boot Camp

The Ultimate Network Penetration Class

*HANDS ON*

*HANDS ON*

#### Simi Valley, CA

December 3 - 7, 2007

December 3 - 5, 2007

December 6 - 7, 2007

The IT Audit & Security Boot Camp

Automating Technical Auditing

Control & Security of Windows 2003

*HANDS ON*

*HANDS ON*

Registration for a Canaudit public seminar can be performed online at [www.canaudit.com](http://www.canaudit.com). For additional information or interest in hosting a Canaudit seminar, please email [Brenna@canaudit.com](mailto:Brenna@canaudit.com) or call (805) 583-3723.