Using CAATs to Support IS Audit

S. Anantha Sayana, CISA, CIA

CAAT refers to computer-assisted audit technique. This implies that an auditor's use of a computer-assisted audit technique is something special—normally the techniques used by an auditor are not computer assisted. Today, in most large and medium-sized enterprises, there are few business processes that are not driven by computers. The business does not refer to them as computer-assisted business processing. The use of computers and information technology for doing business is taken for granted, so why should auditors talk about something special called CAAT?

Performing audits without using information technology is hardly an option. When all the information needed for doing an audit is on computer systems, how can one carry out an audit without using the computer? While the audit world will likely grow out of using this terminology, for the purpose of this article, the term CAAT refers to the use of certain software that can be used by the auditor to perform audits and to achieve the goals of auditing.

CAATs can be classified into four broad categories:

- Data analysis software
- Network security evaluation software/ utilities
- OS and DBMS security evaluation software/utilities
- Software and code testing tools

Data Analysis Software

Data analysis software is the most popular of the four and is loosely referred to as audit software. The generic products available under this segment are termed as general purpose audit software, also known in some parts as GAS or generalized audit software. This software has the ability to extract data from commonly used file formats and the tables of most database systems. Thus, these systems can be used during the audits of almost any application on any technology platform. The audit software can perform a variety of queries and other analyses on the data. Some of the features are: data queries, data stratification, sample extractions, missing sequence identification, statistical analysis and calculations. This software also can perform operations after combining and joining files and tables. The list of features grows with each version of this software and a recent added feature is Benford analysis.

Need for Audit Software

Going back to the very basics, the IS audit methodology starts with risk analysis, which translates into, "What can go wrong?" The next step is to evaluate controls associated with the situation to mitigate risks, or, "What controls it?" The evaluation of controls goes into not only the design of the controls, but also their actual operation and compliance. Most observations, interviews, scrutiny and compliance testing are to determine whether controls exist, are designed well, are understood, operate effectively and are being complied with by the operating personnel. At the end of this phase the IS auditor could have observations about some controls that exist and are operating satisfactorily or some controls that are nonexistent, badly designed or not in compliance.

The following is an example of an IS auditor performing a payroll review. While doing an application review, the IS auditor observed that many of the required validations relating to the salary ranges and admissible allowances and perks were not built into the application software and concluded that it was possible to process values that did not meet the rules. When performing compliance testing, the auditor also observed that the modification logs and exception reports were not being checked regularly by the payroll officer. The application was in use at the organization for more than two years. While the observations were noted and corrective action was immediately taken on modifications to the software to include the validations, management's concerns were, "Have any errors or fraud really taken place? Have we lost any money? Have we erred in any payroll-related tax compliances?"

The IS auditor's job is not really complete until these questions are answered. The IS auditor's job is not only to notify concerns and alarms but also to recommend corrective action and provide concrete assurances and proof of errors wherever possible. The IS auditor is faced with the daunting task of verifying payroll for two years for, perhaps, thousands of employees. Doing this manually would take many audit clerks working for weeks and weeks and with no guarantees about the coverage.

In comes audit software. The complete verification of the entire payroll for two years, covering all the doubtful cases where validations and checking were inadequate, is possible. And this can be done with minimal effort and time, with guaranteed accuracy.

The number of occasions where such assurances and answers are sought by management from the auditors is not confined to just payroll. Progressive management teams and boards that are IT savvy would ask these questions for many cases as an effective aid to good governance. The disclaimers stated by auditors based on sampling are increasingly becoming luxuries that are neither affordable nor available anymore. Using audit software for substantive testing to provide total assurance or clear pinpointing of errors and frauds greatly increases the credibility and value provided by the audit function. That is obviously the way to go.

Prerequisites for Using Audit Software

Connectivity and Access to Data

The first prerequisite for using audit software is access to data. The auditor needs to obtain access to the "live" production data. In most cases, this is fairly easy to do. The IS auditor has the audit software installed on a notebook computer and connects it to the network where the server holding the data exists. The auditor then needs to obtain "read only" access to the

files/tables that hold the data and can transfer the data files to the notebook computer. Once this is done, the audit software can use the data files and perform the audit. It is necessary to ensure that the data that are downloaded are the actual copy from the real production data. This can be achieved when the data transfer is done either by the auditor or by the specialist IS auditor assisting a general auditor. In large enterprises using wide area networks, it would be possible to do this data transfer even from a remote location in the network, such as from the audit headquarters, without traveling to the actual geographic location.

Knowledge of the Application and Data

The IS auditor needs to know technical details of the platform on which the application is built. Knowledge of the files or tables in which the data reside also is necessary. The auditor needs to get the file description and the data field types. If certain codes are used in the tables, the corresponding description of the codes also needs to be known. While discovering all this looks daunting, it is not. If the IS auditor has performed an application review, these details would have been scrutinized and are readily available. The ideal situation would be to perform an application review and then use audit software to carry out the substantive testing. In many organizations specialist IS auditors perform application reviews, leaving behind notes and details on the technical issues for general auditors to perform compliance and substantive tests using audit software year after year, as long as the application remains without major changes. In cases where the application data reside on a relational database, most of the currently available audit software can connect to the database using open database connectivity (ODBC), and the entire set of tables can be seen together with their descriptions.

In the payroll example, the auditor would see some typical files or tables, such as the employee master, that contain details such as employee number, name, age, sex, designation, department and grade. There could be another table that contains the various salary components payable to certain grades, designations and departments. There may be other tables that contain other parameters that determine salaries. The database also would contain tables that hold data about various special pay, deductions, statutory payments, etc. Finally, there would be the processed payslip file that contains the details about what was paid to the employees under various heads. All these files/tables would be downloaded by the auditor into the auditor's notebook and taken into the audit software. Audit software requires that these input files be defined to them and that most audit software has menu-driven wizards that pick up these definitions fairly easily. It is to be noted that well-established audit software that is available commercially operates only on a copy of the data downloaded from the main database and does not affect the live data in any way.

Audit Skills and Identifying the Concerns

After the data are downloaded and ready for analysis by the audit software, the auditor needs to know what control concerns are to be tested and validated. This is probably even more basic than the skill needed to download the data. Audit software has many features but the features cannot perform an audit on their own. The auditor has to design the procedures and tests. The tests that the auditor carries out are designed using the knowledge of the application, the business rules behind the function and the findings of the application review. For example, a few of the tests that can be done on the payroll data are as follows:

- Scan the payslip file to determine total payments above a threshold limit.
- If there are ceilings for certain elements of the pay, check if any of the payments have exceeded the limit.
- If rules on ceilings relate to grades, designations or departments, check for such combinations to see if limits have been exceeded.
- Check for differences between the payroll employee master and the personnel department's employee master, if available (ghost employee test).
- If some elements of the pay are calculated, check those elements against calculations made by the audit software.

Many other tests can be carried out based on the business rules relating to the function and the knowledge of the application. The designing of these tests requires good audit skills combined with knowledge of the business and expertise with the audit software.

The kind of tests that are run will vary with the applications. For example, in a procurement audit, the auditor may download the purchase order and related files and perform analysis of prices. In a financial accounting application, the auditor may analyze expenses on dollar value, revenue expenditure, account head, and department or cost code. In a banking application, the auditor may verify interest payments using the audit software. In a sales application, the correctness of product prices or incentives may be analyzed. It is the audit skill of determining what is to be verified and tested, coupled with the knowledge of the business and the application, that makes the software actually do the audit work.

Benefits of Using Audit Software

With data volumes growing and management expectations on assurances becoming more specific, random verifications and testing do not yield the desired value. The use of audit software ensures 100 percent scrutiny of transactions in which there is audit interest, and pointed identification and zeroing in on erroneous/exceptional transactions, even when data volumes are huge. And all this can be done in a fraction of the time required with manual methods.

Another advantage of the audit software is the uniform user friendly interface that the audit software presents to the auditor for performing all the tasks, irrespective of the data formats or the underlying technology used by the application. The audit software also maintains logs of the tests done for review by peers and seniors, and advanced features allow the programming of certain macros and routines that can further enhance audit speeds and efficiency.

A Few Words of Caution

The first-time deployment of audit software in any organization is not without pain. Problems will occur in almost all areas, beginning with the reluctance of the IS staff. Following this are obtaining access to the production data, fearing that the audit software may interfere with the processing, the improper processing of downloads, the incorrect input of file definitions and so on. Investing in training on the audit software is essential and this cost should be considered while purchasing the software. The training should not be confined to the commands and menus in the software but must include real-life exercises using one of the applications running in the organization. It

also would help if the trainer is not strictly an IT person, but has some audit background, too. Although the first attempt at using audit software is painstaking, there need be no doubts on the benefits and gains of continued deployment, so the need is to persevere and win through the initial difficulties with help from the IS department and the trainer.

Selecting Audit Software

The important criteria that are followed in any software selection are applicable to audit software, too. The IS auditors also may develop audit software on their own. However, the key requirement of the audit software is that the results that the audit software produces must be of high reliability and accuracy. From this perspective, it may be preferable to use a commercial well-established product. The maintenance and change management relating to self-developed audit software may prove to be a big burden for auditors and take their minds away from their core function.

The web sites of a few illustrative audit software providers are given for reference at the end of the article. There obviously are many more, but visiting some of these sites is a good way to begin for someone who contemplates using CAATs.

Other CAATs

The areas of work of an IS auditor extend to evaluating security relating to operating systems, databases and the network. There are tools that can be run to find the various parameter settings that influence security. These tools also can compare the settings against the defined security policy of the organization and list the noncompliances. Some of these tools have specific versions for different technology platforms, and the right one needs to be procured. The use of these tools brings a consistency to the security evaluation process and also speeds it up. However it should be remembered that these tools do only a portion of the evaluation and need to be supplemented by observation and scrutiny of system administration practices and procedures.

The evaluation of network security uses tools such as sniffers and scanners. It also is acceptable to perform "attack and penetration" testing (after proper preparation and approvals) that detect vulnerabilities in networks. This involves the use of tools, many of which are available freely on the Internet. While using this, the auditors need to exercise due care to ensure their integrity and reliability by due testing and other references.

Traditionally, textbooks have detailed methods using test decks and other software testing mechanisms as tools. While these are true, their application by auditors is becoming rare. The huge improvements in the quality and reliability processes reinforced by certifications in the software industry, the rigorous user acceptance testing and signoffs by aware users have made testing by auditors redundant throughout the years. Auditors should examine the environment in which they operate and decide accordingly on software testing, using techniques such as test decks, audit hooks and integrated test facilities.

Linkage to the Standards

The IS Auditing Guideline issued by the Standards Board of ISACA on the use of computer-assisted audit techniques (CAATs) relates the guideline to Standard 060.020 (Evidence), Standard 050.010 (Audit Planning) and Standard 030.020 (Due Professional Care). The use of CAATs becomes very useful, if not imperative, to comply with standard 060.020, which states, "During the course of the audit, the Information Systems Auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence." The guideline also provides useful information on planning for use of CAATs, security of data and CAATs, performance of audit work and CAATs documentation and reporting, and is a must-read for anyone who wishes to use CAATs. The guideline can be downloaded from the standards section of ISACA's web site. Hence, it is not reproduced here.

References

Web sites of selected audit software vendors (illustrative):
www.acl.com
www.caseware-idea.com
www.wizsoft.com
www.ecora.com

S. Anantha Sayana, CISA, CIA, is deputy general manager of corporate IT with Larsen & Toubro Limited, Mumbai, India. Anantha has more than 13 years of experience in IS audit and internal audit in banking, manufacturing and service industries spanning a wide variety of applications and technical platforms. He is a past president of the ISACA Mumbai Chapter. He can be contacted by e-mail at *sas-pia@powai.ltindia.com*.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.