Chapter 4

Tools and Techniques Used in Auditing IT

LEARNING OBJECTIVES

1. Define auditor productivity tools and describe how they assist the audit process.
2. Describe techniques used to document application systems, such as flowcharting, and how these techniques are developed to assist the audit process.
3. Explain what Computer-Assisted Audit Techniques (CAATs) are and describe the role they play in the performance of audit work.
4. Describe how CAATs are used to define sample size and select the sample.
5. Describe the various CAATs used for reviewing applications, particularly, the audit command language (ACL) audit software.
6. Describe CAATs used when auditing application controls.
7. Describe CAATs used in operational reviews.
8. Differentiate between "Auditing Around the Computer" and "Auditing Through the Computer."
9. Describe computer forensics and sources to evaluate computer forensic tools and techniques.

Computer technology has become an integral part of most organizational functions. It is likely that many audit clients either have eliminated or will eliminate a substantial portion of their paper documents and replace them with electronic documents filed only in computerized form. An auditor who is unable to use computerized audit tools and techniques effectively will be at a disadvantage.

Today's auditor must be equipped with an understanding of alternative tools and techniques to test the operations of computerized systems and gather and analyze data contained in computerized files. Auditors can take advantage of those tools and techniques to be more efficient and effective when performing audit work. Tools and techniques used in IT audits include:

- *Audit productivity tools*—software that helps auditors reduce the amount of time spent on administrative tasks by automating the audit function and integrating information gathered as part of the audit process.

- *System documentation techniques*—methods, such as flowcharting, data flow diagram, and business process diagrams applied to document and test application systems, IT processes, and their integration within the IT environment.
- *Computer-assisted audit techniques (CAATs)*—software that helps auditors evaluate application controls, and select and analyze computerized data for substantive audit tests.

This chapter starts by defining auditor productivity tools and describing how they help the audit process. This chapter then touches upon the various techniques used to document application systems, in particular financial application systems, and how they assist the audit process. Explanations of CAATs and the role they play in the audit will follow along with descriptions of the various CAATs used when defining audit sample size, selecting samples, and reviewing applications (e.g., Audit Command Language (ACL), etc.). CAATs used in auditing application controls and in operational reviews will then be described followed by explanations of auditing around or through the computer. Lastly, computer forensic tools and techniques are discussed.

Audit Productivity Tools

The core of the audit process is assessing internal controls to determine if they are effective or need improvement. However, many of the tasks associated with performing an audit, such as planning, testing, and documenting results, although necessary, take time away from performing the actual control assessment work. This is where auditor productivity tools come into play. Auditor productivity tools assist auditors in automating the necessary audit functions and integrating information gathered as part of the audit process. Examples of audit functions that may be automated through auditor productivity tools include:

- Audit planning and tracking
- Documentation and presentations
- Communication
- Data management, electronic working papers, and groupware
- Resource management

Audit Planning and Tracking

Developing an audit universe with all of the potential audit areas within the organization, a risk assessment prioritizing these audit areas, an audit schedule, and a budget to track audit progress are some of the necessary tasks in any audit planning. Solutions such as spreadsheets, database software, and/or project management software can be used to document and plan audits, as well as track their current status. However, each of these solutions is standalone, as their integration may not even be possible. Because planning tasks are interdependent, an auditor productivity tool software that integrates these planning and tracking tasks would provide quicker update and ensure that all phases of planning are kept in sync. For example, the budget should provide sufficient costs to accomplish the audit schedule, or the audit schedule should not exceed the resources available, etc.

Documentation and Presentations

Tools, such as the Microsoft Office suite, provide features to facilitate the creation and presentation of documents. For example, spreadsheet data containing functional testing results can be incorporated into a report document with a few clicks of a mouse. These same data can then be copied to a presentation slide and also be linked, so that changes to the source documents will be reflected in any of the related documents. Software tools like these save time and ensure consistency and accuracy. Other tools include video conferencing and/or video capture software to provide presentations to collaborators worldwide and to document audit evidence, respectively.

Communication

Because the auditor operates as part of a team, the need to share data as well as to communicate with other members of the group is important. Providing immediate access to current data, electronic messaging, and online review capabilities allow audit staff to quickly communicate and gather research information for audits and special projects. In addition, auditors may occasionally need to operate from a host computer terminal, yet still have all the capability of a dedicated desktop processor. Therefore, it is necessary to have the required computer hardware, media hardware, protocol handlers, desired terminal software emulators, and high-speed wired or wireless connectivity at the audit site.

Electronic connectivity not only allows auditors to communicate but also provides access for organization management personnel or audit clients to exchange information. For instance, client's or organization's management personnel can be given access to the auditing risk universe database. This allows management to browse the database and suggest changes to current audit risk areas.

Video conferencing capabilities are also an effective way for communication. Video conferencing allows meetings to be conducted and members to participate worldwide. Some of the best video conferencing software includes Cisco WebEx Meeting Center, Citrix GoToMeeting, and Adobe Connect, among others.[*] Video conferencing software uses computer networks to transmit video, audit, and text data, smoothing the process of initiating and conducting live conferences between two or more parties regardless of their locations. Through video conferencing, participants can see a spreadsheet, a graph, or a video clip; receive live data feeds; and see responses from all parties involved.

Data Management, Electronic Working Papers, and Groupware

Establishing electronic connectivity provides audit personnel with the capability to access and input data into a central data repository or knowledge base. The central data repository (e.g., database, etc.) can archive historical risk, audit schedule, and budget data that can be accessed electronically by all authorized users throughout the audit group, regardless of physical location. Database applications can be developed to automatically consolidate data input electronically from all audit functions.

---

[*] www.pcmag.com/article2/0,2817,2388678,00.asp.

Resource Management

Another challenge for audit supervisors is to manage a remote workforce. Whether a staff auditor is working on a local audit or out in the field, managers need to be able to provide guidance and review work as the audit progresses. Audit managers need to provide feedback while the staff auditor is on location in case follow-up action is necessary.

A distributed workforce requires a very informed and responsive management team that can gather and disseminate information quickly. Important information can be rapidly gathered and disseminated function-wide through e-mail and message boards or computer forums. Supervisors can provide immediate feedback and direction on audit projects through online review of electronic work papers.

System Documentation Techniques to Understand Application Systems

Emphasis on understanding and documenting the organization's/client's information systems is particularly appropriate during the application analysis phase of an audit engagement. It is important for the auditor to understand the relationship of each application to the conduct of the organization's or client's business, and to document such understanding. For this, auditors typically request organizations or clients for an entity relationship diagrams (ERDs). If available, these ERDs are a great starting point for auditors, as they graphically represent the relationship between "entities" (or people, objects, places, concepts, events, etc.) within the information system (i.e., financial application system).

Documenting information systems, particularly financial application systems, help auditors, accountants, consultants, management, etc. in understanding what's going on financially at the entity and, most importantly, how to effectively evaluate those systems. Auditors also document financial application systems, as required by auditing standards, to understand the automated and manual internal control procedures the entity uses. In documenting financial application systems, auditors mostly use graphical representations, why? It has been said that a picture is worth a 1,000 words. Also, pictures tend to be easy to understand.

Documentation of application systems is commonly performed using narratives, diagrams, tables, data flow diagrams, business process diagrams, flowcharts, etc. Data flow diagrams or DFDs, for instance, are process-oriented and use graphics or symbols to describe data transformation and how it flows throughout the organization. Refer to Exhibit 4.1.

In Exhibit 4.1, the squares or rectangles represent data sources or destinations. Arrows indicate flows of data, and the circle symbol means that a transformation process is taking place. Business process diagrams visually show the various activities going on in a business process. These business process diagrams also show the organizational unit or process (e.g., payroll, accounts payable, cash disbursement, etc.) that is actually performing the activity. Refer to Exhibit 4.2.

In Exhibit 4.2, the rounded rectangles represent the activities or procedures occurring in a process. The circle indicates the start of a process, while the bolded circle indicates the end of the process. The arrow shows the flow of data. The dashed arrow is the annotation information or information that helps explain the business process. A third and most common example for documenting financial application systems is through flowcharting. Similar to the other system documentation techniques, flowcharts are a graphical description of a system representing how business processes are performed and how the various documents within the business process

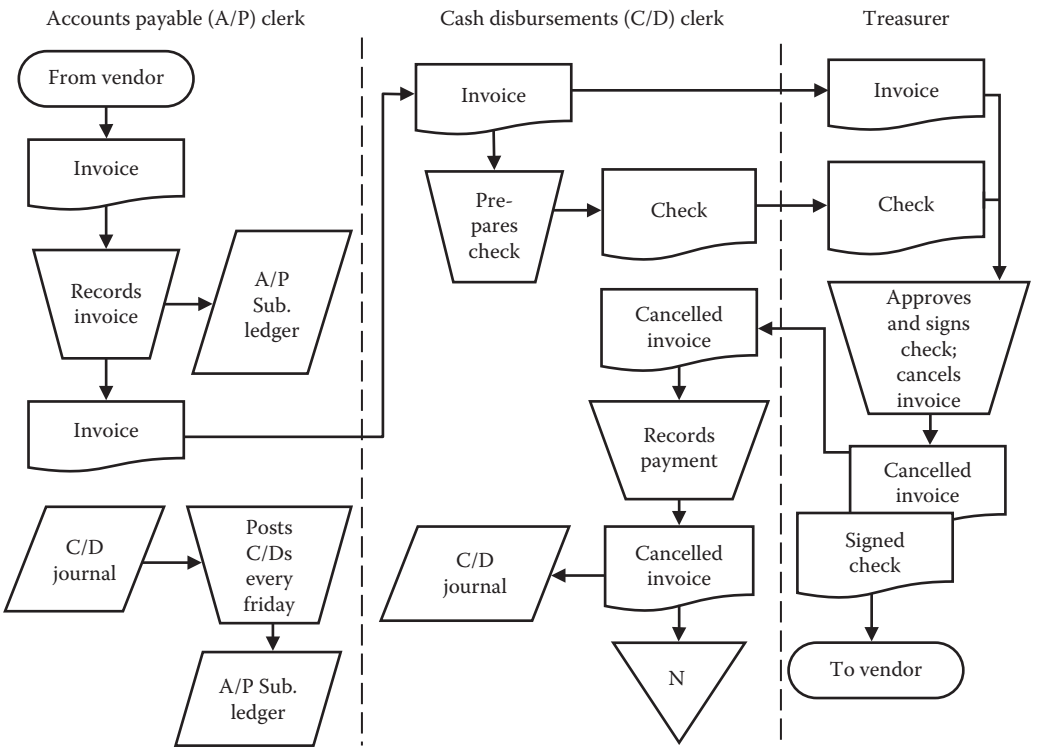

Exhibit 4.3 Example of a flowchart for a cash disbursement process.

Flowcharting as an Audit Analysis Tool

Auditors prepare flowcharts using standard symbols and techniques to represent application systems, workflows, or processes. Flowcharts developed during the application analysis phase of an audit engagement are most useful if they distinguish processing according to department, function, or company area. There are some very good application support packages for flowchart development as well as the power of the word processor to build diagrams and illustrations of the process.

For an IT auditor, flowcharts represent a method for identifying and evaluating control strengths and weaknesses within a financial application system under examination. It can be time consuming to build an understanding of strengths and weaknesses within a system to be audited. However, identification of strengths and weaknesses often is crucial because they will drive the direction of the remainder of the audit (e.g., substantiating and determining the effect of identified control weaknesses, etc.).

For example, Statement on Audit Standard (SAS) No. 109 requires the auditor gain an understanding of the entity and its environment and determine those controls relevant to the audit. The auditor must have an understanding of the nature and complexity of the systems that are part of the control environment being audited (i.e., financial application systems). One way of gaining that understanding is through any existing documentation which may provide a visual illustration of the system under review and any interaction with other systems. Any existing documentation, such as flowcharts, provides a benchmark for the auditor's review.

As a step toward building the needed understanding of control weaknesses, the audit staff should develop a flowchart diagram of all information processed. Flowcharts should encompass all information processed, from source documents to final outputs. Either automated or manual techniques can be used in preparing these flowcharts. With either approach, the process leads to the evaluation of a number of elements of a system, including the following:

- Quality of system documentation
- Adequacy of manual or automated controls over documents
- Effectiveness of processing by computer programs (i.e., whether the processing is necessary or redundant and whether the processing sequence is proper)
- Usefulness of outputs, including reports and stored files

Common flowchart symbols are described in Exhibit 4.4. Following are steps in the development of flowcharts.

Understanding How Applications Process Data

The auditor should understand how the financial application system, for example, generates its data. This understanding should encompass the entire scope of the financial system from preparation of source documents to final generation, distribution, and use of outputs. While learning how the system works, the auditor should identify potential areas for testing, using familiar audit procedures, such as:

- Reviewing corporate documentation, including system documentation files, input preparation instructions, and user manuals
- Interviewing organization personnel, including users, systems analysts, and programmers
- Inspecting, comparing, and analyzing corporate records

Identifying Documents and Their Flow through the System

To understand document flow, certain background information must be obtained through discussions with corporate officials, from previous audits or evaluations, or from system documentation files. Because this information may not be current or complete, it should be verified with the appropriate personnel (e.g., accounting, IT, etc.). A user or member of the IT department staff may already have a document flow diagram or flowchart that shows the origin of data and how it flows to and from the application. This diagram should not be confused with either a system flowchart that shows the relationship among the input, processing, and output in an IS, or a program flowchart that shows the sequence of logical operations a computer performs as it executes a program.

If not available, auditors will have to develop document flow diagrams. The document flow diagram should include:

- Sources and source document(s), by title and identification number, with copies of the forms attached
- Point of origin for each source document
- Each operating unit or office through which data are processed
- Destination of each copy of the source document(s)

- Actions taken by each unit or office in which the data are processed (e.g., prepared, recorded, posted, filed, etc.)
- Controls over the transfer of source documents between units or offices to assure that no documents are lost, added, or changed (e.g., verifications, approvals, record counts, control totals, arithmetic totals of important data, etc.)
- Recipients of computer outputs

Defining Data Elements

The auditor must build a clear understanding of the data being recorded on the application for definition purposes. When defining individual data elements, titles can be deceptive. For example, is a cost derived from the current period or is it cumulative? Is the cost accrued or incurred? What are the components of a cost? Use descriptive names when defining data elements and action verbs for processes (e.g., update, prepare, validate, etc.). The organization's data element dictionary is a good source for such definitions. If a data dictionary is not available, a record layout may contain the needed definitions.

Developing Flowchart Diagrams

Inputs from which flowcharts are prepared should include copies of the following:

- Narrative descriptions of all major application systems
- All manually prepared source documents that affect application processing as well as corresponding coding sheets and instructions for data transcription
- Record layouts for all major computer input and output records, computer master files, and work files (such as update or file maintenance tapes and computation tapes)
- All major outputs produced by the application system
- Lists of standard codes, constants, and tables used by the application

These documents, along with the information developed in the previous tasks, should enable the audit staff to prepare a detailed and well-understood flowchart.

Evaluating the Quality of System Documentation

On the basis of user and IT staff inputs, as well as on the degree of difficulty experienced in constructing a flowchart, the auditor should be able to comment on the quality of system documentation. There are two basic questions to answer: Is the documentation accurate? Is the documentation complete?

To illustrate, if a federal auditor was examining control issues at a U.S. Navy computer facility, he or she might use the *Federal Information Systems Controls Audit Manual* (FISCAM) from the U.S. Government Accountability Office (GAO). This publication provides a basis for assessing the compliance of information system controls to federal guidelines.

Assessing Controls over Documents

Control points on the flowcharts should be identified and evaluated. By reviewing a diagram of this type, the auditor can determine whether controls have been used and if so, highlight

gaps, strengths, and weaknesses within the system. Identified controls, including automated and IT dependent application controls, should be adequately designed and implemented in order to mitigate risks. They should also be assessed to determine whether they address potential misstatements, or prevent/detect unauthorized transactions that could result in a materially misstated financial statements. An example of a common control includes the three-way match verification between the vendor's invoice, purchase order, and reconciliation report that is performed by the system as confirmation before payment is released. Other examples of controls include performing verifications and approvals, as well as configuring the system to identify transactions falling outside defined tolerable ranges. If these transactions are identified, an adequate control would prevent their processing.

Determining the Effectiveness of Data Processing

The audit staff should determine how effective data processing is by identifying problem areas, such as the ones below, in the processing cycle:

- Redundant processing of data or other forms of duplication
- Bottleneck points that delay or congest processing
- Points in the operating cycle at which clerks do not have enough time to review output reports and make corrections

Upon identification, the auditor should make recommendations on how to address these problem areas.

Evaluating the Accuracy, Completeness, and Usefulness of Reports

The audit staff should review key or major outputs (e.g., edit listings, error listings, control of hour listings, etc.) of the financial application system and determine if the outputs are accurate, complete, and useful as intended. The auditor should confirm the accuracy, completeness, and usefulness of the generated reports by interviewing appropriate users. One suitable technique might be the completion of a questionnaire or survey, perhaps conducted by e-mail, on user satisfaction with output reports.

Appropriateness of Flowcharting Techniques

A distinction should be noted between the use of flowcharts in computer auditing and in the broader field of systems analysis. In recent years, systems analysts have begun to favor other methods of modeling and documentation. DFDs, for example, are often preferred over flowcharts for purposes of analysis (see Exhibit 4.1). As stated earlier, DFDs are process-oriented and emphasize logical flows and transformations of data. By contrast, flowcharts emphasize physical processing steps and controls. It is just this type of control-oriented view, however, that is the auditor's primary focus. Thus, although the use of flowcharting may be declining for systems development purposes, this modeling tool remains important for IT auditors.

Flowcharting is not necessarily always the most practical approach for the auditor. Existing documentation including DFDs, narratives, or descriptions of programs in pseudocode may be used as points of departure. Based on a review of existing documentation, the auditor can decide

Computer-Assisted Audit Techniques (CAATs)

Another type of software techniques used in IT audits is CAATs. As mentioned in an earlier chapter, the American Institute of Certified Public Accountants issued SAS No. 94, "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit." This SAS does not change the requirement to perform substantive tests on significant amounts but states, "It is not practical or possible to restrict detection risk to an acceptable level by performing only substantive tests." When assessing the effectiveness of the design and operation of IT controls, it is necessary for the auditor (IT or financial auditor) to evaluate and test these controls. The decision to evaluate and test is not related to the size of the organization but to the complexity of the IT environment.

CAATs can be used by both IT or financial auditors in a variety of ways to evaluate the integrity of an application, determine compliance with procedures, and continuously monitor processing results. IT auditors, for instance, review applications to gain an understanding of the controls in place to ensure the accuracy and completeness of the information generated. When adequate application controls are identified, the IT auditor performs tests to verify their design and effectiveness. When controls are not adequate, IT auditors perform extensive testing to verify the integrity of the data. To perform tests of applications and data, the auditor may use CAATs.

Automated techniques have proven to be better than manual techniques when confronted with large volumes of information. The auditor, by using automated techniques, can evaluate greater volumes of data and quickly perform analysis on data to gather a broader view of a process. Common CAATs like ACL and Interactive Data Extraction and Analysis (IDEA) can be used to select a sample, analyze the characteristics of a data file, identify trends in data, and evaluate data integrity. Other techniques used for analyzing data include, for example, Microsoft Access and Microsoft Excel. Microsoft Access can be used to analyze data, create reports, and query data files. Microsoft Excel also analyzes data, generates samples, creates graphs, and performs regression or trend analysis. SAP Audit Management (part of the SAP Assurance and Compliance Software that comes encapsulated with SAP GRC) also streamlines the auditing process by providing cost-effective alternatives to spreadsheets and manual tools.[*] SAP Audit Management facilitates the documentation of evidence, organization of working papers, and creation of audit reports. This technique also provides analytical capabilities to shift the focus of audits from basic assurance to providing insight and advice.[†]

A large part of the professional skills required to use CAATs lies in planning, understanding, and supervising (e.g., SAS No. 108—Planning and Supervision, etc.) these audit techniques, and conducting the appropriate audit functions and tests. The computer has a broad range of capabilities. By way of illustration, three broad categories of computer auditing functions can be identified:

- Items of audit interest
- Audit mathematics
- Data analysis

[*] www.complianceweek.com/blogs/grc-announcements/sap-delivers-new-audit-management-tool-for-internal-audit-teams#.WEhtkE0zW72.

[†] https://www.sap.com/products/audit-management.html.

Items of Audit Interest

The auditor can use the computer to select items of interest, such as material items, unusual items, or statistical samples of items by, for instance, stipulating specific criteria for the selection of sample items, or by stating relative criteria and let the computer do the selection.

An example of selection by specific criteria might be a specification that the computer identifies all transactions of $100,000 or more and prepares a report including such transactions for audit review. However, the auditor could take a relative approach and instruct the computer to select the largest transactions that make up 20% of the total dollar volume for a given application. This approach abridges manual audit procedures because the auditor can rely on the computer's selection of items of interest. If computers were not used, the auditor would have to validate the selection process. Under traditional approaches, for example, it would be common for an auditor to ask organization or client personnel to list all transactions of $100,000 or more. With the computer, the auditor can be satisfied that the CAAT used has looked at the total universe of accounts payable items, for example. The validation of the selection process is inherent in the auditor's developing and accepting the computer-auditing application program.

Audit Mathematics

Performing **extensions** or **footings** can be a cost-effective payoff area for the application of computers in auditing—particularly if the calculations can be performed as a by-product of another audit function. For example, suppose the computer is being used to select significant items from an accounts receivable file. In the process of looking at this file, the computer can be programmed to extend and foot all invoicing transactions. Because of the speed of the computer, these calculations can be performed on 100% of the items in a file with no significant addition of time or cost for this processing.

By contrast, extensions and footings are both tedious and costly under conventional manual examination techniques. Typically, the auditor must limit examination of any given application to extension and footing of a judgmental sample covering a few short intervals of the period under examination. Clearly, reliance can be far higher when these verification calculations are performed on complete files.

Remember, however, that the computer has limitations in this area. Although it can be programmed to make many logical comparisons and tests, the computer cannot supplant human judgment in examining items to be tested.

Data Analysis

Using the computer for analysis of data represents a major opportunity for innovation by the auditor. The computer can compare and summarize data and can represent data in graphic form. Data analysis programs use techniques such as:

- Histograms
- Modeling
- Comparative Analysis

Histograms are bar charts showing graphic relationships among strata of data. In computer-assisted auditing, histograms typically represent graphic frequency distributions of records within

CAATs for Sampling

Some audit techniques assist in defining sample size and selecting the sample. For example, ACL automatically calculates the sample size and selects a sample from a population. Spreadsheet applications also generate random numbers for selecting a sample. There are two types of sampling techniques:

- *Judgmental sampling*: The sample selected is based on the auditor's knowledge and experience. The judgment may be to select a specific block of time, geographic region, or function.
- *Statistical sampling*: The sample is randomly selected and evaluated through the application of the probability theory.

Both methods allow the auditor to project to the population. However, only statistical sampling allows the auditor to quantify the risk that the sample is not representative of the population. The specific method selected for a sample will depend on the audit objectives and the characteristics of the population. The appropriateness of the method selected should be reviewed for validity purposes by statistical or actuarial staff with expertise in this area. Also, the applied sampling method should be revisited and reassessed over time to see if there is any change to the characteristics or attributes of the population under review. Two common statistical sampling methods are: Random Attribute Sampling and Variable Sampling.

Random Attribute Sampling and Variable Sampling

Random attribute sampling is a statistical technique that tests for specific, predefined attributes of transactions selected on a random basis from a file. Attributes for which such testing is done could include signatures, account distribution, documentation, and compliance with policies and procedures. To perform attribute sampling, the auditor must specify three parameters that determine sample size:

1. Estimate the "expected error rate," or estimated percentage of exception transactions, in the total population.
2. Specify the required "precision," or degree of accuracy desired, of the sample conclusion to be made.
3. Establish an acceptable "confidence level" that the conclusion drawn from the sample will be representative of the population.

The size of the sample will be determined by the combination of the expected error rate, precision, and confidence level parameters.

Variable sampling is another statistical technique that estimates the dollar value of a population or some other quantifiable characteristic. To determine the sample size using variable sampling, the auditor must specify four parameters:

1. Acceptable "confidence level" that the conclusion drawn from the sample will be representative of the population.
2. Absolute value of the "population" for the field being sampled.
3. "Materiality" or maximum amount of error allowable in the population without detection.
4. "Expected error rate" or estimated percentage of exception transactions in the total population.

CAATs for Application Reviews

There is a variety of CAATs that are useful when auditing applications and data integrity. An example of such techniques includes generalized audit software. Generalized audit software can be used to analyze spreadsheet logic and calculations for accuracy and completeness, evaluate data produced from applications (residing in databases), and produce logical data flowcharts, among others. In auditing databases, for example, techniques related to data mining can search "through large amounts of computerized data to find useful patterns or trends."* Data mining techniques help analyzing data from different perspectives and summarizing it into useful information. Another related example include data analytics (DA), or procedures to examine raw data in order to draw conclusions. DA is used in many industries to allow for better decision making, and in science to verify or disprove existing models or theories.† DA differentiates from data mining by the scope, purpose, and focus of the analysis. Data mining sorts through huge amounts of data using sophisticated software in order to identify undiscovered patterns and establish hidden relationships. DA, on the other hand, focuses on the process of deriving a conclusion (or inferring) based solely on what is already known.

Generalized audit software makes it possible to perform required functions directly on application files as it uses auditor-supplied specifications to generate a program that performs audit functions. Financial auditors, for example, use generalized audit software to:

- Analyze and compare files
- Select specific records for examination
- Conduct random samples
- Validate calculations
- Prepare confirmation letters
- Analyze aging of transaction files

IT auditors also use these software techniques for testing and/or documentation of selected processes within the IT environment in the form of flowcharts, and data flow diagrams, for instance. Generalized audit software allow IT auditors to evaluate application controls as well as query and analyze computerized data for substantive audit tests, among others. Some of the most popular software packages include Audit Analytics by Arbutus Software, TopCAATs, CaseWare Analytics IDEA Data Analysis, Easy2Analyse, TeamMate, and ACL. These are all virtually similar in regards to functionality. The ACL software package is described below as an example of what these techniques can do.

Audit Command Language (ACL)

ACL is a general audit software that reads from most formats (e.g., databases, delimited files, text files, Excel files, etc.) and provides data selection, analysis, and reporting. More specifically, ACL is a file interrogation tool designed to assist the audit of applications as it can handle and process large amounts of data. ACL functions range from: (1) identifying negative, minimum, and maximum balances; (2) performing statistical sampling and aging analyses; (3) identifying duplicates

* www.merriam-webster.com/dictionary/data%20mining.
† http://searchdatamanagement.techtarget.com/definition/data-analytics.

Exhibit 4.9 (*Continued*) ACL Commands Commonly Used in Performing Data Analyses

ACL Command	*Description*
Look for Duplicates	Detects whether key fields in the current table contain duplicates in the sequence.
Sampling	ACL offers many sampling methods for statistical analysis. Two of the most frequently used are record sampling (RS) and monetary unit sampling (MUS), both created from a population within a table. Each method allows random and interval sampling. MUS extracts sample records from a data set. MUS is typically used if the file is heavily skewed with large value items. RS, on the other hand, treats each record equally, using a nominal value of one. RS is used when records in a file are fairly evenly distributed across data, resulting in each record having an equal chance of being selected. The choice of methods will depend on the sampling overall purpose as well as the composition of the file being audited.

When planning for an ACL data analysis project, it is important for IT auditors to follow the steps below:

- Step 1: Acquiring the data
- Step 2: Accessing the data
- Step 3: Verifying the integrity of the data
- Step 4: Analyzing and testing the data
- Step 5: Reporting findings

Step 1: Acquiring the Data

The auditor must be aware of the data he or she requires to meet the goals of the specified project. For this, the auditor should gather the necessary information by meeting with various organization and/or client personnel, including, but not limited to, IT, MIS, and/or accounting or finance personnel to understand the data, its size, format, structure, and required data fields.

Step 2: Accessing the Data

The auditor must become familiarized with the data he/she is about to work with, particularly, the file where the data are stored, the file's structure, format, layout, size, data fields, number of records, etc. The auditor must assess the data included within the file in order to determine which data analysis task should be used and what platform or environment.

Step 3: Verifying the Integrity of the Data

The auditor must ensure that data are good data. In other words, the data that are to be analyzed must be valid, accurate, and complete, particularly, when working with data files that are not organized in records. ACL provides tools such as count, total, and verify to deal with these types of data files.

Step 4: Analyzing and Testing the Data

Data to be analyzed and tested can be of any size, format, and from almost any platform. Auditors use ACL to evaluate and transform such data into meaningful information that can assist their decisions-making process. There are several ACL commands that are commonly used when performing these types of data analyses and tests (refer to Exhibit 4.9). Appendix 4 also shows best practice audit procedures when using ACL to perform, for example, testing on accounting journal entries.

Step 5: Reporting Findings

Upon completing performing data analyses and tests, IT auditors must present and communicate their results and findings in an easily readable format. As part of reporting the results, auditors must maintain file layouts and ACL projects for backup purpose and to allow recreation, if necessary. Auditors must include ACL-related information in the audit work papers, including, but not limited to, copy of ACL program, ACL logs/file layouts, and data requests for future year audits.

CAATs for Auditing Application Controls

When auditing application controls, auditors examine input, processing, and output controls specific to the application. Application controls are also referred to as "automated controls." Automated input controls validate the data entered in the system, and minimize the chances for errors and omissions. Examples of input controls include checking for: characters in a field; appropriate positive/negative signs; amounts against fixed/limited values; amounts against lower and upper limits; data size; and data completeness, among others. Processing controls are those controls that prevent, detect, and/or correct errors while processing. Examples of processing controls include matching data before actions take place (e.g., matching invoice amount against purchase order and receiving report, etc.), recalculating batch totals, cross-footing data to verify accuracy of calculations, and ensuring that only the correct and most updated files are used. Output controls detect errors after processing is completed. Examples of output controls include performing report data reconciliations (e.g., general ledger with subsidiary ledgers, etc.), reviewing reports for accuracy and completeness (e.g., performing comparisons of key data field, checks for missing information, etc.), and protecting the transfer of data to ensure data are being transmitted completely and adequately (e.g., encryption, etc.).

CAATs come very handy to the auditor when evaluating application controls related to the processing of transactions. As described above, controls regarding the processing of transactions are concerned with the accuracy, completeness, validity, and authorization of the data captured, entered, processed, stored, transmitted, and reported. Auditors typically work with organization- or client-provided spreadsheets and/or databases when performing their procedures. Application controls found on spreadsheets and/or databases that are commonly tested by auditors include checking for mathematical accuracy of records, validating data input, and performing numerical sequence checks, among others. Auditors must ensure these types of controls are effectively implemented to ensure accurate results.

Spreadsheet Controls

Spreadsheets may seem to be relatively straightforward because of their widespread use. However, the risks presented are significant if the spreadsheet results are relied on for decision making.

Lack of reliability, lack of auditability, and lack of modifiability are all risks that are associated with poor spreadsheet design. Auditors use CAATs to assess client- or organization-prepared spreadsheets for analyzing their data and ultimately forming opinions. Controls should be implemented to minimize the risk of bad data and incorrect logic, particularly, if spreadsheets are reused. Some of the key controls that minimize the risks in spreadsheet development and use include:

- *Analysis.* Understanding the requirements before building the spreadsheet
- *Source of data.* Assurances that data being used are valid, reliable, and can be authenticated to originating source
- *Design review.* Reviews performed by peers or system professionals
- *Documentation.* Formulas, macro commands, and any changes to the spreadsheet should be documented externally and within the spreadsheet
- *Verification of logic.* Reasonableness checks and comparisons with known outputs
- *Extent of training.* Formal training in spreadsheet design, testing, and implementation
- *Extent of audit.* Informal design reviews or formal audit procedures
- *Support commitment.* Ongoing application maintenance and support from IT personnel

Database Controls

Department databases should be protected with controls that prevent unauthorized changes to the data. In addition, once the database is implemented, it should be kept in a separate program directory and limited to "execute only." The database can also be protected by enabling "read-only" abilities to users for data that remain static. Access rights should be assigned to specific users for specific tables (access groups). The input screens should include editing controls that limit data entry to valid options. This can be accomplished by having a table of acceptable values for the data fields. Data accuracy can also be enhanced by limiting the number of free-form fields and providing key entry codes with lookup values for the full description. Controls that auditors commonly expect to identify (and ultimately assess) within client or organization-prepared databases include:

- *Referential integrity.* Prevent deleting key values from related tables
- *Transaction integrity.* Restore value of unsuccessful transactions
- *Entity integrity.* Create unique record identification
- *Value constraints.* Limit values to a selected range
- *Concurrent update protection.* Prevent data contention
- *Backup and recovery protection.* Ability to back up critical information and applications and restore to continue
- *Testing protection.* Perform tests at the systems, application, and unit level

CAATs for Operational Reviews

Earlier, we covered a number of techniques used for performing tasks to support the audit of applications. Most of these techniques can be used to support operational reviews as well as collect information about the effectiveness of general controls over IT operations. However, the use of techniques need not be limited to specialized packages. Computer languages can be useful in

performing operational tests and collecting information about the effectiveness of general controls. Even basic tools such as Access in MS Office can be used to take an imported data file of operational data (e.g., users' account information and file accesses, rights to number of file accesses, etc.), perform analysis on the file (histograms, frequencies, summaries), and then move data into MS Excel and visually portray information for management or even forecast trends with regard to workload, growth, and other IT operational areas.

The focus of an operational review is on the evaluation of effectiveness, efficiency, and goal achievement related to information systems management operations. Basic audit steps in an operational review are similar to IT audits or financial statement audits, except for the scope. Specific activities in an operational review include:

- Review operating policies and documentation
- Confirm procedures with management and operating personnel
- Observe operating functions and activities
- Examine financial and operating plans and reports
- Test accuracy of operating information
- Test operational controls

Auditing Around the Computer Versus Auditing Through the Computer

There may be situations in the IT environment where *auditing around the computer* or "black box auditing approach" may be more adequate than *auditing through the computer* when automated applications are relatively simple and straightforward. When performing *auditing around the computer*, the auditor obtains source documents that are associated with particular input transactions and reconciles them against output results. Hence, audit supporting documentation is drawn and conclusions are reached without considering how inputs are being processed to provide outputs. Unfortunately, SAS No. 94 does not eliminate the use of this technique. The major weakness of the *auditing around the computer* approach is that it does not verify or validate whether the program logic of the application being tested is correct. This is characteristic of the *auditing through the computer* approach (or the "white box auditing approach").

The *auditing through the computer* approach includes a variety of techniques to evaluate how the application and their embedded controls respond to various types of transactions (anomalies) that can contain errors. When audits involve the use of advanced technologies or complex applications, the IT auditor must draw upon techniques combined with tools to successfully test and evaluate the application. This audit approach is relevant given technology's significant increase and its impact on the audit process. The techniques most commonly used include integrated test facility, test data, parallel simulation, embedded audit module, systems control audit review file (scarf), and transaction tagging. Again, many of these techniques should be embedded into the application for use by auditors and information security personnel. These techniques provide continuous audit and evaluation of the application or systems and provide management and the audit or security personnel assurances that controls are working as planned, designed, and implemented. These are described, with their advantages and disadvantages, in Exhibit 4.10.

Computer Forensics Tools

Computer forensics is the examination, analysis, testing, and evaluation of computer-based material conducted to provide relevant and valid information to a court of law. Computer forensics tools are increasingly used to support law enforcement, computer security, and computer audit investigations.

A good source for evaluating computer forensics tools is the Computer Forensics Tool Testing (CFTT) Project Website at www.cftt.nist.gov/. CFTT is a joint project of the NIST, the U.S. Department of Justice's National Institute of Justice (NIJ), the Federal Bureau of Investigation (FBI), the Defense Computer Forensics Laboratory (DCFL), the U.S. Customs Service, and others to develop programs for testing computer forensics tools used in the investigation of crimes involving computers.

One tool recently reviewed by the CFTT was EnCase Forensics by Guidance Software, Inc. EnCase enables "noninvasive" computer forensic investigations, allowing examiners to view relevant files including "deleted" files, file slack, and unallocated space. Other valuable resources for experience in the use of computer forensics tools would be those professional associations or organizations that support this area. Some of those would be The International High Technology Crime Investigators Association, Association of Certified Fraud Examiners, the Institute of Internal Auditors, Federal Government's Electronic Crimes Task Force, FBI Regional Computer Forensics Laboratory, and the Colloquium for Information Systems Security Education. Note that when applying computer forensics tools, one must be aware of the investigative methodology, processes, and procedures that must be followed to ensure that the evidence can be gathered successfully, documented, and not contaminated as evidential matter that could be used in court. An excellent resource here is the U.S. Department of Justice publication, *Prosecuting Computer Crimes* (2nd edition) published in 2010, as well as information provided by the High Tech Criminal Investigation Association (www.htcia.org).

Conclusion

The continued evolution of IT has placed advanced (software) features in the hands of IT auditors to apply in support of conducting, documenting, and executing the audit process. These software tools and techniques allow the auditor to apply innovative approaches to validating processes at the applications level.

Auditor productivity tools, for instance, include software to automate the audit function and integrate information gathered as part of the audit process. These tools allow auditors to reduce the amount of time spent on administrative tasks. System documentation techniques are also very common, and are mainly used to document and test application systems, IT processes, and their integration within the IT environment. Flowcharts, data flow diagram, and business process diagrams are good examples of system documentation techniques. Lastly, CAATs assist auditors when assessing application controls, and selecting and analyzing computerized data for substantive audit tests.

CAATs can be used by IT and/or financial auditors, in a variety of ways, to define sample size and select samples, determine compliance with procedures, and continuously monitor processing results. IT auditors, for instance, use CAATs to review applications in order to gain an understanding of the controls in place to ensure the accuracy and completeness of the information generated.

Auditors use generalized audit software (a type of CAAT) to evaluate the integrity of applications. Generalized audit software allows auditors to analyze and compare files, select specific records for examination, conduct random samples, validate calculations, prepare confirmation letters, and analyze aging of transaction files, among others. Some of the most popular generalized audit software include Audit Analytics by Arbutus Software, TopCAATs, CaseWare Analytics IDEA Data Analysis, Easy2Analyse, TeamMate, and ACL. These are all virtually similar in regards to functionality.

The ACL software package, described in this chapter, is a file interrogation tool designed to read data from most formats (e.g., databases, delimited files, text files, Excel files, etc.) and to provide data selection, analysis, and reporting. ACL handles and processes large amounts of data in order to identify negative, minimum, and maximum balances; perform statistical sampling and aging analyses; identify duplicates or gaps in sequence testing; and perform comparative joining and matching.

CAATs are also used when conducting operational reviews and as a computer forensic tool. An operational review focuses on the evaluation of effectiveness, efficiency, and goal achievement related to information systems management operations. As a computer forensic tool, auditors examine, analyze, test, and evaluate computer-based material in order to provide relevant and valid information to a court of law. Computer forensics tools are increasingly used to support law enforcement, computer security, and computer audit investigations.

Review Questions

1. What are audit productivity tools? How do they assist auditors?
2. What are CAATs and what benefits they provide to IT auditors?
3. Describe the following system documentation techniques commonly used to understand financial application systems:
   a. Data flow diagrams
   b. Business Process Diagrams
   c. Flowcharts
4. List the steps required in the development of flowcharts.
5. CAATs are known to assist auditors in defining sample size and selecting a sample for testing purposes. Describe two techniques used by CAATs to define sample size and select the sample.
6. What is the audit command language (ACL) audit software? List the benefits it provides.
7. Explain the four steps to follow when planning for an ACL data analysis project.
8. Spreadsheet controls are one type of application controls used by auditors. List and describe five key spreadsheet controls.
9. What is the emphasis or focus of an operational review? List specific activities when performing an operational review.
10. What is computer forensics? What do computer forensic tools support? How do you think computer forensic tools may assist the IT auditor?

Exercises

1. List and describe three broad categories of computer auditing functions IT professionals use to support the audit of an application. Explain their application.

After a formal review, the Change Control Board may:

- Reject the change (the reasons for the rejection are notified back to the Change Requester)
- Request more information related to the change
- Approve the change as requested or subject to specified conditions

Once approved, the Change Control Board forwards the change and any related supporting documentation to the Implementation Team.

ROLE: IMPLEMENTATION TEAM

The Implementation Team schedules and tests the approved change. If test results are not successful, the change and all related supporting documentation are sent back for re-testing. If results are successful, the Implementation Team formally implements the change, and notifies the Change Requester.

TASK: Prepare a flowchart depicting the change control management process just described. Make sure you segregate the roles (i.e., Change Requester, Project Manager, Change Control Board, and Implementation Team) in vertical columns when creating the flowchart to illustrate the procedures performed in the process. This representation is useful for auditors to evaluate segregation of duties and identify incompatible functions within the process.

Further Reading

1. AICPA. Audit analytics and continuous audit—Looking toward the future, www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/AuditAnalytics_LookingTowardFuture.pdf (accessed August 2017).
2. AICPA. (2007). *Information Technology Considerations in Risk-Based Auditing: A Strategic Overview*, Top Technology Initiatives. New York: American Institute of Certified Public Accountants (AICPA).
3. Barbin, D. and Patzakis, J. (2002). Cybercrime and forensics. *IS Control J*., 3, 25–27.
4. Bates, T. J. (2000). Computer evidence—Recent issues. *Inf. Sec. Tech. Rep.*, 5(2), 15–22.
5. Braun, R. L. and Davis, H. E. (2003). Computer-assisted audit tools and techniques: Analysis and perspectives.*Manage.Audit.J.*,18(9),725–731.www.emeraldinsight.com/doi/full/10.1108/02686900310500488
6. Cerullo, V. M. and Cerullo, M. J. (2003). Impact of SAS No. 94 on computer audit techniques. *IS Control J*., 1, 53–57.
7. Computer Forensic Tool Testing (CFTT) Project Website, National Institute of Standards and Technology, www.cftt.nist.gov/ (accessed March 2017).
8. Deloitte, LLP (2014). *ACL for Auditors*. Unpublished internal document.
9. Deloitte, LLP (2014). *IT Audit Planning Work Papers*. Unpublished internal document.
10. EY's ten key IT considerations for internal audit—Effective IT risk assessment and audit planning. (February 2013). Insights on Governance, Risk and Compliance, www.ey.com/Publication/vwLUAssets/Ten_key_IT_considerations_for_internal_audit/$FILE/Ten_key_IT_considerations_for_internal_audit.pdf
11. Gallegos, F. (2001). *WebMetrics: Computer-Assisted Audit Tools*, EDP Auditing Series, #73-20-50, Auerbach Publishers, Boca Raton, FL, pp. 1–16.
12. Gallegos, F. (2002). *Personal Computers in IT Auditing*, EDP Auditing, #73-20-05, Auerbach Publishers, Boca Raton, FL, pp. 1–7.