CHAPTER 2

Audit Technology

Information technology is not only all-pervasive, it is also critical to auditors who must analyze data and information and report on them. This is especially true when much of the essential data and information is accessible only by computers. This chapter illustrates the audit technology continuum, identifies general software useful for auditors, introduces specialized audit software, and describes software helpful for audit management and administration.

Audit Technology Continuum

The use of computer technology in auditing is not consistent across companies or even within organizations with branch operations and separate audit groups. Some audit organizations are leaders in adopting, and deriving the maximum benefit from, new technologies. Others are taking a more cautious approach to implementing the new technology. Many organizations exist somewhere in the middle of what can be called the audit technology continuum.

An audit organization's place on this continuum is based upon the degree to which auditors and audit management have integrated the use of CAATTs into their audit operations. There are four distinct regions along the continuum: introductory, moderate, integral, and advanced. The regions can be characterized according to the degree to which general software, audit software, and audit management and administrative software are used. This is illustrated in Exhibit 2.1, Audit Technology Continuum, and subsequently explained with a view to assisting auditors in achieving the more advanced stage of using information technology in auditing.

Introductory Use of Technology

Audit organizations at the introductory stage of the continuum have not really begun to employ computer-based audit tools and techniques. Typically,

EXHIBIT 2.1 Audit Technology Continuum

Introductory	Used by audit management Administration: budgeting, time reporting, and text processing
Moderate	Used by limited number of individual auditors Data extraction and analysis for a few audits; limited use of spreadsheets and presentation software
Integral	Used by all auditors and audit management All audits, all phases, to define the audit universe and annually identify and assess risk; electronic working papers and distribution of audit reports
Advanced	Used by all auditors and audit management Continuous auditing for ongoing identification and assessment of risk and to perform assurance audits; extensive use of intranet

automation has been on the periphery of the main audit functions. The efforts have focused on automating basic audit tasks rather than addressing new or different requirements. Examples include e-mail, word processing for preparing audit reports and working papers, and spreadsheets for managing the audit division's budget. The audit process has not changed, nor have any of the inputs to, or outputs from, the audit process. The audit organization has failed to see how important technology is and how it can help. Coincidently, the audits performed are also most likely to be the traditional "tick-and-bop" efforts, relying on manual file reviews, rather than more comprehensive audits.

While organizations at the introductory stage of the continuum have accrued some benefits from the use of computer technology, most audit-related tasks are still performed manually. Such audit management does not have a plan that will see the organization taking the next step in supporting the audit function with technology. Technology is not anticipated, planned for, or considered in either the short- or long-range plans of the audit organization. Any use of technology is piecemeal and usually only intended to deal with one problem, one functional area, or one specific audit.

Moderate Use of Technology

In a growing number of audit organizations, technology is having an impact on the actual audits being conducted. However, this impact is still somewhat limited. Technology is not used by all audits, nor is it consistently applied or managed in a centralized manner. Often, only one or two auditors are making use of specialized audit software, and their efforts may not be sponsored or sanctioned by audit senior management. In many cases, management may not even be aware of the type, or extent of the use, of

automated tools and techniques by these auditors. Even in cases where data extraction tools are used with management's knowledge and consent, it may only be used to select a sample of transactions. The resulting records are then manually reviewed rather than analyzed electronically.

The types of audits performed, the results achieved, and the methodology employed have not changed, only the tools used to perform the functions necessary to deliver the final report. If there are a sufficient number of successful examples of the application of automated tools and techniques, the audit organization may move to the next stage on the continuum. However, since there is no focus on the use of technology and no vision for where the organization's use of technology is going, there is a risk that minor setbacks will alter management's view of CAATTs and the initiative will falter. Further, the application of technology is still isolated to specific tasks rather than integral to the entire audit function. The future of CAATTs may lie with an informal group of users, without management's backing or guidance; however, these individuals may become frustrated and move on to other opportunities. As a result, the modernization of the audit function may fail to come to fruition. Also, in audit organizations that emphasize a rotation of staff through internal audit, the expertise may quickly be lost before plans can be made to ensure that the expertise is passed on to others so it can be expanded.

Integral Use of Technology

At this point on the audit technology continuum, the technology is recognized by audit management as the way of the future, and resources have been assigned to continue to develop its use and integration within the audit function. Technology has successfully been used to improve some of the basic components of the audit process. To a certain extent, the inputs to, and the outputs from, the audit process have changed through the use of computer-based tools and techniques. Computers are used in more sophisticated ways to improve the efficiency and effectiveness of the audit process. Some examples of these are:

- Extraction and analyses of client data in support of specific audit objectives
- Automation of the administrative functions of the audit organization, such as time reporting and billing, audit planning, risk analysis, and project management
- Establishment of an electronic library of audit-related reference materials (policies, procedures, federal statutes)

- Automation of working papers and cross-referencing of source documents, possibly including the development of a corporate intranet with hypertext links
- Development of databases summarizing several years worth of client data for critical or key information systems to be used for trend analysis, audit planning, or early-warning systems

In particular, the use of technology is managed and encouraged in all phases of audits and for the administration of the audit function. Audit senior management has formalized the use of computer technology and has a vision for the future of CAATTs. An effort is being made to do more than simply automate current processes and tasks that had previously been performed manually. CAATTs are factored into the organization's business plan, and resources (time and money) have been set aside to ensure the continued development of new and innovative tools and techniques for audit in order to provide the added value that should be expected of modern auditing.

Advanced Use of Technology

At the advanced stage of the continuum, technology is changing not only the way audits are conducted, but also the types of audits undertaken. Audit organizations become involved in the design and development of new and innovative uses of technology such as self-auditing systems, which continuously review transactions. Once audit functions become part of a system, auditing will become a continuous process that identifies anomalies based on predefined, audit-determined criteria. Audit tools that are highly integrated with the company's information systems could be used to perform audit procedures simultaneously with the company's processes and controls (Canadian Institute of Chartered Accountants [1999]).

For example, the comparison of customers' current long-distance usage to their typical calling patterns can detect possible calling card theft before the owner is even aware of the loss. Other examples include trend analysis on credit card purchases or the comparison of the profitability level for a division to other divisions in other plants, after being normalized for various factors that might affect costs. The results of these comparisons are used as red flags by audit management to help determine what will be audited and when. Continuous auditing of key information systems allows auditors to use data-driven indicators to identify and assess risk in support of the development of the annual audit plan. In addition, auditors can review potential problems before they become serious, with red flags raised and investigated for causes, and recommendations made in real time rather than months after the fact.

At this point on the technology continuum, the nature of the audit function is substantially different. The inputs, outputs, and processes of a typical audit are not the same as that of an organization that has not embraced automation in audit. To a large degree, the types of audits conducted, the planning cycle and cycle time, and many other functions will also be affected by the implementation of advanced tools and techniques. Information technology is utilized to the fullest extent in order to maximize the benefits of the audit to the audited organization.

Getting There

Very few organizations are at the advanced stage of the audit technology continuum, and not every organization can expect to reach this point in the short term. However, substantial benefits in terms of efficiency and effectiveness can be gained by auditors using specialized audit software. For example, the increased use of analytical review can aid in the prevention and detection of fraud (Pacini and Brody [2005]). Most organizations can improve upon their use of computer-based tools and techniques and maximize their return on the investment in computer technology.

There need not be a large internal audit organization within the company in order to use the computer more effectively as an audit tool. Nor is it necessary to have a lot of dedicated computing resources such as powerful hardware, sophisticated software, and highly trained programming professionals. In fact, many steps can be taken to produce significant benefits at a minimal cost.

The remainder of this chapter describes various uses of technology. Most of the uses are typical of the moderate to integral stages on the continuum. The examples range from the more intelligent use of the features available in word processing software to expert systems. Most do not require the development of audit-specific applications, the generation of test decks, the embedding of audit modules into existing application systems, or the use of advanced programming techniques.

These tools and techniques can be implemented one at a time, on a stand-alone workstation or on a local area network (LAN). It is strongly suggested that the audit organization choose what will work best, starting with the tools and techniques that will produce the greatest payback. But, keep in mind that the degree to which the organization has adopted automation is a factor that auditors must consider when implementing automation in audit (EDP Auditors Association, Toronto Area Chapter [1990]).

The examples of CAATTs begin with general software that can be most easily implemented, producing immediate results. The examples of specialized audit software may require more familiarity with audit technology and

support the application of more advanced and sophisticated approaches to auditing without being technologically difficult.

General Software Useful for Auditors

The use of technology by auditors requires not only a change in the mind-set of auditors, but also a degree of comfort and familiarity with the technology and the concepts. The use of general software to support audit, such as text processing, spreadsheet, and graphics, while beneficial in its own right, will also introduce auditors to more relevant technology. The following section discusses general software useful for audit with nontypical uses of these packages from an audit perspective. Even if the organization is going to remain at the moderate stage of the continuum, the auditor can make better use of the technology already available. Simple word processing software can become more than a text processor and more integral to the audit function when looked at from a different perspective.

Word Processing

All writing is carried out with one aim in mind: to communicate an idea or fact to the reader. One of the main functions of audit is to report the results of audit reviews and to communicate opinions on a variety of subjects. In order for this to be achieved effectively, we must capture the readers' attention. The auditor must be skilled in the techniques of writing to ensure that the messages are clear, concise, and readable. While the auditors may think that audit reports are clear and to the point, their view is not always shared by the readers. The clients will often criticize a report if it is too long-winded or difficult to follow. As a result, auditors must improve their writing style to make reports clear, concise, and readable. The first use of technology is quite simply the production of audit reports and working paper documentation using word processing software. Word processing software can help in improving writing skills.

A simple word processor allows the user to enter and manipulate textual information. It is a supportive typewriter, because most word processors provide much more functionality than an electronic typewriter. Edits, updates, and corrections can be made easily, and the electronic versions can be stored for future use in follow-up audits. Text can be reformatted on the screen to change the layout to the format the writer feels will have the greatest impact. The word processor allows the writer to manipulate the text using simple commands to copy, move, or delete the text as required. This speeds up the drafting process, as the entire document does not need to be retyped every time a correction is required. In addition, all members

of the audit team can be actively involved in the production of the final report. Members of the team can work on different chapters, and the overall document can easily be pulled together at a later date.

Many audit departments now provide auditors with laptops and portable microcomputers, which allow them to write the draft audit report in the field and be ready for its issue on their return. Draft reports can be edited using redline; document compare features can be used to identify the changes; and version control can be tightly maintained. Final reports will benefit from the flexibility and clarity of electronic formatting, laser printing, and the integration of text with graphics and even color printing. Further, word processors have the added advantage of exposing all auditors to the computer, as well as building confidence in technology.

Word processors are being packaged with a wider array of capabilities. Previously, many audit organizations found that management review comments focused on spelling errors rather than the issues raised in the report. This can be virtually eliminated by the spell-checking feature of many word processors. Spell-checking features, as well as reporting incorrectly spelled words, will also suggest alternative spellings. Further, the value of a report can be diminished by the repetition of particular words. Most word processors are also equipped with a thesaurus, a valuable tool for the auditor who needs to find other ways of saying discovered (e.g., detected, determined, learned, realized, uncovered, noticed, established, ascertained).

Word processors also have style (or grammar) checkers to assist in ensuring that audit reports are clear and concise. A style checker will analyze the readability of the text. Studies have shown that readable writing has common characteristics: sentence length, number of syllables per word, frequency of punctuation, and use of the active voice. However, the main use of this type of tool is as a check. Auditors must know what is required to produce readable reports at their organization. The checker can be used to analyze reports or highlight sentences that are too long and can be split into two or more sentences. They can also highlight long words with which the reader may not be acquainted or where a simpler word may suffice.

Many audit reports also suffer from being disjointed; the audit findings are not always written in a logical sequence, and major points are often hidden in a plethora of minor findings. An outliner can help to plan the structure of any document. The outliner (sometimes called a thought processor) is a text processor that allows the user to enter items as a list and then move these items around until they are in the best possible sequence. Items that are entered are automatically numbered, and the numbering sequence will change automatically as the list is rearranged. Many levels of detail can be supported, and when a high-level item is moved, the underlying details are also moved. Many word processors now include an outliner that can be used

to plan the structure of the entire document. The findings can be entered as a list of paragraph headings that can then be sorted until the best presentation sequence is found. The outline then can be transferred as a template to the word processor and the details can be typed into each paragraph.

Outliner software even can be used as an audit planning tool. The audit can be broken down into a series of distinct sections, and each section can be further broken down into a series of steps. This process can continue until the auditor is satisfied that all areas have been covered and can result in more structured audit programs.

Other possibilities for word processing software include the automatic production of confirmation letters using mail merge capabilities to improve the production efficiency and final look of the letters, and the use of standardized working paper, report formats, and templates to reduce the time required to format the final report. Further, standardization can make the automatic generation of preliminary findings and final reports easier to accomplish. Hypertext links can also be established between the final report and the audit program or detailed working papers. (This application of technology is discussed further in this chapter under Electronic Working Papers.)

The main problem with word processing software is that very few people use more than 25 percent of the power of the word processing packages. Capabilities such as spelling checkers, thesaurus, automatic paragraph numbering, and the generation of indexes and tables of contents, as well as grammar checking routines, can vastly improve the quality of the final report. However, they require an investment in training. Audit organizations are finding that the improvement in the quality of the correspondence more than outweighs the training costs to acquire more advanced skills.

Text Search and Retrieval

The majority of the output from any audit department is in the form of text. Reports and correspondence are produced within the department on a word processing package, and there is a considerable amount of text littering the hard disks. Usually, these documents are printed and maintained in manual filing systems, making retrieval more difficult. However, since the documents already exist in electronic format, there are better methods of storing and retrieving required information for follow-up audits or research.

Microsoft operating systems (XP, NT) and most word processors provide search capabilities, including the capability to search all files within a directory, or even an entire hard disk drive for a specific string of characters. However, there are now a considerable number of packages on the market that perform these functions with more speed and functionality. Text search and retrieval is achieved in two ways: (1) some packages index words in documents and can therefore perform fast searches of all files

for specific words or phrases, and (2) others carry out the scan of all files for the required text as the query is entered into the system. The indexing packages are obviously faster in operation, but have an overhead in storage requirements, as the indexes often take up as much space as the documents themselves. The pure search and retrieve packages are slower, but do not have any additional storage requirements. Both types of packages allow the user to retrieve all instances of a word or phrase.

For example, one architectural firm needed to find all correspondence where they had quoted a certain section of the building code in the last year and a half. This involved searching hundreds of proposals and letters. Manually, the search would have taken days and there would have been no guarantee that they found all references. Electronically, the search took only minutes and was 100 percent complete.

Document management software also can be used to manage electronic documents, even performing version control for draft audit reports.

Reference Libraries

The proper management of electronic documents can make them easier to control and retrieve—in short, more useful. In particular, audit programs or audit reports often contain information that might be relevant to future audits. Audit management should ensure that a document management program is enforced to protect the integrity of pertinent information.

A centralized reference library of company policies, procedures, previous audit reports, and methodologies, supported by text search and retrieval, provides auditors with easy access to historical information. Cut-and-paste capabilities can also allow auditors to use these electronic files during the planning phase to create new audit programs, to build background working papers, or as part of a follow-up audit of a client area.

The reference materials could contain just about anything—from specific legal statutes to generalized audit procedures. For example, modern audit software is designed such that standard audit programs can be developed to be repeatable and maintained and made available to all audit teams, improving their efficiency and effectiveness.

Further, reference materials that are fairly stable, such as company policies and procedures, could be written to CD-ROM and given to auditors for use with laptop computers when working at remote locations. Today, the organization's intranet often contains all up-to-date versions of policies and regulations and is accessible by all employees.

Spreadsheets

The spreadsheet started the revolution in the use of personal computers for business. Spreadsheet software gave users the ability to automate many

of the functions of business administration and accounting. An electronic spreadsheet is like an automated calculator that can work in two or more dimensions. A spreadsheet consists of rows and columns. The intersection of each row and column forms a cell, and these cells form the basis of the spreadsheet. They can contain text, numbers, formulae, or even programmed instructions (macros). Combinations of these types of cells can be used to build applications. Rows, columns, or blocks of data can be summed, sorted into sequence, moved to other locations, or copied. In addition, spreadsheets can be linked to other spreadsheets.

The spreadsheet format of data presentation is so natural that it has also been used by audit software to facilitate various views into any, and practically all, electronic data files and summarizations of the data in diverse ways. Other facilities offered by spreadsheet software include the capability to generate graphical representations of data, which is often the most effective way of showing data. The graphs either can be copied or hot-linked into audit reports, improving the understandability and presentation of the results. Spreadsheet software also includes simple commands and formulae to perform statistical functions such as cross tabulations (pivot table) and regressions (linear or nonlinear).

Spreadsheets can be used by audit management to track budgets or to record time and billing information. Some organizations have developed risk and materiality criteria and use spreadsheets to evaluate the audit universe in order to determine which audits to perform next. In fact, any audit process that involves the analysis of quantities of data or repetitive calculation can be made more efficient by using a spreadsheet. Where relationships exist between data items, these relationships can be checked by entering the data into a spreadsheet and writing a simple checking routine.

Audit packages, such as Spreadsheet Auditor and ExcelSmartTools Auditor, also have been written and can be used to verify the internal consistency of spreadsheets. These packages examine spreadsheets for circle references and other anomalies, and compare the basic layout and structure of the spreadsheet for good programming practices and will highlight all formulae. In addition, packages like XLAudit analyze spreadsheets to evaluate the required controls, errors in formulae, and mapping precedents and dependents.

Another concern for auditors is the error rate for spreadsheets, estimated at 2 to 4 percent of all formula cells. At that frequency, a material error in financial reporting is almost a certainty in spreadsheets of any reasonable size. Some of the risk related to spreadsheets include errors in downloading of corporate information—partial or out-of-date information; errors in spreadsheet calculations; inappropriate changes to the data or the spreadsheet logic; and invalid interpretations of the information (Institute of Internal Auditors (IIA), Sarbanes-Oxley Section 404 [2008]).

Studies have recommended that companies maintain a detailed inventory of their spreadsheets and implement a number of controls over changes, version, access, input, security, and data integrity (PricewaterhouseCoopers, Use of Spreadsheets, [2004]). This leads to a host of spreadsheet management software, promising to fill the many compliance holes inherent in typical spreadsheets.

Management and auditors now have numerous choices, including products such as Actuate, Cerity, Compassoft, ClusterSeven, Lyquidity, Mobius, Prodiance, Qtier, Sheetware, and Spreadsheet Advantage. These products generally include the ability to (1) track changes to spreadsheets, including changes that cross multiple spreadsheets; (2) create and maintain access and segregation of duties controls; (3) control versions; and (4) produce audit trails. Other features may include workflow, spreadsheet-development tools, spreadsheet archiving, and analytical reporting. Their overall goal is to combine the user-friendliness and widespread use of spreadsheets with a centralized control infrastructure—to reduce the likelihood of errors.

Presentation Software

The use of presentation software can help auditors deliver their message in an interesting and condensed format. In particular, presentation software can help improve the quality and utility of the exit debrief to the client. Concepts or recommendations that are complex are often more easily presented in graphical format rather than straight text. Graphics and the use of color can make audit reports more readable and understandable. Further, the appropriate use of graphics can focus the reader's attention on the audit findings and key recommendations. A number of audit organizations have introduced multimedia presentations to senior management. These presentations include audio and visual (digital pictures and movies) components.

Case Study 6: Audit Reporting

The audit team was given a 15-minute time slot for their briefing to the senior vice president. The facilities audit had taken more than six months to perform and had identified seven major recommendations and a number of minor findings. The detailed audit report was over 150 pages in length. Obviously, the auditors could not fully explain the entire audit to the senior vice president in the time allotted to them. However, using a graphics package, they produced ten full-color slides and incorporated a one-minute video of a particularly decrepit facility. The presentation covered the main points raised by the audit and highlighted the key results and recommendations. The senior vice president was sufficiently

concerned by the contents of the briefing that she asked for a more comprehensive report, at which point the audit team handed over the detailed audit report and a condensed executive summary. Had they not caught the attention of senior management, the detailed findings may never have been given the focus they deserved. The use of presentation software helped the audit team to maximize the time the vice president was able to spend with them.

Auditors should use graphics and video to assist the reader in understanding the text, not as a replacement for the written word. One of the temptations with presentation software is to stress form over substance. So, be warned, do not go overboard; too many fonts, pictures, or the use of sound and animation may distract from the main message of an audit.

Flowcharting

One of the tasks within any operational audit is to document business flows and procedures or to ensure that existing documentation is updated to reflect changes in the flows. Flowcharting is used as one technique that enables the auditor to analyze the procedures and identify controls (or the lack thereof). Updating and redrawing flowcharts used to be time-consuming, but now specialized flowcharting software is available to assist the auditor. As a result, it is much easier to change one symbol or flowline on a microcomputer and produce a new version than to erase or redraw it on paper. In addition, standards of flowcharting can be enforced more easily through the use of computer software.

There are packages that will follow any of the generally recognized flowcharting techniques. Therefore, auditors can produce audit flowcharts using the Rutterman standards, computer flowcharts, or even data flow diagrams. Some flowcharting software is even capable of transforming English constructs directly into a diagram.

Flowcharting software can be used to illustrate many relationships, such as organizational charts, flowcharts for computer software or applications, network diagrams, process flows, decision trees, and cause-and-effect relationships. The resulting diagrams can consist of one or more pages and can be automatically sized or resized. Many flowcharting packages contain standard templates for ease of use and offer online help.

Audit teams can use flowcharting software, such as Visio and Code Visual to Flowchart, to model the audit entity, making any revisions or updates easy to perform. Flowcharting critical processes can help identify key control points and can be used to produce process and data flow

diagrams. Of course, the flowcharts can be reused for the next audit of the client or for audits of similar operations.

Documenting process flow has proved to be one of the most important steps in Sarbanes-Oxley compliance because it provides the foundation for all subsequent work (Kendall [2004]). While maintaining this documentation is also costly, audit teams can use flowcharting software, such as Visio and Code Visual to Flowchart, to model a process flow, making any revisions or updates easy to perform. Flowcharting critical processes can help identify key control points and can be used to produce process and data flow diagrams. Of course, the flowcharts can be reused for the next audit of the client or for audits of similar operations.

Antivirus and Firewall Software

Antivirus software is a class of programs that search your computer (hard drive and floppy disks) for any known or potential viruses. All auditors should ensure that their computers and LAN are protected from malicious software by installing and maintaining adequate antivirus software. Equally important is ensuring that your antivirus engine and database are up-to-date.

A firewall is a set of related programs, located at a network gateway server (permitting the flow of data between two servers on the Internet). The firewall protects the resources of a private network from users from other networks. A firewall is designed to prevent unauthorized access by persons external to the organization and to stop employees from going outside to unauthorized sites. Audit organizations with either a direct Internet connection or an intranet that allows its workers access to the wider Internet should install a firewall to prevent outsiders from accessing private data resources and to control what outside resources the auditors will be able to access.

Software Licensing Checkers

The issue of copyright infringement and the associated penalties are serious concerns. Previously, auditors wishing to conduct reviews of microcomputer software to ensure that the company was not breaking any license agreements by running illegal software faced a difficult task. The job meant visually scanning all the directories of all the microcomputers in the organization to identify all software on each microcomputer. Today, however, other options are available that make the task less time-consuming and more effective. Software exists that will scan all directories searching for file names and compare these with a user-defined database of software (e.g., SPAudit). Other packages (e.g., Barefoot Auditor) will read portions of all executable files, searching for a foot print that uniquely identifies the software package,

even if the user has renamed the file. The program retrieves the software's product name, version, license number, serial number, and date by reading the information contained in the executable file. The auditor can use this information to check for the appropriate software license.

Specialized Audit Software Applications

In addition to all the generalized software available to all users of microcomputers, specialized audit software has been designed to support auditors in their various activities. Of course, since audit software is supporting auditing under diverse circumstances and in various ways, it is by definition and functionality also a powerful accounting, controllership, and management information tool. The following discusses software applications that may assist auditors in taking a more critical view of information. The use of specialized audit software allows auditors to formulate and test hypotheses, look for transactions that meet specific audit-defined criteria, and much more. The software applications described as follows range from simple extractions to the use of expert systems.

Data Access, Analysis, Testing, and Reporting

Increasingly, the auditor is faced with electronic rather than paper files. The source documentation may not be readily available—if at all—and then only in electronic format. Often the sheer volume of information precludes the use of manual analysis techniques. A variety of applications can give auditors the capability to analyze information contained on mainframe, mini-, or microcomputer systems.

Audit software was designed to facilitate universal data access, comprehensive analyses, exhaustive tests, and representative reports, both interactively and using scripts. The interactivity and speed of these tools and techniques lets the auditor explore and test hypotheses. Consequently, auditors have had a lot of success in analyzing data to address issues related to data integrity, including the interrelationships between or anomalies with data elements, the effective and efficient operation of the client's accounting and data processing, detection of control weaknesses, and so on. Various sampling methods are also available with audit software. But even more importantly, modern audit software facilitates electronic analysis, screening, and testing of 100 percent of the audit populations.

Computerized audit techniques can also be used to supplement the review of a system's controls. Simple application controls such as edit checks can be easily verified by sorting or summing the application's transactions on the given field to determine if the field contains only values that would

pass the edit check. Sometimes, the edit check may verify field values on data entry but does not verify data coming from another electronic source. CAATTs can also be used to check for invalid combinations or fields, such as a person with sex = male and pregnant = yes.

Case Study 7: Verifying Application Controls

In this example, an audit of the finance system (accounts payable) determined that the control over the payment of duplicate invoices relied on two fields. The financial system would reject and flag any transaction where the combination of vendor number and invoice number was not unique. The auditor raised concerns when he found that there was poor control over the vendor table (the table that assigned vendor numbers to vendors). As part of the review of the controls over duplicate payments, the auditor summarized the vendor table on vendor name and found that numerous vendors had more than one vendor number.

In many cases, vendors with slightly different names, such as ABC Limited and ABC Ltd and ABC Ltd., had a different vendor number assigned for each spelling of the vendor name.

Vendor Name	Vendor Number	Address
ABC Limited	N3450D12	1080 Castlehill Cres
ABC Ltd.	N5478X23	1080 Castle Hill Cres
ABC Ltd	N5471C10	1080 Castle Hill Cres

The auditor informed management that the poor control over the vendor table, which allowed not only different vendor numbers to be assigned to the same vendor, but also permitted any invoice clerk to add or delete vendors from the vendor table, compromised the control over the payment of duplicate invoices. Management did not seem to feel that there was any significant exposure. They stated that other compensating controls, including a manual review of payments by the budget managers, would catch any duplicate invoices.

The auditor was convinced that management would not address the control weakness in the vendor table without further audit evidence. So he performed a test to check for duplicate payments. The auditor-defined criteria for duplicate payments were same invoice number and same payment amount. The resulting file contained several thousand potentially duplicate transactions. On reviewing the file, the

auditor realized that these criteria were not sufficiently restrictive, that too many firms had invoice numbers using a similar sequence (#2005-1 for example), and that too many invoices were for even dollar amounts ($100.00).

The auditor refined the criteria by requiring that the invoice number be at least four characters in length and that the invoice amount be greater than $1,000.00. The second extraction produced 214 possible duplicate transactions totaling just over $1.8 million. A manual review eliminated 36 transactions for a variety of reasons, such as vendors' addresses at opposite ends of the country. The final file contained 178 transactions totaling more than $1.5 million. The auditor selected the ten largest payments and requested copies of the invoices from the invoice processing sections that had processed the payments. Nine of the payments turned out to be duplicates, although two vendors had returned the duplicate payment. The total overpayment for the remaining seven duplicate invoices amounted to close to half a million dollars.

When management was presented with the results of the auditor's test for duplicates, they readily agreed to implement tighter controls over the vendor table and even proceeded with a review of the other 168 potentially duplicate transactions that the auditor had identified, and ordered recovery action for all identified duplicate payments.

The use of CAATTs in Case Study 7 allowed the auditor to search through millions of transactions for audit-specified criteria in hours. Further, CAATTs permitted the auditor to adjust the criteria after reviewing the initial results. While the test did not identify all duplicates and not all of the transactions were duplicates, the test did validate the auditor's initial suspicion and highlight a significant system weakness.

All audit phases can be supported with modern audit software, such as Audit Command Language (ACL) and Interactive Data Extraction and Analysis (IDEA). For example, during the planning phase, the software can be used to define the audit populations, review previous and current years' expenditures and budgets, identify resource consumption and outputs, or perform trend analyses. As a result, the auditor will have a better understanding of the client's business even before leaving the office, and the conduct phase can be much more focused.

During the conduct phase, audit software can be used in many ways, including:

- Testing reasonableness, edit checks, and interrelationships
- Verifying posting and control totals

- Calculating days-aged for receivables and inventory turnaround times
- Summarizing expenditures and revenues by location
- Selecting statistical samples
- Identifying judgmental samples or directed samples (based on risk or materiality issues)
- Producing (exception) reports

Case Study 8: Allocation of Cleaning Expenditures

The company had recently expanded its cleaning services to include several new office buildings. This placed some unique requirements on the cost-tracking system. Previously, all other buildings were occupied by a single client; however, the new buildings each housed several clients.

The audit reviewed the cleaning expenditures incurred for one of the new office complexes that housed eight clients. The objective was to identify and verify the allocation of the costs to each client. The costs included the value of materials used in cleaning activities and the direct labor costs. Headquarters paid all invoices, but the allocation of the costs to each client and the production of client invoices were performed by the staff at each local office building.

During the planning phase of the audit, information from the headquarters' financial system was extracted to determine the composition and characteristics of the audit population. The data was downloaded to a microcomputer, and several standard reports were used to analyze and size the audit population. Summary reports were produced to obtain an overall view of the audit population and to provide a basis for developing a sampling methodology. For example, all expenditures over $5,000 were identified to determine the percentage and type of high-dollar transactions.

The audit team then selected two samples from the population. The first sample was a dollar unit sample, where every dollar had the same probability of being chosen; the second was a directed or judgmental sample, selecting records from the high-dollar transactions. During the conduct phase, the local office provided a copy of the data that it used to produce billing statements for each client. The audit team compared the data extracted from the headquarters' financial system with the local office's data to verify the integrity of each client's bill and to identify unrecovered expenditures. A 100 percent verification of transactions in the headquarters' financial system, but not in the local database (potential unrecovered expenditures) was performed. A sample of the

transactions in the local system that were not in the headquarters' financial system (potential erroneous recoveries) was also reviewed.

During the on-site visit, the local database was also used to produce a judgmental sample. In particular, expenditures were sorted and summarized by client and by type of expense (material or labor). All cleaning projects that had material costs, but no direct labor costs, were reviewed. Further, the audit team performed limited testing of the validity of the local system's data (edit and validation checks) and reviewed the completeness and accuracy of the administrative overhead charges.

Much of the initial analysis was conducted at headquarters, including selection of sample transactions. This meant that the on-site time was spent conducting analyses rather than selecting samples; therefore the disruption to the client was kept to a minimum. The comprehensive analysis that was performed on-site was only possible with the use of the computer and appropriate audit software. Further, the speed and detail achieved in identifying data errors enabled the local office to take corrective action before the audit team had left the site.

In Case Study 8, the direct and unrestricted access to the data and its immediate analysis, screening, and testing allowed the audit team to also ask what-if questions and to view the data comprehensively and interactively. In this way, audit teams can reduce audit time significantly and produce audit results that are more reliable and much more comprehensive and exhaustive with modern audit software.

Standardized Extractions and Reports

Often, similar information is required for diverse audits. Sometimes the only variable that changes is the location or branch. Rather than writing new programs to extract the information each time an audit begins, it is often more efficient to develop standardized reports. Of course, modern audit software facilitates such designs and customizations in various ingenious ways. Audit software can be used to create executable jobs (also called scripts or macros) to perform repetitive tasks, such as combining monthly files to create a year-to-date picture at any point in time.

The standardized reports can be used by auditors to access the key information systems, such as finance, personnel, inventory, payroll, payables, and compensation and benefits. Various types of standard reports can be developed, including high-level summaries and detailed listings of transactions meeting certain thresholds. High-level summaries will give the auditor an overview of the audit entity for use during the planning phase. Detailed

reports will more likely be required at the conduct phase to review specific issues or concerns.

When starting to build standard reports, it is a good idea to obtain a copy of the data dictionary, preferably in electronic format, and ensure that you have an adequate understanding of all the data fields. A good understanding includes knowing:

- What kinds and types of data are stored in the system?
- What possible values do the fields contain?
- Where did the data come from?
- What information is derived from the data and what does it mean?
- How is the data administered, protected, and secured?
- How is the data and the information used by (senior) management?

This knowledge will help you in designing report contents and layout formats based upon your own data naming conventions. The information gathered can go considerably beyond the data stored in the original computer files, and the extraction routines can easily access more than one type of data file.

If appropriate, consider developing a catalog of standard reports for use by all auditors. The catalog could list all standard reports (purpose, layout, description, and possible uses) and provide a sample printout for each type of report. This type of documentation is useful to all auditors, but particularly to new audit staff who are trying to develop an understanding of the various application systems. Of course, by knowing the information requirements of the client's management, it will be possible to generate various management reports with the same ease and to suggest even better ways of keeping informed. Today's audit software was designed as meta-software, such that it provides the same or better answers to critical questions about organizations and their data (Will [1996]). In organizations where auditors are using CAATTs effectively, the clients often also acquire audit software to be used as a management tool after the audit is completed.

Information Downloaded from Mainframe Applications and/or Client Systems

Many corporations have large centrally managed mainframe applications or enterprise-wide systems. The detailed transaction files for any given year may be so large that frequent access through the mainframe computer system would be costly and time-consuming. With the increase in storage available on LANs and even microcomputers, auditors can download gigabytes of data and have the detailed transactions on the audit LAN or a specialized

CAATTs workstation. Another option is to create views of the data by summarizing the information on key fields and downloading the summaries to a microcomputer. Thus, instead of taking hours to access, read, and extract information (usually requiring knowledge of mainframe operating systems and extraction tools and therefore requiring programming staff—with the usual backlogs and delays), the summarized data is available in seconds or minutes, in an easy-to-use format on the microcomputer.

Case Study 9: Detail and Summary Data

The summarized data on the microcomputer can be used by auditors for planning and trend analysis. For example, one organization created three different views (summaries) of their financial data.

Summarized Information Available on the LAN

Mainframe File—detailed transactions

Dept	Account	Amount	Period	Trans #
Pers	Salary	2,100.23	09/09/2004	123P0234
Pers	Salary	2,435.37	09/09/2004	123P0235
. . .				
Pers	Salary	1,982.20	09/09/2004	123P0236
. . .				
Pers	Salary	2,985.34	09/09/2004	123P9964
Ops	Salary	1,432.78	09/09/2004	128RO456

PC File—Summarized by Department, Account, and Period

Dept	Account	Amount	Period	Count
Pers	Salary	1,463,445.78	09/09/04	731
Ops	Salary	5,672,129.54	09/09/04	3,245
. . .				

The detailed files (more than 2.3 gigabytes—nine million records—in size for each year) took more than one hour to read using a mainframe extraction tool that was only understood by IT specialists. The views created for the auditors contained eight years worth of data, 16 gigabytes of storage space on the mainframe, but only 14 megabytes of disk space in summary format on the microcomputer.

In Case Study 9, summary files can be used by audit teams during the planning phase to get a snapshot of the current data and to examine trends over the last eight years of financial information (by resource

code, by responsibility center, etc.). Other financial summaries can be created to provide budget, commitment, and expenditure information for each responsibility center. Also, summaries of information from other systems, including the personnel and inventory systems, may be created and downloaded.

Case Study 10 is another example that illustrates the usefulness of maintaining summary files.

Case Study 10: Use of Summary Data

Summary information from the pay system was used for an audit of overtime to easily determine the salary and overtime totals by location. The percentage overtime/salary helped auditors to identify locations with high levels of overtime use, such as overtime more than 10 percent of total salary. These locations had a higher risk of poor management of overtime and salary budgets.

The audit of hazardous materials used a summary of inventory holding by locations to determine the total value of hazardous materials at all locations and to help the auditors decide which warehouses should be visited and inspected. A large volume of a variety of hazardous materials represented higher levels of environmental and health and safety risks.

Case Study 10 illustrates summary files that are easily accessible through audit software and depict the whole audited organization or specific facets of it. These summary files provide all audit teams with quick access to several years' worth of data in a format that is readily understandable, and is easy to use—all without the help of programming specialists or the associated mainframe computing costs. Abnormal trends or overly large values may indicate higher levels of inherent risk, requiring audit attention.

This greatly improves the planning phase of the audit, allowing the team leader to quickly size the audit entity and view the audit universe. This can assist in both the development of the annual audit plan, including the identification and assessment of risk, and the planning for a specific audit (see later in this chapter, see also the section on Continuous Auditing). Having several years' worth of data during the preliminary phase of the audit means that trend analysis can be performed, helping to further define specific lines of inquiry for the conduct phase. Previous years' data do not change and can be stored on the LAN. Current-year data can be summarized and downloaded as often as necessary (daily, weekly, monthly). Thus, the

summary files even can be kept current with standardized audit software applications.

Electronic Questionnaires and Audit Programs

An electronic questionnaire can range from a simple form used to capture user input electronically to a complex interactive form leading the user through the relevant questions or sections, based on the answers supplied. Electronic questionnaires can be used for several purposes. For example, they can be used to survey clients or to create standardized audit programs to be used by several auditors.

Visual Basic and Delphi are two microcomputer-based tools that allow auditors to rapidly develop electronic questionnaires. The questionnaires can be used when performing interviews or can be used by the client. The fact that the questionnaires are in an electronic format means that they can be easily sent to the client by e-mail, on disk, or through an Internet or intranet site. The questionnaires can also be programmed so that the output can be directed to a printer or saved in a file for further analysis using data analysis software.

With modern audit software, detailed audit programs that involve many steps (some of which will or will not be followed depending on the results of the previous step) can be partially automated. This has enormous advantages when dealing with multisite audits being conducted by several audit teams. The development of an audit program in electronic format can help ensure consistency across sites. Further, if the subject area is complex and the decision tree has many possible branches, it may be difficult to ensure that all the auditors are fully conversant with all aspects of the audit. An electronic audit program will lead the auditors through each step and automatically jump to the appropriate question.

For example, in an audit of overtime, the electronic audit program uses the answer to the question, "To which union does the employee belong?" to determine the proper overtime rates and criteria for the remainder of the audit program. The portion of the audit program dealing with shift work would be ignored if not relevant for that union.

Another advantage of using an electronic audit program is its ability to capture data in a file for further analysis by the auditor. Client surveys can be sent to the users directly, via e-mail, or on disk. The completed questionnaire files can be returned to the auditor via the same means. All of the completed questionnaires are readily available for electronic analysis. Thus, instead of having to review perhaps hundreds of paper questionnaires that had been completed manually, the auditor can simply use audit software to analyze the results electronically.

Case Study 11: Data Capture Options

In an audit of a workforce adjustment program, the electronic program captured information on employees who had been laid off. Three audit teams were conducting concurrent audits at different locations. Each night the data files were uploaded to the corporate headquarters and combined into a single database that was analyzed for specific trends and issues. When required, changes were made to the audit program, and the new version was sent to the audit teams for use for the remainder of the audit. As a result, the manager responsible for the audit was able to monitor the progress of the audit (number of employee payouts reviewed), determine interim results, and ensure that all audit teams were following the new audit program, electronically. (See later in this chapter, the section on Expert Systems for more information on automated flow and control of audits.)

Control Self-Assessment

The idea of control self-assessment has been around for many years. However, the concept is seeing a resurgence in use, partially because of support it is receiving from technology. Self-assessment and facilitation software can help auditors to facilitate self-assessment sessions. The software can assist auditors in encouraging the participants from the operational area that is being audited to determine which controls are important and how well these controls are functioning.

One approach to control self-assessment starts with the definition of the primary objective of the entity and the statement of the supporting objectives. An auditor, leading the self-assessment session, captures the results of the participants' discussion using a computer connected to an LCD panel. Facilitation software often can allow participants to contribute anonymously to the discussion. The participants can readily see their input and often feel that it is recognized as more important and relevant to the process when it is actively captured and displayed on the screen.

The self-assessment software also allows the participants to use voting pads to rate items being discussed, such as their level of agreement with the statement "The controls are working effectively." The results of the voting are anonymous and can be displayed in graphical format in real time. This highlights the control successes (strengths) and obstacles (weaknesses). Auditors can easily capture and consolidate the participants' ratings of the desired and actual level of effectiveness for each control objective—the

difference representing the opportunities for improvement. The graphing of all participants' responses to control questions immediately highlights differences in opinions and facilitates open and honest discussion.

The interactive nature of the tool and the graphical support provided by self-assessment and facilitation software can contribute directly to the success of the self-assessment sessions. Also, the results of the upfront evaluation of the controls can help focus auditors on specific areas of higher risk.

Parallel Simulation

As explained in Chapter 1, the use of parallel simulation, a technique whereby the auditor simulates the functioning of a system or portion of a system, can be very effective in identifying errors in the original system. The results of the simulation are compared to the original system and any discrepancies are noted. Case Study 12 illustrates the use of parallel simulation.

Case Study 12: Insurance Premiums

At one organization, the auditors wanted to verify the calculation of insurance premiums to be paid to moving companies to cover the loss or damage of furniture for employee moves. First they obtained copies of the source code and developed a good understanding of the routine that calculated the insurance premium. The main cost driver of insurance was determined to be the weight of the goods being moved. The formula to calculate the insurance premiums included the distance of the move, the weight of the goods, and other factors.

Next, the auditors used their own software to write a job to simulate the application's calculations of the insurance premiums. They then obtained the move data file, ran their job, and calculated the premiums. By comparing the simulation's results with those of the actual application, the auditors discovered that the weight of the car was being added to the household goods and the insurance premiums were being erroneously calculated using the combined weight (goods and car). The production system was including the weight of the employee's car under both Household Goods and Vehicles. As a result, the total weight of the goods (one of the variables in the premium calculations) was overstated by the weight of the vehicles being moved. A modification was made to the production program, which reduced the total premiums paid by almost 30 percent.

Any module of the application system being audited can be tested through the use of parallel simulation. This also can often be done quickly through the use of fourth-generation languages on the microcomputer. In some cases, spreadsheet software has been used in a parallel simulation exercise. The fact that the simulation does not require data entry screens or nicely formatted output makes the process easier. The simulation uses the same data as the production system, and the electronic comparison of the results (i.e., production versus simulation) quickly identifies any errors.

Electronic Working Papers

In recent years, a lot of emphasis has been placed on electronic working papers. Some of the large accounting firms have developed and are selling electronic working paper packages. While these packages use different software and can be customized, most contain similar modules, including a standard format for working papers, a standard format for a report, a reference directory, and a methodology directory.

The basic capabilities of most electronic working papers packages include:

- Quick and reliable replication of databases and documents across one or many servers
- Automatic routing of information
- Support for unstructured data types (text, graphics, spreadsheets, flowcharts, etc.)
- Ability to create forms or standard templates for working papers (memos, reports, worksheets)
- Enforcement of a standard methodology/approach to the conduct of audits
- Automatic naming and management of files, solving document management and version control issues
- Interactive working paper supervisory review
- Multiple views of data (audit in-progress, recommendations by group, audit phase, etc.)
- Easy access to, and sharing of, all relevant data for auditors working off-site

Electronic working papers standardize the formats of many of the required elements of an audit, making it less time-consuming for each auditor. The software contains automatic routing capabilities (e-mail) usually with a sign-off feature. Thus, the draft report will be automatically routed to the team leader, and once signed off, to the audit manager, and so on up the chain. Electronic working papers software also allows the auditor to establish links between various files or even between paragraphs within separate

files. Thus, for example, step 5.1.a of the methodology, "Ensure the accuracy of the time reporting data," can be linked to the test performed, which in turn can be linked to the working papers file containing the results of the test. This is particularly useful for the manager who is performing a review of the working papers. By simply clicking the mouse on step 5.1.a of the methodology, the manager can review the test. Another click will display the results.

Several useful areas where the functionality of electronic working papers software can have a significant payback are:

- Audit procedures
- Best practices
- Company policies
- Control questionnaires
- Issue tracking
- Reference materials and documentation
- Report tracking
- Risk assessment
- Working papers
- Follow-up on audit recommendations

While some of the features of electronic working papers can be implemented using a standard word processor that supports templates and hypertext, the full functionality requires more sophisticated software that includes interfaces to audit software for data access, analyses, screening, testing, and reporting.

Data Warehouse

A data warehouse is an extraction of existing operational data that is optimized for use by end users. Basically, it is a collection of data that is used for decision-making support rather than for operational support. The information contained in a data warehouse is typically used to analyze trends in data. The information derived from the data warehouse is used to support long-term decisions rather than short-term or immediate decisions. It can be used to answer questions like "What is the long-range demand forecast for a certain product?" rather than "Should we manufacture 2,000 or 3,000 of brand X?"

Often the data warehouse is developed for use by senior management, but it also can be extremely useful to auditors. If a corporate data warehouse does not exist, the audit department can develop its own data warehouse. In these cases, the audit-developed data warehouse can often form the basis for the corporate data warehouse or an executive information system.

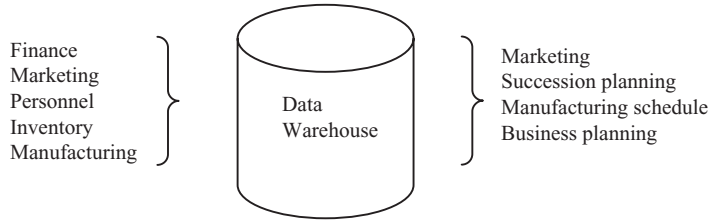

EXHIBIT 2.2 Business Application Data Warehouse Datamarts

Data warehouses are developed to allow users to have easy access to the data in order to examine trends and perform what-if analysis.

The underlying business systems may be difficult to use or not in a format that supports what-if analysis, or they may be live production systems that do not support direct queries or are slow (long response times). The data warehouse takes users from an environment where they have to spend 80 percent of their time trying to find and extract the data and 20 percent of their time analyzing it, to one where 80 percent of their time is spent in the analysis and only 20 percent in finding and extracting data.

The data warehouse is usually developed along subject lines such as personnel, material, or facilities. The data represents a snapshot in time and provides users with an integrated view of the data.

A data warehouse contains information extracted from a variety of business applications. Often, specific views, or Datamarts, are developed for specific users (see Exhibit 2.2).

Application systems collect and store data to support the specific business applications. The application provides edit checks, entry screens, and standard reports as well as information processing capabilities. The information contained in the business applications is extracted and integrated into a data warehouse. The business applications are still used to support the immediate requirements of their respective business operations, but the data warehouse allows for the processing of a wide variety of integrated information to support management decision making.

The basic methodology that should be employed to develop a data warehouse consists of the following steps:

1. *Data Model*. Determine what information is required to support the decisions that need to be made.
2. *Data Sources*. Determine the current applications that contain the required information.
3. *Physical Database*. Determine the type and structure of the database to contain the data.

4. *Extraction and Transformation*. Develop programs to extract the required data from the various business applications and transform the data into a format that is compatible with the data warehouse structure.
5. *Populate Data Warehouse*. Run the extraction and transformation programs and load the data in the data warehouse.
6. *User Tools and Training*. Develop appropriate tools, such as query capabilities, and provide users with the required training.

Audit can contribute to the development of effective data warehouses by ensuring the integrity of the business systems and the information contained therein. In order for the data warehouse to be successful, the underlying business application must contain complete and accurate data. Further, audit can influence the data warehouse development if it has knowledge of the basic business systems. The users must have a good understanding of the data and its meaning, and they must have easy access to the data warehouse. In addition, the data warehouse must contain enough data to add value to the decision-making process, but not so much that it slows down the user response time. Audit, through its use of the key business systems, can provide advice to the developers of the data warehouse, by defining critical data sources and identifying potential errors. Finally, audit can review the integrity of the data warehouse by comparing the data contained therein with the underlying business systems.

The development and use of a data warehouse by audit can greatly improve the capabilities of audit to provide management with useful recommendations. Further, the development of a data warehouse provides audit with a useful tool for performing trend analysis and for conducting risk analysis. The results of these analyses would help audit to focus its resources on areas of risk and materiality, leading to more value-added audits.

Data Mining

Once a company has developed a data warehouse, the possibility of using this data to answer complex problems becomes a reality through the application of data mining techniques. The term *data mining* comes from the notion of being able to drill down into the data to obtain more detailed information. The user begins with a high-level view of the information and can then go a step deeper into the actual data for selected criteria and areas. For example, the auditor may be reviewing trends in production costs by assembly line. This may lead to the desire to review a particular assembly line's production costs by month, which in turn may lead to the examination of the detailed cost items for a particular month. The auditor used the

EXHIBIT 2.3 Data Mining Processes

notion of data mining, digging deeper into the details along specific lines of inquiry (see Exhibit 2.3).

Many audit software packages offer this type of functionality, and some allow the auditor to examine the information interactively, making data mining a hands-on activity and providing quick response times. More business applications are being developed, which allow the production or business managers to use data mining tools to analyze operations (see Exhibit 2.4).

It is important for audit to be aware that data warehouse and data mining do present problems/issues as well as opportunities. Data warehouse systems rely on business systems to supply the raw data for input. This raises problems in that the databases are dynamic and tend to be incomplete, noisy, and large. Other problems arise as a result of the adequacy and relevance of the information stored in the business systems. The business systems are designed to support specific operational concerns and may not contain all the information required to support data mining. For example, the data may not support the proper diagnosis of malaria if the patient database does not contain the red blood cell count—a critical field in diagnosing the disease. Audit must be careful to ensure that inclusive data, errors in data elements, missing data, and other problems related to data integrity, timeliness, and completeness do not lead to invalid or overlooked relationships and conclusions.

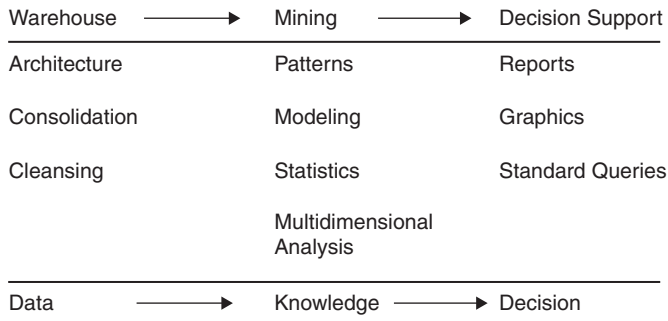

EXHIBIT 2.4 Decision Support

Software for Audit Management and Administration

Internal auditors looking for ways to add value to their organizations are becoming more creative and resourceful in finding ways to make maximum use of a critical resource. CAATTs help auditors conduct audits in today's electronic age, and they can improve the audit function. Audit managers can apply software to help them focus on areas of risk, manage their scarce resources, and monitor the operations of the organization. The range of tools available to audit management continues to grow and improve. Computers have also become an indispensable management audit tool.

In order to provide a conceptual frame of reference for the variety of software support that is available to audit managers and administrators, and is applicable to their challenging tasks, this section begins with the concept of an audit universe and concludes with that of an audit early warning system.

Audit Universe

Few, if any, audit departments have the resources to audit every aspect of the company. Nor do many companies require every aspect of every operation to be audited every year. Thus, audit management must decide what should be audited and when to conduct the audit. In order to allocate limited audit resources appropriately, audit management must have a means of defining the audit universe. This means identifying risk factors, establishing audit priorities and frequencies based on a relative risk ranking, developing and maintaining an audit plan, and preparing activity reports. This approach is required for both the current year and for long-range audit planning. Computerized tools exist to assist audit management in defining the audit universe and in assigning risk to each of the components. A simple audit universe can be developed using spreadsheet or database software. Each row in the spreadsheet, or each record in the database, represents an audit entity. For each entity, the audit would identify the risks. By assigning risk scores and multiplying the risk scored by the weighting factor, each auditable entity can be assigned a total risk score. The entities with the higher risk would be audited first.

Commercial audit universe software packages offer more features and functionality than simple spreadsheet and database software, such as reporting capabilities and a structured format to defining the audit universe. Examples of audit universe software include ADM Plus and AutoAudit.

One of the main advantages of this type of software is that the information is reusable and reduces the time required to update the audit plan for the next year. Thus, management can deal conveniently and explicitly with issues such as audit coverage, cycle time, risk, and materiality.

Audit Department Management Software

Audit department management software, such as Audit Leverage, enables all internal audit department data (e.g., Annual Planning and Budgeting, Timekeeping, Staffing and Scheduling, Audit Histories, Work Papers, Audit Program Templates, Review Notes, Audit Report Generation, Tracking of Findings, Recommendations, Management Action Plans, and Follow-up) to be stored in one truly integrated and secure database solution. The result is that auditors spend less time on work paper documentation and administrative tasks and more time completing audits and performing macro-level analysis and monitoring of risk and control issues.

Typically, audit department management software allows auditors to work either in the office or offline. It enables teams of auditors to work remotely in the field and then synchronize with each other or with the central server, enabling managers to review the workpapers without visiting the site.

Software such as Audit Leverage allows you to do more with fewer audit resources and is flexible enough to adapt to your audit process, methodologies, and risk criteria, without your having to spend money on software customization.

E-mail

Electronic mail (e-mail) is an excellent vehicle for communication within the audit organization and with audit's clients, because it is faster and more flexible than traditional mail. Within the audit organization, e-mail can be extremely useful when trying to keep in touch with auditors who are working off-site. Today, the ability to send and receive information in electronic format is almost essential. Auditors working at client sites do not have to be isolated from their headquarters. Off-site auditors can simply use their laptops to dial-in and receive or respond to their messages. E-mail can virtually eliminate the problem of telephone tag and also provide a physical record of the communication for future reference.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a standard Internet protocol that enables the exchange of files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers Web pages and related files, FTP is an application protocol that uses the Internet's Transmission Control Protocol/Internet Protocol (TCP/IP) to provide Internet users with access to files on connected servers. As a user, you can use FTP to update, delete, rename, move, and copy files at a server located anywhere on the Internet.

This allows an auditor working at a client site to retain electronic access to headquarter's information and support. Previously, if an audit team discovered that vital data files were missing, they had to return to headquarters to get the needed information. Now, with FTP, auditors are able to request and receive information in electronic format in a matter of minutes.

Additional travel costs can be avoided and the disruption to the client kept to a minimum. Instead of traveling to a client's site for a preliminary survey, the auditors can now do much of their analyses at headquarters before they go to their client's office. Once at the client's site, if client-specific information is needed but not available, it can be sent to the auditor electronically by staff at headquarters.

Another use of FTP software is to produce a daily consolidated progress report by the daily capture of the actual results from each site. Each night, the audit results from each site can be uploaded to headquarters, combined into a single database, and processed to produce various status reports. For example, one company found this extremely useful when trying to size the total dollar amount of a certain type of error across several regional offices to determine if additional testing was required. By comparing the results from various sites, the team leader was also able to identify anomalies at specific sites and redirect the audit according to the new-found insights.

Case Study 13: Multisite Audit

The working papers of the on-site team were sent back to the audit supervisor for review, prior to the team leaving the client site. The project leader easily reviewed the working papers daily and provided additional instructions to the audit team via a modem. This was particularly useful when trying to manage a concurrent, multisite audit project with changing audit requirements or criteria. Each audit team sends the results of their work back to the audit supervisor, and once the supervisor has reviewed the work, the comments are sent back to the audit teams.

Access to external databases is another valuable use of FTP capabilities. Using a microcomputer, auditors can have easy access to reference materials such as governmental regulations; corporate policies, procedures, and regulations; audit guides and methodologies used by other companies; and so on. For example, U.S. Government Accounting Office (GAO) audit guides, methodologies, and other reference materials are available on the Internet.

The Internet also provides access to journals, newspaper databases, and a wide variety of other information, including audit software suppliers, as well as e-mail to other auditors. Access to these sources of information can greatly reduce the time required to perform the initial research during the audit planning phase or to address compliance issues during the conduct phase. In particular, the auditor in the field can access all relevant regulations and references, whether or not they are available at the regional office.

Today, organizations concerned about the potential exposure of being on the Internet are creating corporate-wide intranets with the same features as the Internet, but within the physical confines of the corporation.

Intranet

The computing pendulum has swung from centralized computing to stand-alone computing and back to centralized, or at least distributed, computing. It went from mainframe computing to personal computing on stand-alone microcomputers and then back to where all employees are connected to distributed systems. Local area networks (LANs) connect employees in the same work group or same location to each other. Metropolitan area networks (MANs) expand this connectivity to all employees within a geographic location (often a city), and wide area networks (WANs) take this a step further by connecting employees in many cities.

The Internet has been a well-known source of international connectivity for research. While it has been around for many years, only in the last ten years has its use expanded rapidly in the business area. This has opened up many new opportunities for businesses and has also spawned a new technology—the intranet. An intranet is basically an Internet that exists within the physical and logical control of an organization. The establishment of an intranet allows the corporation to create an Enterprise Wide Web, linking information from all branches, locations, departments, and so on. It also protects the corporation from external hackers, since the only access is from persons physically within the corporation. However, some intranets are using trusted firewalls to provide external users with secure access to the corporate intranet on a special-case basis.

All company employees have access to corporate information such as personnel policies and job postings. The audit organization will have access to a wide variety of corporate information, including corporate policies, procedures, regulations, and other performance information. The intranet could also provide auditors with easy access to financial statements and business plans and those of every division. Audit can also use the intranet as a tool to market audit services, publish best practices and audit plans,

and showcase significant results achieved by audits. It can also be used as an efficient means of acquiring and disseminating business intelligence.

All documents on the corporate intranet are searchable. Therefore, auditors can use it to search for documents based upon keywords and then use the electronic links to other documents. The hypertext links (document linking) capabilities of the intranet can be useful to audit in several other areas; for example, you could link the findings to the detailed working papers. Simply clicking on the finding statement would send the user to the supporting documentation. Another click brings you back to the original finding statement. Also, the table of contents for each document can be set up with hypertext links. Click on an item in the table of contents and automatically jump to that section.

Audit could also use the corporate intranet to set up internal newsgroups to discuss specific issues with auditors from other branch offices or with clients throughout the organization who have a similar interest. It is an excellent way of gaining and sharing expertise.

Finally, an intranet offers e-mail capabilities to the entire organization. Auditors can send and receive information, including data files, from branch offices when conducting on-site reviews. Teams working at client sites will also still have access to all corporate files (policies, audit programs, etc.) on the intranet.

Databases

Microcomputer-based Database Management Software (DBMS) provides a means of storing, organizing, and retrieving data records. The software also provides facilities for inquiring against the records stored and for producing standard reports. Some databases also include a programming language so the auditor can manipulate the data directly. Even more conveniently, modern audit software interfaces with a rapidly growing number of DBMS, so that knowledge can be applied directly to various data management and administration tasks, including the audit.

There are many possible applications of database software in managing and administering audits. For example, databases can be used to create the audit universe to support the developing, managing, and administering of the audit plan. By establishing a database that describes all of the organization's auditable units, audit management can evaluate the many factors that determine whether or not an area will be audited. The database could contain one or more records per auditable unit, detailing all factors involved in arriving at priority, risk, time, and volume indicators for audits of that unit. It then becomes relatively simple to analyze the data and to determine and outline the audit plan.

A DBMS can also be used to record and analyze audit skills for each auditor. This can be used to determine staffing for each audit and for training requirements. Another use for database software is the tracking and billing of auditor time against various projects. For example, each auditor's time can be coded against the client and the hourly rate defined. Of course, the number and type of databases is only limited by the imagination of the developer, but the availability of managerial and administrative computer support makes it even easier to remain "on top of things" in any and all audit situations.

Groupware

While networking connects hardware, software, and data, groupware connects people. Groupware allows any member of a group or organization to contact and work actively with any other member of the same group. Group members can work with the same information simultaneously, ensuring that all members are informed of changes and updates. The store-and-forward capability eliminates the need to arrange meetings to discuss issues.

Some audit organizations use groupware software to discuss audit recommendations with the client. An added advantage is the capability for auditors and their clients to review findings with a view to arriving at workable solutions in a forum that allows members to contribute to the discussion anonymously. Of course, some of the functions offered by groupware exist already in ordinary e-mail, but the groupware market is evolving rapidly. This should provide interesting options, especially for managing and administering audit teams and departments. For example, international auditing firms have developed and are marketing their own groupware-based audit management and administration systems.

Electronic Document Management

Electronic forms, version control, workflow, and groupware are all pieces of an electronic document management system. However, the most basic elements are the creation, use, storage, and retrieval of electronic pieces of information. The applications supporting electronic document management include office automation suites (word processing, graphics, and database), text search and retrieval software, and document management software. The office automation suite allows users to create, access, and distribute documents, and document management software performs version control.

The utility of this type of software is obvious to any auditor who has written an audit report and the associated draft reports. However, the software is also useful in maintaining control over electronic working papers, particularly if more than one auditor is working on the same audit.

Electronic document management software is also useful to auditors accessing and using company policies, procedures, and operating procedures. Often it is important to know which version of the policy was in place at the time of the audit. Changes to policies and procedures must also be recognized and any standard audit programs changed to reflect the new procedures.

Electronic Audit Reports and Methodologies

Most audit organizations are already using word processing software to produce the final versions of their audit reports. However, many often fail to fully capitalize on the fact that the information is now in electronic format. Too often the electronic version of the report is only used to produce the paper version of the audit report. The final report and the audit methodologies are buried in the working papers, often filed away, so that they are of little or no use to anyone else.

All documentation relevant to a particular audit should be kept in a single folder or directory during the audit. Using standard naming conventions for folders and working paper files can make it relatively easy to distinguish between various types of files such as reports, interview notes, and data and other files.

The audit reports and associated methodologies can be made more usable by collecting the reports and methodologies and giving all auditors read-only access to the electronic versions. The first step in accomplishing this task is to collect all final versions of audit reports and methodologies according to standardized naming conventions. Next, place them in specific directories on a microcomputer or on a LAN server. For example, you could establish two directories: one called Final Reports, with subfolders for detailed reports and for executive summaries, and the other called Methodologies, containing all the relevant audit programs and methodologies. By establishing and enforcing a file naming convention to relate audit reports to audit programs and methodology, it is easier to understand both audit reports and audit approaches. In this way, it is easy to flip from the audit findings to the steps or procedures followed by the audit team and vice versa. The whole audit methodology can also be organized into modules, eliminating procedural confusion, duplication, and inconsistencies.

Once the standard naming conventions are established and the reports and methodologies are placed in the appropriate directories, the electronic versions of these files can serve other purposes. For example, many word processing packages have built-in text search and cut-and-paste capabilities, or you can purchase specialized software to perform these functions. Specifying the keywords of interest to you will enable you to electronically search through thousands of pages of text in minutes. This will also help in

conducting follow-up reviews by allowing you to easily find the original recommendations, management responses, and the associated audit programs for any audit without having to request the paper files or search through mounds of working papers. Because the audit report and the audit program have standard names, anyone searching the audit report would easily be able to determine which audit program and data files were used and vice versa.

The planning process can also be greatly improved; within minutes, all auditors can search through previous audits to determine whether something similar has occurred somewhere else in the organization. If a finding is relevant, the auditor can search through the methodology used by the previous audit team and electronically cut-and-paste audit lines of inquiry into the current audit program. Research time can be reduced from days to hours, and audit programs can be standardized to serve the whole organization rather than just a specific audit.

Additional advantages can be obtained by releasing audit reports in electronic format. Using communication lines, the reports can be distributed faster and easier than on paper. Further, if instead of retyping the client's comments you simply request all responses to be in electronic format, you can then electronically cut-and-paste them into your report—saving time and reducing the risk of misinterpreting the clients' comments. It has been estimated that 80 percent of what is entered into a computer came from a computer in the first place. Add the cost of data entry errors to the cost of reentering the information, and you can see why electronic capture of information can be extremely cost-effective.

Finally, most software applications support linked files. For example, the chart in the final report can be hot-linked directly to the spreadsheet containing the data. Updated data in the spreadsheet will automatically be reflected in the report—ensuring that the report always contains the most recent chart.

Audit Scheduling, Time Reporting, and Billing

For large audit organizations, scheduling audits can be difficult. The assignment of auditors with the appropriate skills to audits can be a complex task, but becomes easier with scheduling software. If scheduling is not difficult enough, try to manually calculate the impact of slippage in the first quarter on the remainder of the year's audit plan. The use of information technology in developing and managing the audit plan can help identify opportunities for improvements, and when and where to use external consultants. Further, appropriate scheduling software can permit management to make changes to the plan and determine the overall effect.

The computer can also be used to capture actual hours of work; to calculate billable hours, using the actual rates; and to produce the audit service invoice. Further, time reporting software, such as TimeSheet Pro, can be used to analyze the audit function by tracking the hours spent on types of audits or by audit phases. This information can help to improve the audit planning process, enabling management to make more accurate estimates of the time needed to conduct each type of audit in the future.

Project Management

To be effective, audit management must plan activities to make the best use of available resources. Work must be monitored to ensure that it is being carried out according to plan, and any variances should be recorded to determine the effect on outstanding plans. There are two levels of planning: strategic and tactical. In the audit environment, strategic planning is used to establish the areas that will be subject to audit over a specified period. Tactical planning is performed for each individual audit to specify the steps to be carried out in the audit program.

Project management software, such as Harvard Total Project Manager, can be used to improve the process of planning, whether it involves all audits to be undertaken in a year or a single audit with several phases. All audit activity can be defined, along with details of the audit resources. Activities can be linked to show the interrelationships, and resources can be allocated to each activity.

Most project management software supports the production of PERT or Gantt charts and allows the user to determine critical paths and the effect of slippage. The ability to measure the effect of slippage in one audit project on the entire audit plan can help audit management determine whether additional—perhaps contracted—resources are required or whether other projects can be adjusted to make up for the slippage.

Extensible Business Reporting Language (XBRL)

XBRL is a platform-independent means of identifying, extracting, and representing financial data and other business information in whatever way the user requires. Using XBRL, organizations can capture financial information at any point in the business cycle, from the creation of invoices and orders to the collection, aggregation, and reconciliation processing performed by their financial departments. XBRL is also a specialized business reporting language for existing and emerging financial and business reporting requirements, such as regulatory filings, statements, and corporate reports. It makes the analysis and exchange of corporate information easier to facilitate, as well as more flexible and reliable.

XBRL is basically three things: (1) a community of people and organizations, (2) a set of rules for developing identifiers for business reporting languages, and (3) a specialized business reporting language for existing and emerging financial and business reporting requirements.

XBRL International is a consortium of people and organizations who have come together to improve the flow of financial information from organizations to capital markets. It includes representatives from all of the stakeholder communities affected by corporate reporting. Members include the companies themselves, their trading partners, internal and external auditors and accountants, regulators and government entities, data aggregators, the investment community, academic institutions and researchers, consultants, and software developers. Together, the consortium members are developing solutions for creating, publishing, and consuming financial data.

XBRL is also a language for capturing financial information throughout a business's information processes. The information can be captured at any point in the business cycle—from the initial creation of invoices, orders, and other documents and actions, through to the collection, aggregation, and reconciliation processing done in the financial departments, and eventually, to the reporting formats such as regulatory filings, statements, and corporate reports. The goal of XBRL is to make the analysis and exchange of corporate information easier to facilitate, more flexible, and more reliable. It does this by tagging each segment of computerized business information with an identification code or marker. The ID markers stay with the data when it is moved or changed, no matter how the data is formatted or rearranged.

XBRL offers many benefits to internal and external auditors, and now is the time to jump on the bandwagon. Currently, for financial information to become reusable, more often than not, there is a need for auditors to search and manually input information into different software. This may be more efficient than using paper, but the improvement is one of speed rather than substance. The adoption of XBRL will reduce mechanical data entry, eliminate entry errors, encourage more analysis of data, facilitate comparisons against external data, and provide greater transparency. XBRL should subsequently affect the quality and quantity of financial reporting data. As a result, it is also a critical tool for audits of the key provisions of the Sarbanes-Oxley Act (SOX), specifically the review of management assessment of internal controls (Section 404) and Section 409's requirements for real-time reporting. In addition, it will enable powerful efficiencies in internal reporting systems and due-diligence for audits of mergers and acquisitions.

Auditors need reliable information on a timely basis, and they want it in language that can be understood and in a format that can easily be used for additional analysis. Since XBRL can be integrated into existing financial and accounting software, it allows for electronic exchange. Virtually any

software product that manages financial information can use XBRL for its data export and import formats, thereby increasing the potential for full interoperability with other financial and data analysis applications. This significantly streamlines the preparation, dissemination, and analysis of financial and compliance reports. XBRL also facilitates paperless financial reporting, supports the single-entry of financial information that can then be used for a wide variety of purposes and recipients, and increases the transparency and timeliness of reported information. Effectiveness is increased because data in XBRL format can be retrieved more easily and can be analyzed with greater accuracy. XBRL provides more relevant and reliable interorganization exchange of information by allowing for technology independence, less human involvement, and more reliable and efficient extraction of financial information. XBRL makes financial information more readily available by providing faster, more accurate electronic searches for information because each instance of information is identified specifically through the attached label.

Auditors will benefit from increased possibilities for automated analysis, the more frequent release of information, and the receipt of information in an electronic, reusable format. XBRL enables auditors to access financial reports in a matter of seconds and move the data to analytical software with literally a click of a mouse. Auditors will be able to tailor searches for multiple company data and export the collected information easily into a spreadsheet for further analysis. This will give auditors access to industry benchmarks, more accurate financial information, and make it easier to segregate the information for trend analysis and continuous auditing. This is possible because each piece of data is identified with an XBRL tag, so comparisons and calculations can be automated when comparing one company's operation with another's or intracompany comparisons from period to period.

By creating a standard computer markup language for government agencies, organizations, auditors, regulators, and financial statement users, XBRL will enhance the availability, reliability, and relevance of financial reports. The use of the XBRL format can standardize all aspects of the electronic financial reporting process, thus auditors will have online, real-time access to standardized financial information. XBRL also encourages and facilitates the use of continuous auditing and Web-based audit programs for standards-based financial statement reviews. By integrating data analysis software programs into accounting functions, XBRL allows auditors to extract, analyze, and interpret audit evidence and to detect unusual transactions or patterns of transactions to deter potential fraud. Continuous auditing, supported by the XBRL format of financial data, can increase substantially the efficiency and effectiveness of the audit process, resulting in cost savings for auditors and their clients.

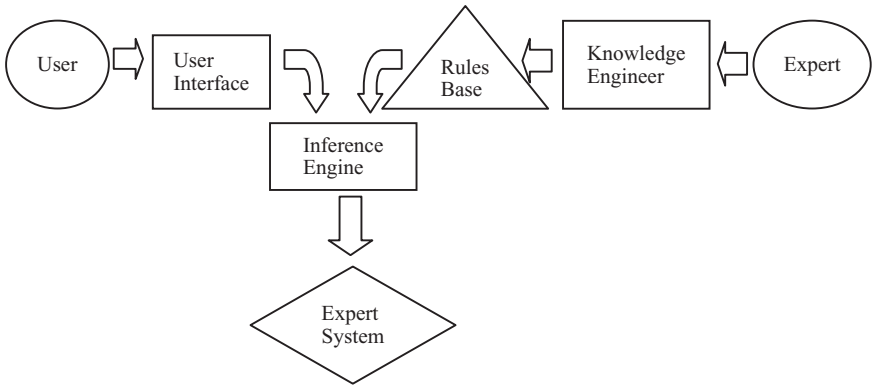

EXHIBIT 2.5 Components of an Expert System

Expert Systems

An expert system can be defined as a computer program that guides a nonexpert user according to a set of rules to arrive at a particularly critical outcome. The components of an expert system are shown in Exhibit 2.5.

Typically, an expert system requires that:

- There is an easily defined problem.
- The problem can be solved analytically.
- The problem has a limited domain.
- The problem is relatively static.

The use of such expert systems has declined dramatically during the last six to eight years due to major methodological limitations (Fetzer [1990]); however, an audit can employ expert system methodology to maintain consistency across audits or at various sites.

Case Study 14: Audit of Hazardous Materials

In performing an audit of hazardous materials, many factors were involved in determining whether or not the materials were being properly stored and handled. The health and safety requirements varied depending on the volatility of the materials and a number of other factors. Some chemicals had to be stored in dry areas, others were extremely toxic—or even cancer-causing—and required handlers to wear protective gear. The result made the audit much more dangerous than a usual inventory audit and more confusing for the auditors.

Dealing with chemical compounds with names difficult to pronounce, and even to spell, was going to be a challenge, and a chemical specialist was hired to provide advice on the audit program. Using a set of rules developed by the specialist, an expert system was developed to lead auditors through a series of questions, ultimately providing a measure of the appropriateness of the storage and handling procedures. Thus, the on-site auditors did not have to possess an expert level of knowledge of all possible hazardous materials they might encounter, as this was handled by the expert system. The system also ensured that all sites were audited with the same level of consistency and completeness.

Expert systems are not easy or inexpensive to develop, but for repeat audits of high risk or importance, they can be a useful alternative. For simpler problems, programming tools, such as Visual Basic, can be used to design an elementary expert system that leads the auditor through a series of questions, capturing and evaluating the input before branching to the next appropriate question (see previous section in this chapter, on Electronic Questionnaires and Audit Programs). Alternatively, expert system shells are available, making it easy to establish the rules (knowledge-based) and provide an inference engine as well as a user-friendly interface.

Audit Early-Warning Systems

Audit organizations, in an effort to act as early-warning systems for senior management, need to know when problems or opportunities arise that require decisions. This entails the use of a reporting system and the establishment of warning levels. Most organizations have more than enough reporting systems, but these present two problems. First, they can overload management by creating too much detailed information, most of it irrelevant. And second, they can provide too little useful information, highlighting certain information, but missing other critical business information altogether (Oxenfeldt, Miller, and Dickenson [1981]).

If audit wants to develop a warning system, then it must do the following: (1) identify the key information systems to be monitored; (2) identify the criteria for anomalies (good or bad) that are of interest; (3) describe the symptoms of the anomalies; and (4) establish indicators for the anomalies. Finally, target and warning levels must be established. When the levels move significantly far away from the target and reach the warning level, an exception report is automatically generated. Upon receipt of the exception report, audit management can decide to investigate the problem or to monitor the results more closely to see if the condition is an aberration and

will thus correct itself. By developing warning systems, audit can be more selective in the audits and the timing of these audits and, therefore, use its resources more productively.

Warning systems can be developed one at a time and used as another source of information when evaluating risk and materiality. They can be entirely automated or simply periodic snapshots, which are used to generate trends for comparison with projections or with data from previous years.

Continuous Auditing

In the 1980s, the notion of continuous monitoring was first introduced to auditors. The basic premise of continuous monitoring was the ongoing use of data-driven attributes to draw conclusions concerning risk in a subject area. The results were used to determine where an audit was required and to focus the audit on the areas of greatest risk. Unfortunately, auditors were not ready—they lacked the tools and necessary data access—or willing to embrace this idea at the time. Now, however, there is a proliferation of information systems in the business environment, giving auditors and managers easier access to more relevant information. Further, the rapid pace of business requires a prompt response to issues. This, in conjunction with SOX Section 409's requirement for disclosure to the public, in a rapid and current basis, material changes to financial conditions or results of operations, changes in auditing standards, and the evolution of audit software are persuading auditors to adopt new approaches to assessing information for audit purposes. There is a demand for independent assurance that control procedures are effective and that the information produced for decision making is both relevant and reliable. In many instances, the need for high-quality information for decision making in the highly volatile business environment is greater than the need for reliable historical cost-based financial statements. If a company cannot adjust to the changing market, and technological and financial conditions, it will not be in business for long. The environment, technology, and audit standards are driving auditors to make more effective use of information and data analysis and encouraging auditors to adopt continuous monitoring. This has produced a shift in the focus of internal audit activities.

However, many auditors are still resistant or confused about continuous monitoring, so it has not become widely implemented or accepted by the profession. One of the main reasons for the reluctance is the term *monitoring*, which is seen as a management function. The second barrier is early attempts to apply continuous monitoring to both instantaneous auditing (a review of transactions in real time) and to the notion of ongoing or frequent, but not real time, audits. Real-time analysis is still beyond the capabilities of

many audit organizations. To address these concerns, proponents of continual monitoring have modified the original intent to one that is used to identify systems or processes that are experiencing higher-than-normal levels of risk, such as where the values of the performance attributes fall outside the acceptable range. In this context, continuous monitoring measures specific attributes that, if certain parameters are met, will trigger auditor-initiated actions. The nature of these actions will vary depending on the risk identified and ranges from sending an e-mail to the manager to a rapid-response audit of the area. For example, the financial system may notify the auditors of any journal vouchers over $250,000. What they do will depend on whether or not this is seen as a single item of concern or more of a systemic problem.

The audit profession still has problems defining the parameters and assessing the importance of continuous monitoring. As a result, few auditor organizations have adopted even the basics of continuous monitoring. In addition, the ability to monitor transactions in real-time is still not always easy or even feasible. To help overcome some of the problems with continuous monitoring, I propose that auditors consider the notion of continuous auditing, a similar, but more powerful approach to identifying and assessing risk. I define continuous auditing as follows:

- *Continuous auditing* is any method used by auditors to perform audit-related activities on a more continuous or continuous basis. It is the continuum of activities ranging from continuous control assessment to continuous risk assessment, all activities on the control-risk continuum. Technology plays a key role in automating the identification of anomalies, analysis of patterns within the digits of key numeric fields, analysis of trends, detailed transaction analysis against cutoffs and thresholds, testing of controls, and the comparison of process or system over time and/or against other similar entities.
- *Continuous control assessment* refers to the activities used by auditors for the provision of controls-related assurance. Through continuous control assessment, auditors provide assurance to the audit committee and senior management as to whether or not controls are working properly by identifying control weaknesses and violations. Individual transactions are monitored against a set of control rules to provide assurance on the system of internal controls and to highlight exceptions. A well-defined set of control rules provides an early warning when the controls over a process or system are not working as intended or have been compromised.

  The extent to which audit is required to perform continuous control assessment activities will depend upon the degree to which management is performing its responsibilities around continuous monitoring. A

strong management monitoring system will decrease the amount of detailed testing audit must perform to provide assurance on the controls.

- *Continuous risk assessment* refers to the activities used by auditors to identify and assess the levels of risk. Continuous risk assessment identifies and assesses risk by examining trends and comparisons—within a single process or system, as compared to its own past performance, and against other processes or systems operating within the enterprise. For example, product line performance would be compared to previous year results, as well as assessed in context of one plant's performance versus all others. Such comparisons provide early warning that a particular process or system (audit entity) has a higher level of risk than in previous years or than other entities. The audit response will vary depending on the nature and level of risk.

  Continuous risk assessment can be used in a large-scope audit to select locations to be visited, to identify specific audits or entities to be included in the annual audit plan, or to trigger an immediate audit of an entity where the risk has increased significantly without an adequate explanation. It can also be used to assess management's actions, to see if audit recommendations have been properly implemented and are reducing the level of business risk.
- *Continuous monitoring* is the process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively. Management identifies critical control points and implements automated tests to determine if these controls are working properly. With continuous monitoring, these tests are performed on an ongoing basis (usually daily) to address management's responsibility to assess the adequacy and effectiveness of controls. The management-monitoring function is often closely tied to key performance indicators (KPIs) and other performance measurement activities.

The techniques of continuous monitoring of controls by management may be similar to continuous auditing. In the event that management performs continuous monitoring on a comprehensive basis across all key business process areas, internal audit can significantly reduce the extent of detailed testing procedures related to continuous auditing. Instead, audit can evaluate the management-monitoring process and then rely upon the output of the continuous monitoring system. In areas where management has not implemented continuous monitoring, more detailed testing, in the form of continuous auditing techniques, will be required by audit.

Continuous auditing is a unifying structure or framework that holds risk assessment, control assessment, audit planning, digital analysis, and the other audit tools and techniques together. It supports the macro-audit issues, such as using risk to prepare the annual audit plan, and micro-audit

issues, such as developing the objectives and criteria for an individual audit. The main difference between the macro- and micro-audit levels is the amount of detail that is considered. The annual audit plan requires high-level information to establish the risk factors, prioritize risks, and set the initial timing and objectives for the planned set of audits. Individual audits start with the risks identified in the annual audit plan, but use digital analysis and other techniques (e.g., interviews, control self-assessment, walk-throughs, questionnaires) to further define the main areas of risk and focus the risk assessment and subsequent audit activities.

Continuous Auditing versus Continuous Monitoring

There are also a number of differences between continuous auditing and continuous monitoring. The main differences are:

- Continuous auditing recognizes and acknowledges that monitoring is a management function, not an internal audit function.
- The frequency of continuous auditing is based on the assessed level of risk and is not continuous unless the level of risk justifies a real-time analysis of transactions.
- Continuous auditing uses not only the comparison of both individual and summarized transactions against cutoff or threshold values, but also the comparison of an entity against other entities (e.g., one operational unit to all other operational units) and a time-wise comparison of the entity against itself (e.g., the entity's performance over the last five years compared to its current performance).
- Continuous auditing also allows auditors to follow up on the implementation of audit recommendations.

Continuous auditing is used by audit to determine if risk is at a level where audit intervention is required. It is not a form of monitoring that would determine if operations are functioning properly (management issue). Continuous auditing allows auditors to quickly identify instances that are outside the allowable range (known thresholds) and those that can only be seen as anomalies when compared to other similar entities or when viewed across time (unknown thresholds). Simply knowing that an audit entity processed a journal voucher that is greater than a cutoff amount will not help auditors to gauge whether or not the entity has improved in its use of journal vouchers. However, it does not have to involve real-time analysis of transactions.

Continuous auditing seeks to measure not only transactions against a cutoff but also the totality of the transactions. This allows you to test the consistency of a process by measuring variability of each dimension. For

example, the consistency of a production line can be tested by measuring the variability in the number of defects. The more variability in the number of defects, the more concerns about the proper functioning of the production line. This premise can just as easily be applied to the measurement of the integrity of a financial system by measuring the variability (e.g., number and dollar value) of the adjusting entries over time and to other similar entities. The concept of variability, over time, and against other audit entities is the key differentiating factor in continuous auditing versus continuous monitoring or embedded audit modules.

Auditors need to be considering questions like: How many journal vouchers were processed this year? What percentage was above the threshold amount? How does this compare to last year and to other audit entities? And, Can we tighten the criteria and lower the cut off value? Answering these questions will allow auditors to develop dynamic set of thresholds that provide a better idea of the direction in which the organization is headed, rather than simply identifying a transaction that failed to meet a static cutoff value.

Finally, continuous auditing supports the automation of follow-up of audit recommendations. With continuous auditing, auditors can track specific data-driven measures of performance to determine if management has implemented the agreed-upon recommendations and if they are having the desired affect. Tracking performance over time is critical to ensuring that the organization is being successful in meeting established goals and in identifying additional actions to be taken. It is an integral element of performance measurement and continued improvement in operations. Audit, through continuous auditing, can assess the quality of performance over time and ensure the prompt resolution of identified problems. Further, once the risks related to an activity are identified and activities to reduce such risks are undertaken, the review of subsequent performance (continuous auditing) can gauge how well the mitigation efforts are working. As the actions of an organization become more observable, continuous auditing facilitates the implementation of ongoing quality improvement and assurance.

The data-driven predictors of performance must be responsive to changes in performance, provide an early warning when performance is deteriorating, be easy to use, and not be resource intensive. They should help an organization answer three basic questions if the indicator goes “red”:

- What happened?
- What is the impact?
- What are we going to do about it?

Example of Continuous Auditing: Application to an Accounts Payable Department

While continuous auditing can be used in any area of the organization, a simple example involving accounts payable will illustrate the differences and strength of this approach. The example assumes that there are numerous separate accounts payable processing centers, of different sizes, performing similar functions. The example will be used to discuss four main aspects:

1. Identification and assessment of risk related to the accounts payable processes
2. Identification of trends related to performance and efficiency
3. Identification of specific anomalies and potential frauds
4. Tracking of the implementation of audit recommendations and their effect on accounts payable operations

In each case, the analysis would consider trends over time and compare the accounts payable sections to other accounts payable sections. Benchmarking against external A/P operations adds another dimension to the examination.

RISK IDENTIFICATION AND ASSESSMENT A wide variety of data-driven and non-data-driven risk factors should be included in the initial risk assessment. A comprehensive evaluation of business performance looks at cost, quality, and time-based performance measures. Cost-based measures cover the financial side of performance, such as the labor cost for accounts payable. Quality-based measures assess how well an organization's products or services meet customer needs, such as the average number of errors per invoice. Time-based measures focus on efficiency of the process, such as the average days to pay an invoice. It is also possible to determine, for each A/P section, the types of transactions and dollar amounts for each. For example, look at the number of correcting journal entries and manually produced checks; these are indicators of additional workload. The analysis will also tell you how many different types of transactions are being processed. Generally speaking, there is more complexity in operations when more transaction types are processed. You can also examine organization structure—reporting relationships, number and classification/level of staff, length of time in job/retention rates, and training received (these should be available from the HR system). The combination of this type of information with the transaction types and volumes can help identify areas of risk, such as a lack of trained staff to handle complex transaction types.

TRENDS IN PERFORMANCE AND EFFICIENCY When considering A/P, trends will easily identity performance and efficiency concerns.

For example, for each A/P operation, continuous auditing can easily determine:

- Number and classification/level of accounts payable staff
- Number of invoices processed by each user (either end of the spectrum [too many or too few] can increase risk)
- Average dollar cost to process an invoice
- Average number of days to process a payment
- Percentage of invoices paid late; percentage paid early (particularly telling if early payment discounts are not taken)
- Percentage of adjusting entries
- Percentage of recurring payments or Electronic Funds Transfer (EFT) payments
- Percentage of manual checks
- Percentage of invoices that do not reference a purchase order
- Percentage of invoices that are less than $500 (purchase card could be more efficient and less costly)

Efficiency measures allow you to compare one audit area to another in a variety of ways, as Exhibits 2.6 to 2.8 show.

The use of trends can help not only to identify problems, but also to recognize areas where improvements have been made. Exhibit 2.8 shows that Division D still has the highest percentage of invoices without a purchase order reference, but it has made considerable improvements over the previous year, whereas Division G's percentage has gone up.

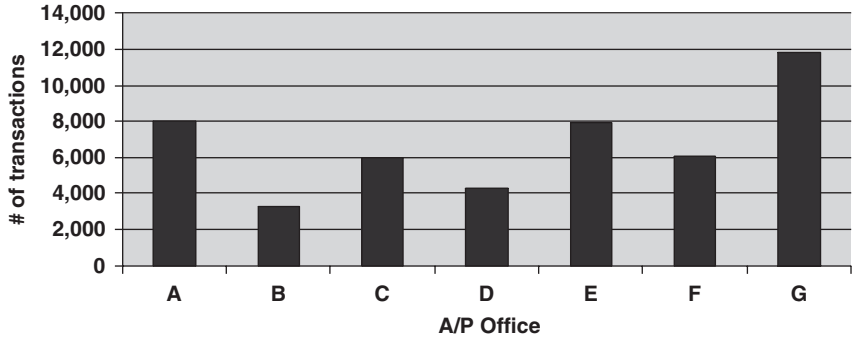

EXHIBIT 2.6 Average Number of Transaction per User

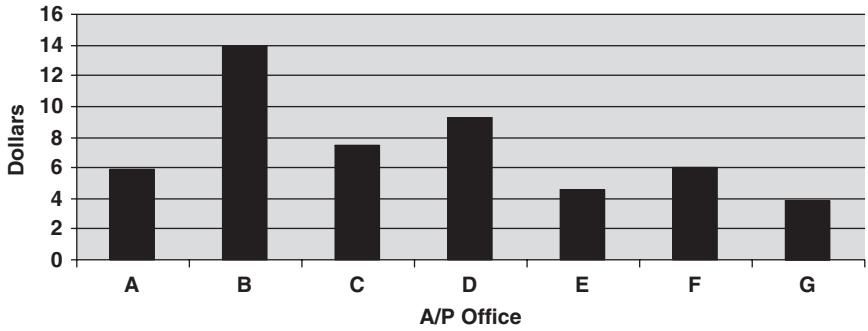

EXHIBIT 2.7 Direct Labor Cost per Transaction

IDENTIFICATION OF ANOMALIES OR POTENTIAL FRAUD Within A/P, possible anomalies and measures of potential fraud include:

- Duplicate payments (should include a comparison to previous years to see if operations are improving)
- Invoices processed against purchase orders that were created after the invoice date (backdated purchase orders)
- Number of invoices going to suspense accounts
- All functions performed by each user to identify incompatible or lack of segregation of duties
- Vendors that were created by, and only used by, a single accounts payable clerk
- Instances where the entry user is the same as the user who approves payment
- Instances where the payee is the entry or approving user

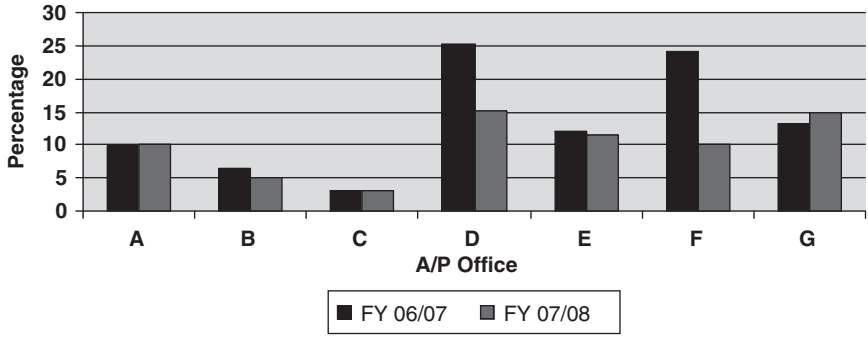

EXHIBIT 2.8 Percentage of Invoices without a Purchase Order Reference

- Duplicates in the vendor table or vendors with names such as C.A.S.H.; Mr.; Mrs; or vendors with no contact information, phone numbers, or other key information

TRACKING OF RECOMMENDATION The final area of continuous auditing is the tracking of recommendations. The aim is to determine if management has implemented the recommendations and if the recommendations are having the desired effect. Possible measures include:

- Evidence of increased used of purchase cards for low-dollar transactions (reduction in percentage of invoices less than $500 and increase in percentage of purchase card payments less than $500)
- Reduction in duplicates in the supplier master table
- Decrease in the number and dollar value of duplicate invoices
- Improvements in the days-to-pay figures (reduction in late payment charges and more opportunities to take early payment discounts)
- Improved operations (lower cost per invoice, more use of EFT payments)

Exhibit 2.9 shows how continuous auditing can be used to determine whether or not A/P operations in each division has successfully implemented the recommendations calling for purchase cards to be used for low-dollar transactions.

Stages of Continuous Auditing

Continuous auditing starts with the selection of audit projects, continues into the conduct and reporting phase, and culminates with the ongoing monitoring and follow-up activities. All stages of the process should be risk-based

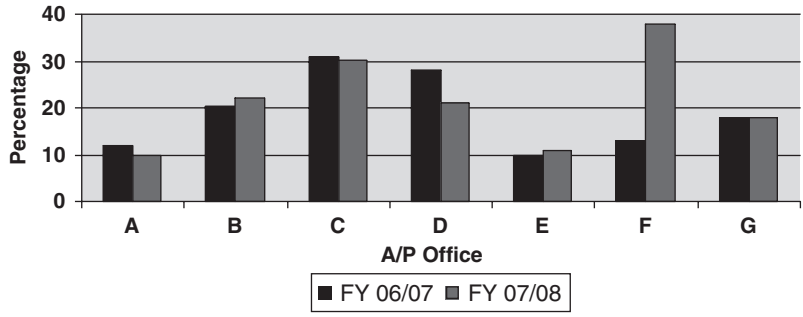

EXHIBIT 2.9 Percentage Purchase Card Use Invoices under $500

and, to the maximum extent possible, data-driven. The basic implementation strategy must include a consideration of the risk, an assessment of the baseline assurance, the design of the predictive indicators, monitoring for changing conditions, and follow-up as required. More detailed steps include:

Audit plan preparation and planning phase

- Identification of categories/areas of risk
- Identification of sources of the data to support risk assessment
- Understanding of the data and an assessment of its reliability
- Assessment of the levels of risk
- Prioritization of risk
- Selection of audit projects

Audit conduct phase

- Integration of audit procedures and technology
- Definition of relevant variables (predictors) to be measured
- Definition of the criteria for these variables to be used to predict outcomes
- Definition of the desired traits for the variables (normal range, anomalies)
- Measurement of the variables (predictors)
- Assessment of the predicted level of risk
- Follow-up audit activity as required
- Revision to variables that will be measured, criteria, and the traits

The implementation of continuous auditing will place certain demands on the auditors. The audit organization will be required to develop and maintain the technical competencies necessary to access and manipulate the data in the myriad of information systems. If the auditors are not already using data analysis techniques to support audit projects, the audit group will have to purchase analysis tools and develop and maintain analysis techniques. The implementation of continuous auditing will also require the adoption of the concept by all persons within the audit organization.

Monitoring and review is the final component of an effective control framework (the Committee of Sponsoring Organizations' five elements of a control component). It is a key ingredient in an organization's continuous improvement process and helps to ensure that the organization implements effective processes and tools to monitor and review relevant data. An effective monitoring and review environment uses both periodic reviews and those undertaken by internal and external audit, as well as built-in

review mechanisms and internal review measures. Continuous auditing will support and strengthen the monitoring and review environment in an organization. Finally, it will help focus the audit effort but will not obviate management's responsibilities to perform a monitoring function.

One of the current, and most visible, drivers for continuous auditing is the high cost of regulatory compliance. In the United States, a Financial Executives International survey (Financial Executives International [2005]) pegged the cost of SOX compliance at an average of more than $4 million per organization. Since most of these costs were related to manual, people-intensive processes—based on use of internal resources and external consultants—it is no surprise that an AMR Research study (AMR Research [2005]) found that key technologies can be used to reduce compliance costs by upwards of 25 percent. Continuous auditing can provide the necessary support to comply with SOX Section 404 by assisting auditors in the following areas:

- Determining the key controls and finding the balance between preventive and detective controls
- Determining whether deficiencies are material or not
- Integrating internal audit into the business processes to assess both emerging risks and control deficiencies
- Designing tests of IT and financial controls

In addition, an important step in reducing the cost of complying with SOX is more reliance on the work performed by a competent and independent internal audit function (Doyle, [2005]).

Continuous Auditing Template

Auditors wishing to develop a continuous auditing program will need to carry out these tasks:

Secure data access and maintain data quality:

- Develop and maintain access to key application systems.
- Understand the applications.
- Assess data integrity and reliability.

Develop and maintain analysis skills and tools:

- Purchase analysis tools (software and hardware).
- Develop and maintain analysis techniques.
- Share skills within your audit organization.

Anticipate all exceptions:

- With the area selected, identify the most critical reports to execute.
- Review the processing flow and past audits.
- Study best practices in the industry and secure insights from external advisors.
- Bring the key players together. Enlist the support of operation management to discuss the following:
  - The objective of the program or organization
  - An assessment of the effects of these risks, and what factors can increase risk
  - Tools currently used to monitor risks
  - The planned versus actual involvement of all pertinent personnel, in order to detect weaknesses
  - The process of creating a monitoring report

Prioritize and plan audit frequency:

- Use risk analysis to select high-priority areas.
- Determine which exceptions should be investigated and consider issues of timeliness versus effectiveness.
- Schedule audits and continuous auditing frequency in accordance with risk and time issues.

For each target, execute the plan:

- Select a suitable target for continuous auditing.
- Define entities and categories to be evaluated (account, and departments).
- Run the analysis and calculate the indicators.
- Compare results to previous periods as well as to similar entities within the organization.

Publish your results:

- Make results known to appropriate management.
- Monitor and evaluate effectiveness of continuous auditing process.

Sarbanes-Oxley

Corporate scandals and failures severely damaged investor confidence in the late 1990s. The Sarbanes-Oxley Act (SOX), named after Senator Paul Sarbanes and Representative Michael Oxley, came into force in July 2002. Its principles supported three main objectives: integrity, reliability, and accountability. SOX was created to ensure that financial records were complete

and accurate (integrity), that the information was reliable, and that management would be held accountable. By doing this, SOX's authors hoped to instill investor trust and confidence.

SOX introduced major changes to the regulation of corporate governance and financial practice, and set deadlines for compliance with the eleven "titles." This caused great anxiety in the business world as companies struggled to meet the deadlines; the most important sections are usually considered to be 302, 401, 404, 409, 802, and 906. In addition, an overarching institution, the Public Company Accounting Oversight Board (PCAOB), was also established by SOX, to provide guidance and assess compliance. The following summarizes the main requirements of the important compliance sections; however, anyone wishing to fully understand the compliance requirements should consult the full text of the Sarbanes-Oxley Act.

Important SOX Sections

SECTION 302 Section 302 deals with the requirement for periodic statutory financial reports to include certifications. Briefly, the certification must state that the report is accurate, complete, not misleading, and fairly represents the financial conditions of the organization; and it has been reviewed by the signing officers (usually the Chief Financial Officer and Chief Executive Officer). Since the CFO and CEO are responsible for the internal controls, they must also certify that these controls have been reviewed within the last 90 days. Further, Section 302 requires that all control deficiencies, significant changes to the controls, and related frauds must be disclosed.

SECTION 401 Section 401 discusses the need for financial reporting to be transparent. Quarterly and annual reports must be accurate and presented in a manner that conforms with generally accepted accounting principles (GAAP). These reports must include all material off-balance sheet liabilities, obligations, or transactions, and any relationships that could have a material impact on the current or future financial condition of the company.

SECTION 404 Section 404 states that the scope and adequacy of internal controls and procedures for financial reporting must be published in the company's annual report. The annual report must also include a statement regarding the effectiveness of the internal controls and procedures.

The annual report must also contain a statement from the registered accounting firm that attests to and reports on the effectiveness of the internal control structure and procedures for financial reporting.

SECTION 409 Section 409 deals with the reporting of material changes in an organization's financial condition or operations. It states that the information must be disclosed to the public in a timely manner (rapid or current basis). These disclosures should be easily understood by the public and be supported by quantitative (graphs) and qualitative information as appropriate.

SECTION 802 Section 802 discusses the fines and/or imprisonment (up to 20 years) for altering, destroying, or changing documents or tangible objects with the intent to affect the outcome or progress of a legal investigation. This section also imposes fines and/or imprisonment (up to ten years) for the failure to maintain audit or review papers for a period of five years.

SECTION 906 Section 906 discusses corporate responsibility for financial reports and outlines the criminal penalties the CEO and CFO could face for certifying a misleading or fraudulent report.

In the first few years, compliance with SOX legislation seemed to be a daunting task to many. However, those companies that addressed its requirements methodically found that compliance with SOX can be planned and implemented in a manner that not only meets the requirements but also helps improve operational efficiency and effectiveness. In many cases, auditors were asked to take a lead role in developing the necessary response to SOX. Further, organizations that integrated their financial statement and audits of internal controls over financial reporting achieved even greater efficiencies.

In response to concerns over the cost and effort required to comply with SOX, both the Securities and Exchange Commission (SEC) and the PCAOB offered additional guidance in the form of PCAOB Auditing Standard No. 5 (AS5) (PCAOB AS5 [2007]). This standard was written to reduce the overall burden of compliance, while addressing the main areas of financial risk. AS5 encouraged both management and auditors to use their judgment and develop a top-down approach to assessing risk. According to AS5, auditors should use a top-down approach to assess and select controls to be tested. Beginning at the financial statement level, auditors should develop an understanding of the overall financial risks and controls over financial reporting. They should start by focusing on the entity-level controls and then work down to the significant accounts, disclosures, and assertions. Finally, auditors should select for testing those controls that significantly address the risk of misstatement.

Instead of trying to identify and assess every possible fraud scenario, companies are encouraged to use informed judgment in developing a process of assessment that is realistic, defensible, and supported by a reasonable level of evidential matter. This means that the documentation and

testing of controls can be tailored to a company's own operations, risks, and procedures. The general intent of AS5 was to ensure that the compliance efforts were focused where they would do the most good, and that the process did not unduly interfere with the production of reliable financial statements.

The Role and Responsibility of Internal Audit

SOX Section 404 clearly states that management, not audit, is responsible for the system of internal controls. In fact, internal audit is considered part of an organization's internal control system. However, internal auditors have an important role in evaluating the adequacy and effectiveness of the control systems. The internal audit function provides senior management and the audit committee with independent assurance that the controls, risk management, and governance systems are working. Because of the unique position of the Chief Audit Executive, the internal audit function often has a significant monitoring role as well.

Under Section 404, management must assess the effectiveness of a company's internal controls over financial reporting and must include the assessment in its annual report. In addition, under Section 302, management must report whether the assessment has identified any material control deficiencies that could impact the company's financial statements.

Internal audit has a different role to play. Typically, internal auditors are encouraged to use a standard control framework such as the Committee of Sponsoring Organizations' (COSO) Internal Control–Integrated Framework (ICIF). The ICIF goes beyond the SOX requirements and covers all aspects of internal control, not just control over financial reporting. It states that an internal control is a process, affected by an entity's board of directors, management, and other personnel. Further, it promotes a process designed to provide reasonable assurance regarding the efficiency and effectiveness of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. The achievement of these objectives improves performance, profitability, the safeguarding of assets, and leads to more reliable financial statements and compliance with applicable laws and regulations.

The COSO framework describes the five related components of internal controls:

- *Control environment*. This includes integrity, ethical values, management's style and philosophy, and the competencies of the entity's people. The control environment sets the tone and is the foundation for the other components on internal control.
- *Risk assessment*. The process of identifying and assessing the risks to the achievement of corporate objectives. It also provides valuable input into the management of these risks.

- *Control activities*. The policies and procedures, at all levels of the organization, in place to ensure that management directives are followed. Control activities include formal approvals, authorities, separation of duties, and reconciliations.
- *Information and communication*. The processes to ensure that information is captured, synthesized, and communicated in a manner that is timely and helps people to carry out their responsibilities. It includes internally and externally generated information, and must occur at all levels of the organization.
- *Monitoring*. The processes that assess the quality of the management control framework. This includes ongoing monitoring activities and specific evaluations, such as audits. The feedback from the results of the monitoring processes is used to improve the system of controls.

COSO guidance gives internal auditors a framework upon which they can tailor their approach to the assessment of internal control over financial reporting. Because the needs of smaller companies can vary significantly from those of larger companies, auditors should consider the most efficient and effective manner of assessing risk. The COSO framework does this by allowing them to select the principles that best fit their company's circumstances. It provides management and internal audit with a tool to use in determining the appropriate level of internal controls over financial reporting. However, it is important to note that the framework can only provide reasonable—not absolute—assurance, and that any control testing is at a point in time.

According to the guidance, smaller public companies may strengthen internal controls by broadening the pool of audit committee members, using controls built into accounting software, leveraging management monitoring, and outsourcing some activities. This new guidance provides a tool for management to use in determining the appropriate level of internal controls over financial reporting for smaller businesses. The document is intended for use by board members, senior management, other personnel, and external auditors. The key is to identify and assess the appropriate financial risks.

Risk Factors

SOX requirements are focused on financial reporting; therefore, the auditor's objective is to express an opinion on the effectiveness of the company's internal control over financial reporting. Auditors must also consider whether identified errors are one-time failures or systematic deficiencies, such that the internal control system no longer provides reasonable assurance that material errors will be prevented or detected. To do so, the audit must obtain sufficient evidence about whether or not material weaknesses exist.

PCAOB AS5 states that the risk factors to be assessed are those that are indicators of the susceptibility of the account, disclosure, or assertion to misstatement due to errors or fraud. This refinement means that there is no need to assess and test every control—only those where the inherent risk of an error exists, that could lead to a material misstatement, are considered reasonably possible. This requires auditors to understand the nature of the business environment, the organization's operations and process, and to consider sources of potential misstatements.

In the first year of SOX, auditors were often testing controls that were not considered key because the controls did not prevent or detect material errors. By focusing the testing and evaluation on relevant entity-level controls, auditors can spend less time on control testing and achieve greater efficiencies. Additionally, efficiencies can be obtained by integrating financial statement audits into audits of the internal controls over financial reporting.

Instead of trying to identify and prevent every conceivable fraud, A5 encourages companies to use a risk-based approach to determining where to improve controls. This includes employing tactics to reduce the pressure, opportunity, and rationalization elements of fraud. Management should consider (1) changing performance bonus policies to eliminate the pressure to commit fraud; (2) performing continuous monitoring of the use of management override of controls; (3) setting the tone at the top with ethical behavior; and (4) developing fraud-awareness programs to help prevent fraud. At the same time, auditors need to be cognizant of the approaches to identifying and assessing fraud risk.

Detecting Fraud

Auditors are generally concerned with the evaluation of controls for the efficient and effective use of company resources. Sound controls are an essential part of any defense against fraud, but they may not be working as intended or may no longer be adequate. Reorganization, business reengineering, or downsizing can seriously weaken or eliminate controls, while new information systems can present additional opportunities to commit or conceal fraud. Auditors must also be constantly aware that mandated controls that are nominally in effect might be poorly enforced or otherwise irrelevant.

Auditors and fraud investigators must be conversant with the key conditions for detecting fraud. There are five such conditions:

- Determining the organization's risk of fraud by studying its operational and control environments to identify risk categories and exposures
- Assessing the risks and exposures

- Examining the risks and exposures from the fraudster's perspective, to determine what he or she can control or manipulate to make the fraud possible
- Thoroughly understanding the symptoms of fraud and data sources that may contain those symptoms
- Being alert to the occurrence of symptoms and knowing how to look for those symptoms in the data

Once these conditions are met, it becomes easier to deter, investigate, and report detected fraud and create new controls to detect any reoccurrence.

Determining the Exposure to Fraud

Auditors must be aware of the areas where their organization could be at risk and the possible impacts. Auditors must understand the various sources of risk and exposure that confront the organization, from the highest to the lowest levels. Risks that are poorly managed or not mitigated are an exposure that can be manipulated to benefit the fraudster. The prevention and detection of fraud will be improved by a thorough understanding of what could possibly happen to the organization in the normal course of operating its business, or as the result of some other unusual event. However, simply identifying all of the possible exposures, given the likely lack of resources to deal with them, is not sufficient. In order to focus audit attention and the prevention and search for fraud, auditors must not only identify, but also assess and prioritize the risks.

The first step is to develop loss scenarios that will define the types of fraud risk to which the organization may be exposed. Typical risk categories include the external environment, legal, regulatory, governance, strategy, operational, information, human resources, financial, and technology issues. The development of risk categories can help identify and assess the risks.

The assessment of risk includes the examination of the controls in place to mitigate against various risks, such as monetary loss, theft of assets, and loss of proprietary data. Auditors must examine the operational environment and its internal controls to identify where weaknesses and deficiencies can leave the company exposed to fraud. Under SOX, the primary fraud risks relate to financial reporting, and the system of internal controls must be carefully evaluated and tested to ensure it is working as intended. Processes, control points, key players, and risks must be carefully reviewed. Fraud is often largely a crime of opportunity, so the opportunities must be found and, if possible, eliminated or reduced.

Two widely distributed audit standards address exposure concerns directly. The Institute of Internal Auditors' (IIA) Statement on Internal Auditing

Standards No. 3 (SIAS 3), *Deterrence, Detection, Investigation and Reporting of Fraud*, requires auditors to have sufficient knowledge of possible frauds to be able to identify their symptoms. Auditors and fraud investigators must be aware of what can go wrong, how it can go wrong, and who could be involved. Also, the AICPA's SAS 99, *Consideration of Fraud in a Financial Statement Audit*, was developed to assist auditors in the detection of fraud. It goes further than its predecessor, SAS 82. New provisions include:

- The need for brainstorming the risks of fraud
- Emphasizing increased professional skepticism
- Ensuring that managers are aware of the potential of fraud occurring
- Using a variety of tests
- Detecting cases where management overrides controls

In most companies, the areas of highest risk involve the general ledger (GL) and revenue recognition. The GL is dynamic and requires adjustments, and revisions to accounts balances can be performed by authorized individuals. However, concerns can arise when management overrides the journal entry or revenue recognition policy or strongly encourages others to do the same; or journal entries can be deliberately split to bypass financial controls.

Looking at risk from a top-down approach may mean that current practices need to be revised. Auditors should consider the risk factors, including:

- Size and composition of the account
- Volume of activity
- Complexity and variability of transactions
- Nature of the account, disclosure, or assertion
- Accounting and reporting complexities
- Existence of third-party transactions
- Significant changes from the prior period

Testing for automated controls normally consists of one or more of the following:

- Control system walkthroughs to confirm the existence and adequacy of adequate control documentation and to assess whether the design meets the control objectives
- Processing of a sample of transactions to confirm that the control is operating effectively
- Examining related application code, including the configuration of control parameters

- Using audit software to test control rules (e.g., testing that transaction debits balance to credits, or searching for journal vouchers over the maximum amount permitted)
- Using audit software to perform parallel simulations of key portions of the applications processing, such as the use of ACL to age open accounts receivable transactions and compare with system-generated reports

Auditors should consider the risk factors for fraudulent financial reporting and theft described in SAS 99. These can be used as a basic model for assessing the risk of fraudulent financial reporting. The risks outlined in SAS 99 include factors such as management conditions, the competitive and business environment, and operational and financial stability. The risk factors for theft include employee relationships, internal control, and the susceptibility of assets.

The AICPA's Audit Standards Board has also issued eight Statements on Auditing Standards (SAS) dealing with the assessment of risk in financial statements. SAS 104 to 111 cover a wide range of topics including reasonable care, auditing standards, and evidence, and form a comprehensive set of risk standards. Together they provide guidance to assist the audit in determining the risk of financial misstatement caused by error or fraud. The standards support the design and performance of audit procedures aimed at detecting risk. In particular, they encourage auditors to develop an understanding of the audit entity, the system of internal controls, and the associated risks. Through this enhanced understanding and improved procedures, auditors can perform a more rigorous assessment of the risks.

Additional information on how to define and assess fraud risk can be found in the book *Computer-Aided Fraud Prevention and Detection: A Step-by-Step Guide*, also by David Coderre.

SOX Software

Initially, companies tended to view SOX compliance as either a financial reporting problem (Are the controls in place to ensure that we have not materially misstated our finances?) or an IT problem (Do we have access to the data we need to ensure compliance?). In fact, it is both. To ensure that internal controls are working, auditors need to drill down into transaction-level data, and IT needs to make this data accessible. SOX demands that cross-organizational teams be involved in the compliance process. Many companies realized that the rules required changes in both the IT and application infrastructures that support the business and the business processes. SOX teams often result in management, audit, and the IT department being involved in compliance discussions.

Since the Sarbanes-Oxley Act was enacted in law in 2002, audit and assurance software vendors have introduced new SOX tools or repositioned existing products for the SOX market. Considerable confusion existed in the marketplace as security, change management, and many other types of software firms marketed their products as SOX solutions. Typically, these products assisted IT departments in partially achieving specific control objectives, such as ensuring system security, but none were end-to-end solutions, and none were intended to comprehensively manage the controls documentation, assessment, and remediation processes required by SOX. The challenge for auditors in understanding SOX compliance software is that solutions can range from relatively simple spreadsheets to highly complex solutions, such as software to reengineer all business processes.

Companies are spending more on IT, business-process change, corporate governance, and/or consulting as a direct result of compliance with SOX. And more companies are using enterprise resource planning (ERP) systems or enterprise performance management tools not only to meet SOX requirements, but also to improve their own visibility into business operations. In 2004, most companies relied primarily on existing tools, particularly Microsoft Word, Excel, and Visio, to achieve SOX documentation compliance (*2005 Buyer's Guide* [2005]). For the most part, they decided to wait until after the first year of compliance to implement SOX solutions.

But this trend changed quickly, and software spending, roughly $2 billion in 2003, tripled by 2006, and is expected to continue to increase as companies gain a better understanding of their corporate governance requirements. To reduce the high labor costs associated with the compliance effort, more and more companies and audit departments are turning to software products that combine flexibility and power, allowing them to read and analyze data stored in a myriad of application systems.

Technology spending accounts for 28 percent of the $6.1 billion being spent in 2006 on SOX compliance, according to AMR Research. Companies want to use technology to lower the cost of compliance by building repositories of control documentation and data about compliance testing and assessments.

SOX software typically provides a capability for documenting the review of risks and controls over financial reporting and other operating risks, and for presenting this analysis to the external auditors. According to PCAOB Auditing Standard No. 2 (AS2), SOX software should include the definition of material accounts and disclosures from your financial statements, risk templates, controls review, discussion and follow-up of an action plan, and a complete framework for risk analysis. It should address the areas of risks and controls, and issue management. It should be capable of documenting issues, tracking remediation efforts, and maintaining accountability and continuity on specific task items.

There are several SOX tools, such as Risk Navigator, Enterprise Risk Assessor (ERA), ControlCase, Methodware, SarbOxPro, and OpenPages. Most SOX software products support the requirement to document a business process and to identify the associated risks and controls. They should assist the auditor who is performing tests of controls and documenting and reporting the results of these tests. Often SOX software will include a library of risks and controls that can be shared across the organization, allowing users to create a central repository of risk assessment and control records, both entity and activity based. This allows multiple users to track changes, share authorship, and distribute consolidated risks across the organization—reducing the amount of control and test documentation and making it easier to maintain the necessary documentation. The software should prevent unauthorized access and should track the history of control tests. Further, most SOX applications will analyze the underlying data, using pivot tables, to show trends over time. Typically, the applications are also equipped with a variety of graphical displays including color-coded "heat maps" of risk areas.

A key to meeting the Sarbanes-Oxley Act's requirements is to understand not only what software is out there, but also what is really needed. In addition, it is possible to start small and incrementally improve the level of technology-based compliance. Auditors must know how to use technology to reduce the amount of paper pushing, to automate routine tasks, improve data analysis, and continuously assess and identify risks and control deficiencies.

Assessment of IT Controls and Risks

One of the problems non-IT auditors experience is trying to determine when and how to test IT controls and risks. For decades, auditors have audited "around the box," satisfying themselves that the controls at either end of the computer application were working and assuming that the application controls were adequate. The only auditors who even dared to look at the application controls were IT auditors; however, the audit world has changed significantly in the past few years.

No longer are IT and business risks considered as separate entities. Auditors are encouraged to consider IT risks as business risks and to develop a more integrated approach to auditing. The COSO model for technology controls risk assessment component examines entitywide risks. It espouses the integration of IT and business risks, and encourages auditors to identify IT controls that operate in high-risk business areas/functions. Further, SOX stresses the requirement for all auditors to understand the business and IT-related risks and controls with respect to financial reporting. While IT general controls and processes do not have a direct impact on financial

statements, deficiency in these controls could result in material misstatements. Therefore, under SOX, business and related IT controls are important components of the assurance that financial reports and disclosures are accurate and timely.

SOX section 404 requires the CEO and CFO to report annually on the effectiveness of the internal controls over financial reporting. A substantial portion of the SOX Section 404 compliance costs are related to the assessment of IT controls over the protection of data and programs from unauthorized changes. This has lead may auditors to realize that, with the proliferation of application systems supporting all aspects of the business, auditors need more proficiency in determining which IT controls need to be considered. Auditors must have a sound methodology in place to help them determine the scope of IT risks that should be considered, as well as the related control activities necessary to mitigate them. Without a rationale for evaluating possible IT risks, there is an increased likelihood that the level of control testing will be either too little or too much.

How then do auditors determine the relevant IT controls and risk and whether they are perform too much or too little testing? Auditors can look for guidance in several publications from the IIA. In particular, they should keep in mind the importance of considering both the application and general computer controls. The IIA guide on information technology controls states that the objective of application controls is to ensure (1) that data is accurate, complete, authorized, and correct; (2) that it is stored and processed properly; and (3) that all output (such as financial statements) is accurate and complete. Application controls maintain a record that tracks the data, from input and storage, through processing and output (IIA—GTAG 1, Information Technology Controls [2005]). The application controls include input controls, processing controls, output controls, integrity controls, and audit trail.

In addition, auditors must consider the information technology general controls (ITGC), which apply to all system components, processes, and data. The ITGCs include controls over user access, the system development life cycle, change and configuration management, physical security controls, and system and data backup and recovery (IIA GTAG 8, Auditing Application Controls [2007]). The application and general controls form a large part of the overall business controls, and auditors must, therefore, understand both the business processes and IT applications and controls in order to identify the key controls where a weakness or deficiency may result in a material financial statement error.

The PCAOB has provided additional guidance in the form of Auditing Standard 5 (AS5). This standard encourages auditors to use a top-down, risk-based approach and to focus their compliance efforts on those areas that present the greatest risk of fraud. Further, Auditing Standard 2 (AS2)

encourages auditors to start by evaluating and understanding the entity-level controls, such as governance, standards, policies, and procedures, and to identify significant accounts, locations, and assertions. The next step in the top-down approach is to determine which business processes could affect these significant areas and to identify the points at which material misstatements or fraud could occur. This will assist the auditor in focusing on the key application and general controls rather than assessing all systems and their controls.

Another important source of direction is the IIA's guide to the assessment of IT risks and Controls (IIA, Guide to the Assessment of IT Risks [GAIT] [2007]). While GAIT is not a control framework, it does provide auditors with guidance on the scoping of the IT general controls, assisting them in determining what should be included when they must provide assurance that the internal controls over financial reporting are adequate.

GAIT provides a principles-based approach to examining IT risk and controls that makes it easier for non-IT auditors to understand how business process and how the related IT systems can affect the accuracy and timeliness of financial reporting. According to GAIT, the greater the potential impact, the more the auditors need to include the IT system in the scope of the work performed to certify the financial statements. For example, auditors should include controls over the proper operation of IT applications and the protection of both the data and the application programs from unauthorized change of systems, particularly if the IT system outputs are a material input into the financial reporting process.

The principles-based approach encourages auditors to examine IT risks and controls from a top-down perspective, starting by considering which business processes should be included. By identifying the business processes with the highest risk of impacting the financial statements, auditors can focus their efforts on identifying the key controls and the amount of testing required to provide assurance regarding the accuracy, completeness, and existence of the transactions. A key control is one that, if it fails, has at least a reasonable likelihood that a material error will occur in the financial statements (IIA—SOX Section 404 [2008]).

GAIT also encourages auditors to examine the different types of controls—preventive, detective, and corrective—and the degree to which these controls are either automated or manual. A higher level of assurance can be attributed to automated detective controls if they are working properly.

Defining the Scope

Auditors must define the key controls that should be included in their assessment. There are two main approaches to defining the scope of controls.

The first is consistent with the top-down approach and starts with the identification of the key GL accounts that make up each line in the financial statement. Auditors should assess each account and determine if it is significant. For the significant accounts, it is important to identify the business processes that generate the transactions and to determine the underlying information system. The key controls to be assessed will be those that address the integrity of the key transactions (IIA—SOX Section 404 [2008]).

The second approach to determining the key controls that should be considered starts with identifying the financial statement assertions. AS5 requires that relevant assertions must be assessed. The assertions suggested by AS5 include:

- *Existence*. Verify that assets or liabilities exist and that transactions occurred during the reporting time period.
- *Completeness*. All transactions and accounts are included in the financial statement.
- *Validation*. Appropriate amounts have been used.
- *Rights and obligations*. Verify they exist and are for the proper period.
- *Disclosure*. Financial statements are properly classified, described, and disclosed.

One approach to identifying key controls relevant to these assertions starts by listing all risks that may prevent the assertions from being satisfied and identifying the controls that address the risks. A second approach identifies the material transactions that affect the assertions and identifies the appropriate controls over these transactions. In either case, by determining the relevant assertions, auditors can identify the associated accounts and appropriate key controls. This supports auditors in determining the scope—the material transactions together with the business process and the automated and manual controls—to be assessed (IIA—SOX Section 404 [2008]).

GAIT Principles

GAIT is a principles-based approach and is strongly linked to the IT-related sections of the COSO internal control objectives. The four principles define the set of IT assets (applications and business processes that depend upon these applications) and the transactions that affect those assets. Defining the relevant IT assets helps auditors determine the scope of IT risks, controls, and processes that must be assessed to provide the required level of assurance.

The first principle is an extension of the top-down risk-based approach promoted in AS2. In particular, auditors are encouraged to consider the risks related to the IT general controls for accounts deemed to be significant. A

top-down risk assessment should be used to identify the areas that are most prone to fraud or financial errors, and then the relevant application controls should be evaluated. This leads to the second principle, which discusses the IT general control processes that also need to be tested. Consistent with Section 404, auditors are directed to assess risk in those IT general controls where impairment to the application system's functionality could result in material errors in the financial statements or in fraud.

The third principle discusses the areas where IT general control risks could exist. GAIT encourages a layered approach, examining risks in application code, databases, operating systems, and networks. However, the auditor must also test system processes, network scans, and the change management, system operations, backup and recovery, capacity planning, and physical security. However, in doing so, GAIT encourages auditors to consider the controls as a whole, rather than the individual controls (principle 4). Taken in their totality, the IT general controls and processes should support the business process and, indirectly, contribute to sound financial statements.

Traditionally, auditors were able to ignore the IT systems and audit "around the box"; however, the integration of, and dependence of business processes on, IT means that this is no longer an option. GAIT assists auditors in determining when it is appropriate (and preferred) to address the IT controls and processes directly. With a clear understanding of the business processes and the related IT systems, auditors can use the GAIT principles and structured approach to scope in or out application systems (IT assets). For those applications that are scoped in, the methodology can help auditors focus on the specific IT transactional processes that need to be assessed and the key risks and controls.

Auditors wishing to know more about the assessment of IT controls and risks should refer to the IIA's *Guide to the Assessment of IT Risks* (GAIT).

Governance, Risk Management, and Compliance (GRC)

Corporate failures and scandals over the past few decades have resulted in reforms, regulations, and laws aimed at improving transparency and accountability in today's business environment. More than ever, organizations are being challenged to conduct operations in a manner that not only meets objectives, but also addresses compliance and the expectations of stakeholders. In response, high-performing companies are integrating their governance, risk management, and compliance (GRC) activities to make them more efficient, effective, dependable, and legally sound. The basic components of an integrated GRC process are the identification and assessment of

risks and controls; however, without a robust governance model and the proper tone at the top, GRC will not meet its expectations.

Governance is a difficult concept to grasp. I like to use the analogy of driving a taxi (the organization) that contains several passengers (the stakeholders), not all of whom want to go to the same destination. The driver (management) must:

- Know where the passengers (e.g., investors, business partners, public) want to go and how they would like to get there (understand their motivations and expectations)
- Respect the rules of the road (laws and regulations)
- Monitor the taxi's gas, oil, temperature, brakes, etc. (internal operations)
- Consider the road conditions and actions of other drivers (external environment)

By addressing all of these factors, the driver will ensure that the taxi makes it to its final destination (meets the desired goals and objectives).

Looking at it from the corporate perspective, management plans, directs, and organizes the activities of the organization to provide reasonable assurance that the stated goals and objectives will be met. Management is also responsible for the ongoing health of the organization and is accountable to the owners, stakeholders, regulators, and public. To deliver on these accountabilities, senior management develops, implements, and maintains processes to ensure that financial and operating information is accurate and timely, and that the organization uses its resources efficiently and effectively. In addition, management is responsible for the identification, assessment, and management of risks, as well as compliance with ethical norms, rules, laws, and regulations. Lastly, assets must also be properly safeguarded. When all of these processes are working together, the achievement of goals and objectives is possible.

Management also develops and maintains the tone of the organization, including the organizational culture and ethical responses to stimuli. These form the basis of the GRC assurance functions that, until recently, have been separate from the main business functions and decision-making processes. From an audit perspective, a periodic review of the GRC processes, and implementation of required modifications, will help the organization adjust to changing internal and external conditions (IIA Practice Advisory 2100-1: Nature of the Work [2001]).

Audit needs to ensure that GRC is treated via an entitywide approach. This will support good governance, the ongoing assessment of the risk management framework, and compliance with applicable laws and regulations. The notion of entitywide controls is not a new concept. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission

introduced its Internal Control Framework in 1992, more than fifteen years ago. The concepts of risk management and compliance are not new either, but the past decade has seen a much greater focus on risk and compliance. Regulations and acts, such as Sarbanes-Oxley and Basel II, have had a huge impact on organizations on a global basis. Compliance costs alone have risen sharply with the ever-increasing volume of rules and regulations. However, the main reasons for the increased cost are operational inefficiencies: the efforts to comply have often resulted in duplication because of silo mentalities and approaches. This has caused many organizations to look beyond the compliance requirements and regard GRC as an integrated process.

Treating GRC as a single process requires careful analysis to ensure the proper integration, across organizational functions. The cost and effort of combining the GRC activities are huge, and, while the benefits are significant, they are not easily derived. It is important to involve a cross-section of the organization's people and to use consistent technology and data. Additionally, the GRC process must be robust enough to deliver on, and remain flexible enough to adjust to, new and changing regulatory requirements.

Many challenges are inherent to integrating the GRC processes. One of the most critical steps is understanding what information needs to be collected and monitored in order to implement an effective and efficient GRC process. Many companies collect and store a vast amount of financial, human resources, and operational data. Understanding which information can support ongoing GRC efforts is not an easy task. Audit can make a significant contribution because the process will require cross-functional cooperation and a common understanding of the need for, and importance of, GRC. In addition, auditors can help organizations develop a common language for GRC and ensure that the GRC processes are incorporated into the core business processes and management decision-making processes. Linking the GRC and business processes will reduce the data collection and analysis requirements.

Traditionally, governance, risk, and compliance were handled in separate departments: Legal addressed the legal and regulatory risks; the Chief Compliance Officer addressed compliance issues; the Chief Financial Officer addressed the finance risks; and the Chief Risk Officer independently addressed enterprise risk management. The result was a significant duplication of effort—with some processes and procedures being assessed three different times and varying standards and terminology being applied by the separate reviewers. But an integrated approach to managing the GRC requirements of the organization, with a common taxonomy and an integrated review schedule, can maximize not only the GRC processes, but also can improve operational efficiency and effectiveness. An additional benefit of an integrated approach is the change from a reactive response mind-set of

assembling teams of people to respond to a specific crisis to a proactive process that seeks to identify potential risks, and critical compliance issues and controls, before the crisis happens.

Internal Audit's Role in the GRC Process

The GRC process should be enabled by a collective suite of management processes and controls that set strategic direction, objectives, plans, and priorities. Implementing an integrated approach will bring internal audit, human resources, finance, legal, procurement, information technology, and other stakeholders together with a common goal: identifying potential risks and the controls necessary to manage those risks. The GRC process provides an oversight function to ensure that management's direction, plans, and actions are appropriate and responsible; audit's assessment of this process will provide the necessary assurance to internal and external stakeholders, and help the organization meet its regulatory requirements.

Internal audit performs an independent assessment of the management GRC processes to determine whether there is reasonable assurance that the overall goals and objectives will be met. To do this, internal auditors must consider emerging areas of risk, the effectiveness of management's monitoring programs, and the adequacy of management's response to identified risks. Internal auditors should use a systematic approach to the evaluation of risk management, control, and governance processes. They should also assess management's performance in carrying out assigned responsibilities. The purpose of an audit of the GRC process is to provide reasonable assurance that these processes are functioning as intended and will contribute to the achievement of the organization's objectives and goals. GRC audits can also provide management with workable recommendations for improving the effectiveness and efficiencies of operations.

As a primary task, audit should seek to ensure that the integrated GRC process builds on existing frameworks and processes rather than inventing new procedures and processes. Typically, auditors will have already examined the risk management practices of numerous areas of the organization, either during audits or as part of the process to develop the annual risk-based audit plan. Knowledge of existing risk management processes is important to identifying the key players, the areas not currently being assessed, and areas of duplication. Auditors can use this knowledge to assist management in reducing both the resistance to change and the duplication of effort by ensuring that GRC processes are aligned with existing organizational competencies, processes, and structures.

Audit review can help ensure that the GRC activities use a common language and approach that encourage integration and collaboration. For example, consistent definitions for likelihood and impact will allow the

comparison of differing types of risk across the organization. Audit can also assess the degree to which the GRC processes are integrated and duplication is avoided. Risk information should be shared and communicated to all areas of the organization, reducing gaps and overlaps. Audit should also be aware of the schedule of risk management activities. Synchronizing risk activities with the planning cycle can lead to quicker risk-intelligent decisions that are supported by timely information and analysis. Finally, audit can help ensure that the GRC activities are embedded in the key business processes and procedures. GRC should not be a necessary evil or an extra step that is taken simply to comply. Audit can assess the degree to which GRC has become institutionalized and is part of the decision-making and strategic planning processes.

The scope of GRC audits requires a disciplined approach that seeks to provide assurance regarding the adequacy and effectiveness of risk management, control, and governance processes. In assessing GRC processes, it is useful to consider the following standard definitions for adequacy and effectiveness:

Adequacy. Refers to the plan and design of the GRC processes. Adequacy seeks to determine if management has put into place plans that are designed so as to provide reasonable assurance that the goals and objectives of the organization will be met efficiently and economically. The plans should provide assurance that the organization's activities and process are timely, accurate, and economical, using resources that are commensurate with the risk exposure.

Effectiveness. Refers to the degree to which the GRC processes contribute to the achievement of the organization's goals and objectives. Effectiveness seeks to measure the impact that the risk management, control, and governance processes have on the organization's overall performance.

A GRC audit seeks to provide reasonable assurance that the processes and activities are cost-effective and designed and implemented to reduce risks to an acceptable level. Historically, this type of internal audit has often been called a management control framework (MCF) audit. It examines the totality of business systems, operations, functions, and activities and the processes management have established to manage them. The MCF audit considers whether the cross-functional activities are operating together to achieve the established objectives and goals. A GRC audit should accomplish the same objectives.

The comprehensive scope of GRC audits allows auditors to provide reasonable assurance that (1) management has designed and implemented an effective system for identifying, assessing, and managing risk; (2) the system of internal controls is adequate and operating as intended; and (3) the

overall governance process is working properly. While audit has been performing integrated GRC audits under various names for years, only recently has management integrated the governance, risk, and compliance processes and procedures. Previously, these management functions existed under separate organizational silos, making it difficult for audit to provide reasonable assurance that GRC processes were adequate and effective. However, the integration of GRC processes has provided internal audit with a single point of contact and has improved management's accountability for addressing audit recommendations.

The assessment of the GRC activities and processes should include a review of the risk management and the system of internal controls. The Chief Audit Executive (CAE) should develop a risk-based audit plan that ensures the sum total of the audit activities will be sufficient to evaluate the effectiveness of the risk management and control processes. The coverage of the annual plan should address all key operating units and business functions. In performing the planned audits, the risk management processes should be assessed during the conduct of individual audits and through an audit of the risk management process itself. Finally, the annual plan should be reviewed continually to ensure that it addresses changes in the internal and external risk environments.

Identifying and Assessing Management's Risk Management Process

As part of the GRC process, audit should consider the potential for internal or external changes to negatively impact the organization's performance. This requires auditors to assess the adequacy of management's risk management processes. Are these processes sufficient, and are they responsive to risks that could affect the assets, reputation, and ongoing operations of the organization? The IIA professional standards state that risk management is a key responsibility of management. Management is responsible for designing and implementing adequate and effective risk management processes (IIA Practice Advisory 2110-1: Assessing the Adequacy of Risk Management Processes [2001]).

At the same time, internal audit has a role to play in assessing and improving the methodologies and controls employed by management to address risks. In particular, internal auditors should provide management with assurance that management has established risk tolerance levels and performs ongoing monitoring activities to reassess the risk processes and effectiveness of controls. Audit should provide assurance that management's processes ensure that risks are properly identified, assessed, and managed.

Internal auditors should recognize that the risk management process will vary from organization to organization. They must consider the size and complexity of both internal and external environments, as well as the

organization's culture, business objectives, and management style. Further, the risk management costs should be commensurate with the underlying risk. In evaluating the risk management process, audit should consider the organization's risk appetite; the effectiveness of management's risk-mitigation and control-monitoring activities; and the timeliness, appropriateness, and completeness of actions taken to address identified risk.

Assessment of Internal Control Processes

As new regulations requiring senior management to document and attest to the effectiveness of the control environment and the accuracy of the information contained in financial reports are enacted, CEOs and CFOs are turning to internal audit to assist in complying with these regulations. Although management is responsible for the assessment of the control processes in their respective areas, internal and external auditors provide assurance about the effectiveness of the control processes. The IIA Practice Advisory 2120 states "audit should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvements" (IIA Practice Advisory 2120.A1-1: Assessing and Reporting on Control Processes [2001]).

The combination of all audit work performed during the year should contain sufficient information to permit the CAE to provide an opinion on the overall state of controls. This opinion should address the degree to which the internal control processes ensure (1) the accuracy, timeliness, and reliability of financial and operational information; (2) that operations are performed in a manner that is efficient and contributes to the effective attainment of desired results; (3) that assets, including personnel, are properly safeguarded; and (3) that the organization complies with applicable laws, regulations, and contracts (IIA Practice Advisory 2120.A1-1 [2001]).

The challenge for internal audit is to consolidate the many audit activities performed during the year to arrive at a holistic opinion on the state of the risk management and controls processes of the organization. In forming this opinion, the CAE must consider the extent to which audit has identified significant control weakness and management's response to the audit recommendations. Were the audit findings understood by management, and was the implementation of management action plans given sufficient priority? In short, did management adequately address the audit findings? In addition, the CAE must determine if these weaknesses were isolated instances or an indication of a systemic problem.

The pressure on audit to do more with less is increasing. Perhaps the most difficult challenges are for audit to provide timely assurance on the effectiveness of internal controls, to better identify and assess levels of risk, and to quickly highlight noncompliance with regulations and policies.

GRC Software

Computer-assisted audit tools and techniques (CAATTs) can assist auditors in performing many types of audits, including financial, operational, compliance, and GRC audits. In particular, they can assist in performing an analytical review of the GRC processes, tests for compliance with general and application controls, and trend analysis to identify emerging areas of risk. In fact, the audit evidence may be largely based on data analysis; therefore, it is important to ensure that the tests are properly planned and executed.

During the planning phase of the GRC audit, the auditor should consider the audit team's knowledge of the underlying systems and the analysis software. The auditor must also consider the efficiency and effectiveness of electronic analyses over manual methods, the integrity of the information system, and its data (IIA Practice Advisory 1220-2: Computer Assisted Audit Techniques [2005]). Finally, it is important to assess the integrity, reliability, and appropriateness of the analyses before relying on the results.

Leading organizations are leveraging technology to integrate the vast array of GRC activities. As a result, more software companies are developing GRC audit software. GRC software can support the dismantling of organizational silos by enforcing the use of a common taxonomy, encouraging ownership and accountability for risk processes, and enforcing the use of a framework for a common risk management approach. GRC software, such as Paisley's GRC Solutions, provides a common point of entry and a single data model that can be shared by internal audit, risk management, and compliance teams. GRC software enables common definitions and organizational reporting structures, which reduce duplication and help ensure consistency and efficiency.

An integrated GRC platform addresses the full range of risks (regulatory, HR, financial, and operational) as well as SOX compliance and internal audit requirements. It typically supports processes related to the documentation and testing of controls, the identification and assessment of risk, and the ongoing assessment of GRC and related internal audit activities.

GRC software unifies risk and control activities to ensure the effective documentation and sharing of information to serve the needs of varying stakeholders. This encourages ownership and accountability while facilitating the identification, assessment, and monitoring of key risk information. For example, Protiviti's Governance Portal provides a single, consistent source of risk and control information; the ability to assign risk and control to operational objectives; and linkages between global and process-level controls. The Portal also provides workflow processes to simplify the process of documenting and testing controls, the tracking of remediation efforts, and ongoing accountability for the GRC activities. It streamlines the

assessment process and facilitates management of the large volumes of data required to keep all GRC processes up-to-date.

Auditors should be aware of, and constantly assess, their requirements and the emerging capabilities of GRC software.

Summary and Conclusions

Many software vendors are willing to sell their packages to any user (even such critical, discerning, and skeptical ones as auditors!). Many such packages are specifically designed to perform audit or audit-related tasks. These software packages can be used to assist not only audit management but also individual auditors and whole audit teams, if they have the conceptual understanding and imagination required to make creative use of the technology. In fact, the issue is one of mind-set rather than technology. The type of microcomputer CAATT employed is only limited by the imagination of the user. As the use of microcomputers becomes more prevalent in audit organizations, new tools and techniques will continue to be developed. What seemed to be "Star Wars" technology yesterday is already commonplace in many organizations. In the early 1980s, a microcomputer with 20 Megabytes of hard disk space and 624K of RAM felt like overkill. Today, microcomputers have more power than early minicomputers and support peripherals such as tape drives, CD-ROMs, DVDs, and more.

What does the future hold? No one can be sure, but auditors had better be positioned to take advantage of what is offered, if they expect to be recognized as value-adding partners in the organization. Making productive use of computer resources to provide critical and constructive assessments of the organization's structure and performance is now a task for all auditors.