June 1987

EDP in the Audit Workplace
EDP IN THE AUDIT WORKPLACE
An annotated bibliography

Compiled by Rennese Hogue
June 1987

U.S. General Accounting Office
Office of Library Services
OLS-87-025
INTRODUCTION

As part of the continuing progress made in the field of technology, auditing methods have been enhanced through the use of computers and data processing. The books, articles and reports cited in this bibliography emphasize the use of electronic data processing (EDP) in the audit process and its importance to auditors, management, private business and government.

The bibliography is divided into six sections: auditors, EDP application systems, micros, portables, security and software. In these sections citations are provided to literature in EDP training, standards, various types of audits (practical, operational, financial, etc.), spreadsheets, DP management, fraud, password usage, security procedures, computer assisted auditing techniques (CAAT), software, legal issues, career alternatives, controls, methodologies, system design, cost effectiveness, encryption, and system audits.

The citations contained in this bibliography are to literature published from 1983 through August 1986. Sources for these citations include the following databases:

- Accountants Index
- ABI/Inform
- Computer Database
- Books in Print
- GAO Documents Database
- GPO Monthly Catalog
- Harvard Business Review
- Microcomputer Index
- NTIS
- SCORPIO

Unless appended with the editor’s initials, the abstracts were taken from these databases.

Most of the items cited in this bibliography are available to GAO staff through the Technical Library (275-5180).
AUDITORS

1. "4GLs Add to Internal Control Issues." Computerworld Australia, Vol. 6, No. 48, June 1, 1984, p. 16.

Auditors should be aware of the procedures used in developing reports and databases with fourth generation languages (4GLs). Because of the increased user involvement, a separation of authority and responsibility within the operation needs to be maintained. The development of information centers should be watched carefully in order to insure the use of proper controls.

2. "Auditing Conflict 'Necessary'." Computerworld Australia, Vol. 6, No. 48, June 1, 1984, p. 16.

Walter Adamson, a speaker at Edpac '84, stated that conflict is necessary between data processing departments and auditors. Therefore, auditors must learn how to manage the conflict. The conflict shows that people are doing their jobs effectively. Ways to manage conflict without eliminating it are discussed.


PC-Audit Card is an add-in board available from Bay Computer Corp. for $239. The product includes a half-slot easy-to-install with its own 16k RAM and all attendant software needed to provide a mainframe-style audit trail of PC usage. PC-Audit contains a gate-keeping function which requires that users sign on with passwords, and in the background it keeps a detailed audit trail which can be printed out and translated using some slightly obscure commands. However, once the string of commands has been entered, it can be saved for execution again at a later time. Lawyers and accountants will find the product very useful when billing clients for computer time, and systems managers will also find it useful for a number of needs including the ability to control user access to PCs to certain times of the day.


Several organizations are experiencing communication differences between MIS/dp managers and auditors. Although data processing auditing is crucial in controlling fraud and costs, many dp managers and auditors tend to work
independently, rather than as a team. Auditor misconceptions and realities are explored. A table shows auditing software packages' vendors, requirements, and price.


This article gives a concise explanation as to Statement on Auditing Standards (SAS) No. 48, "The Effects of Computer Processing on the Examination of Financial Statements", effective 8/31/84. This statement supersedes SAS No. 3. Guidance is given on the audit procedures, supervision by a professional with computer-related knowledge, accounting controls, and review of general control procedures. Useful to the auditor with no computer background or little EDP procedures knowledge. (RH)


EDP auditing involves verifying controls and identifying exposures. EDPA essentially looks for the possibility of loss and the degree of risk involved. Seventy per cent of the time is spent in gathering information by use of questionnaires, checking documentation, checking the source code, and testing masterfiles. Auditing software is important too. Internal auditors keep a close watch on the EDPAs to assure that they are going about their duties properly and checking the areas that most concern management. (RH)


Information systems planners at Peat, Marwick, Mitchell and Company use 3500 Macintosh computers in the auditing department. They were selected for their portability and ease of use. The accounting firm plans to create a network linking the Macintoshes with its IBM Personal Computers and word processors.


User training presents a dealer as a full-service retailer and enhances aftermarket sales. Spreadsheets require user training. Users must learn logical consistency, integrity,
and data consistency in order to use spreadsheets successfully. Users should be taught to work up a model, audit it, create an audit trail, establish change procedures, and reaudit the changes.


EDP career paths are discussed in terms of the future. A general outlook demonstrating the technical requirements and skills that will be needed in the year 2000 by auditors is discussed. These requirements will cover telecommunications, teleprocessing, microcircuitry, systems technology, laws and legislation concerning privacy, security, fraud, interstate data transfer as well as international data transfer. Efforts must be made in terms of training and skills to see that the auditor of the future will have the necessary background to effectively use the advance technology upcoming in the audit environment. It is this background that will alternately advance the auditor into various career opportunities. (RH)


Covered are more than 400 terms and their definitions, in relation to EDP auditing. Definitions are those that are commonly referred to in the DP environment and will prove useful to anyone needing basic EDP terminology. (RH)


Presented are guidelines for creating and implementing an EDP audit career. The six elements needed for a successful career development plan are: career path planning and management support, performance standards, performance measurement, performance counseling, training, and professional development. (RH)


Discussed is the current use of computer-based information.
systems as a replacement for paper as a storage medium. Due to the decentralization of these computer-based information systems there is the need for auditors to have necessary skills in order to perform efficient and conclusive auditing tasks. Skills discussed include specific knowledge, training methodologies, training programs, and matching training to corporate needs. (RH)


Gorham gives an account of how the EDP auditor evolved from the so called "auditor," due to an altered work environment imposed by today's technology of computerized information. Functions relating to the EDP auditor encompass the areas of software system review, timely and accurate data in production systems control, review of operations procedures relating to computer operations, systems life cycle, security and all other relevant forms of control responsibilities involving EDP services.


The role of the EDP auditor is discussed in the purchasing of the microcomputer. Involvement is discussed at each level of purchase before and after installation of the micro in accordance with company policies. Involvement should be maintained at all levels including follow-up procedures and periodic physical inventory of hardware, software, etc. Steps are given in the purchase procedure as well as the auditors' role in this process. (RH)


The Association of Data Processing Service Organizations, Inc. (ADAPSO), in another move in its continuing battle with the Big Eight accounting firms, has filed a petition with the United States Securities and Exchange Commission (SEC) asking for a more definitive ruling relating to the ability of accounting firms to offer data processing services and products to their audit clients. Adapso has maintained for years that a certified public accounting firm's providing data processing services to its audit clients constitutes a violation of SEC and Federal Trade Commission regulations designed to ensure the integrity of external audits.

This article discusses how auditors can audit in a computer environment. Described is the essential information that an auditor should look for, how the auditor can efficiently obtain information and how he or she can effectively evaluate their findings. (RH)


A forum, sponsored by the Institute of Internal Auditors, dealt with the difficulty advancing technology poses to those charged with auditing computer based financial records. Auditors are also concerned about the security of corporate information assets. Auditors do not really know how to control microcomputers and the portability of floppy disks. At present, responsibilities are organized in such a way that auditors have little chance to keep up with technology.


When Blue Cross/Blue Shield looks for a data processing auditor, the successful candidate must possess data processing skills (including COBOL, PL/1, and OS/JCL), a knowledge of accounting, a personality suited to dealing with defensive people, and writing ability. A data processing auditor should also be familiar with data base management and system design. At Blue Cross/Blue Shield, an auditing staff of nineteen is responsible for overseeing 1,100 data processing workers, five mainframes, twenty-seven minis, and nine word processors.


A new guideline for audits of an on-line environment has been published by the American Institute of CPAs. It helps the auditor understand the on-line environment and the impact it has on auditing procedures. Several practical suggestions are given for audit strategies of on-line environments.
20. "Portables Let Auditors Bring the Office to Their Work." 
Computerworld, Vol. 19, No. 17, April 29, 1985, p. 26SR.

Auditors at the Houston office of Price Waterhouse & Co. have access to a pool of about fifty Compaq portable computers. The auditors, who spend about seventy-five percent of their time on location, use the micros to check accounts receivable, count inventories, and check reconciliations with the client's bank. Price Waterhouse is working to make the portables used at client locations self-sufficient by outfitting them with all the necessary programs— in many cases by going to hard disk.


An auditing firm, McGladrey Hendrickson, selected Informatics General Corp's Mark IV processing language. The language was used to write, test and execute the company's own program. The high level language allowed the auditors to accomplish their own data manipulation.


Due to GAO's ever changing role since it's inception in 1921, the use of computers has become an integral part of its operation. Reigle gives a brief history of GAO's changing role and how this change has brought about the need for ADP skills among evaluators as well as their role in the ADP audit. (RH)


Data processing auditing today is a profession undergoing slow but steady change. In the years since it has been accepted as a separate area DP auditing has continued to receive more recognition and move up within the corporate hierarchy and pay scale. In the future, however, DP auditors must be prepared to adapt their skills and talent to new fields. As their salary progression levels off many DP auditors will move into other areas of DP management such as data security and data base administration. Others will be forced to do so by the integration of company auditing functions. Preparing for change is the only way DP auditors can successfully continue their career advancement.

The first time an audit is done in a data processing department there will probably be a lot of resistance to it. It becomes the auditor's responsibility to establish a working relationship with the auditee as well as to conduct the audit. Among the techniques for overcoming resistance to a first-time audit is establishing a liaison with the auditee. However, the auditor must take care to maintain control of the audit.


Data communication systems are increasing along with general data processing. It has become necessary for auditors to understand the workings of data communications systems. The basic units comprising a data communication system are reviewed. Access methods and protocols involved are discussed. The primer is aimed at giving a general understanding of a data communication system.


Since it is assumed that the life cycle costs increase as additional changes are made within a system it is proposed that requirement definitions be a focal point of monitoring in application design, software construction, certification and installation following thereafter. A discussion follows in which requirement documents and user statements are the source for which this application review is to proceed. It is the purpose of these documents to guide design efforts, to provide the basis for alternative control measures, and to achieve user acceptance and system adequacy. (RH)


The trend toward shared management of information resources means information managers must bring internal auditors into the system development process. This is the only way in which DP auditors can properly assess and monitor an organization's computer security needs. Greater involvement of auditors in system development projects will also result in better relations between users and auditors, improved credibility of auditors with information managers and users, and more successful systems.
Ideally, the goals of the MIS director, the end-user and the auditor are not conflicting. All desire solid, cost-effective controls. The auditor concentrates his attention on the adequacy of four areas: specific application controls, general or passive controls, data security features, and disaster recovery procedures. There are several ways MIS professionals can facilitate the auditing effort: by holding preaudit meetings, by reviewing audit reports, by evaluating audit retrieval software, by making auditors a part of the systems development team, by allowing auditors to attend MIS training programs, and by arranging for interdepartmental staff exchanges in order to improve complementary technical skills.

The advantages are given, from a professional standpoint, for the internal auditor based on improved skills acquired due to the Foreign Corrupt Practices Act (FCPA) of 1977. The skills referred to in this article for the internal auditor also have advantages for companies in the business world in terms of training and developing management criteria in personnel with the adequate background. A comparison is drawn between the similarities of the internal auditor and that of a good manager, the focus being on the analytical abilities of both. Detail is given as to the necessary technical skills used in the analytical process with a familiarity of EDP skills. Additional skills mentioned include effective communication, leadership abilities, supervisory accomplishments and interpersonal awareness of others. (RH)

Auditors should be participants in all phases of system design. They can provide advice in the area of internal controls and audit trails, evaluate the progress of the project in meeting users' goals, and have the audit requirements built into the system. Auditors can contribute to the planning, design, and implementation phases.

Some DP auditors believe that there is a growing trend toward DP auditing managers moving into the position of general auditing manager of their company. Most DP auditors have a dual background, with either training or experience in both computers and financial management. This makes them ideal candidates for advancement into upper-level auditing management positions, although those in the profession admit that few companies are aware of the increasing importance of DP auditors. However, they feel that in coming years the integration of data processing and accounting will make DP auditors the most logical choices for promotion.

**EDP APPLICATION SYSTEMS**


The Auditing by Computer specialist group provides a place for computer professionals and accountants to exchange their views. It is a part of The British Computer Society (BCS). The Auditing group exists primarily to promote accounting requirements, control requirements and computer-assisted auditing techniques. Data processing personnel, financial management, auditors and security specialists are brought together to develop a practical approach to security. Software packages for accounting functions are extremely poor and often do not produce the necessary information to manage a business.


Ongoing technology is seeing the increased usage of computers in the world of small business. This article examines control and audit in the small computer environment. The first half deals with the small computer characteristics and gives a very good definition of the terms microcomputer and minicomputer. The small computer environment is discussed by giving the reader characteristics common to what is referred to as a 'small business', and the problems imposed within the environment that leads to weak internal controls. The rest of the article details the general controls and application controls found in SAS No.3, but only as to how it relates to small computer systems used in small businesses. (RH)

Speaking at Edpac '84, John Hughes stated that the use of integrated data dictionaries could give auditors needed control over the information processing area. All levels of users would be able to easily access the same data. In order to be truly effective the data dictionary should be tailored to the company's specific needs.


While writing skills are necessary and authoring systems helpful, Steve Becker feels that courseware designing is the most important prerequisite for developing computer-based training courses. Competent designers should understand teaching concepts and be competent in interviewing and instructional methodology. The designer's attitude should reflect an emphasis on student participation. Good instructional design requires several years of training. An audit conducted by a consultant will determine if the programs have the proper mix of technical expertise and teaching technique. An audit, taking less than a month usually, is a report that includes recommended improvements.


Two systems are discussed in this article: the need to evaluate internal control in EDP systems and the need to involve the auditor in the design and development of EDP systems. Errors in the traditional approach to auditing are reviewed. Through the computer, these errors are counteracted and better internal controls are implemented. (RH)


Coopers & Lybrand uses 3B2 supercomputers and 6300 personal computers, along with 200 accountants to audit the books of American Telephone and Telegraph Co. Top auditing managers, known as partners, are aided by the Computer Audit Assistance Group (CAAG) support group. Some New York programmers are developing off-the-shelf accounting software.
for large accountants, called 'engagements', while other programmers are developing software for the AT&T auditing teams.


Auditing of data processing departments causes anxiety among DP managers. Nearly every data processing department receives an audit by one or more organizations, and public sector workers are subject to government audits. Many problems seem to occur during the data processing portions of the audits. Several common questions are often asked about audits: Considering some of these questions in advance can result in a better relationship with the auditor.


When reviewing application systems, auditors look for an 'internal control', meaning the programs are 100 percent predictable. In fact, few systems are equipped with internal control, but systems lacking internal control are potential time bombs: you don't know if the system has a 'bug', and you don't know how or when the bug, if there is one, will cause a problem. If an organization does not have internal control, such a safeguard should be established. Suggestions for how to do this and a discussion of standards are presented.


The data processing manager has the right to be the first individual to view the audit draft report. The data processing managers should list the findings, associated recommendations, then review the findings. Also, the manager should consider several questions about the findings and recommendations. Although the review process is time-consuming, it is one of the best investments that a data processing manager could make, because a better final product is the result.


After investing in sophisticated disaster recovery equipment such as an uninterruptible power supply (UPS), many DP
managers lapse into a false sense of security. Periodic audits are necessary to confirm that the recovery system will operate in the event of an emergency. Five problems are typically discovered as a result of an audit: improper reliability engineering in the original design of the facility; incompatibilities in conditioning systems; improper equipment installation; lack of maintenance; and a failure to test backup systems.


The proliferation of personal computers (PCs) in the corporate environment has gone on unchecked for some time, and the moment has come when a number of companies are taking a hard look at PC costs and return on investment. Many companies are requiring that PC purchases be cost justified before the purchase can be made, and others are instituting ways of auditing PC usage and measuring returns in productivity. Some organizations, such as accounting firms, are solving PC-cost questions simply by charging clients for PC usage in order to offset the cost of the machine. There are those who feel the use of PCs is so important to the future that they see no need for cost benefit analysis and are willing to undergo the risk of proliferation to gain an unknown future advantage. The processes that a number of firms have instituted to measure and control PC costs and benefits are described including those by: American Motors Corp., with its end-user planning worksheet for cost justification; Peat, Marwick, Mitchell & Co. cost-effectiveness study; Litton Data Systems' auditing system; Security Pacific and Avon, which put justification responsibilities in the hands of the managers; and Gilbert-Commonwealth's effort to measure productivity.


The author explains that due to the Foreign Corrupt Practices Act of 1977 (legalized obligation of an effective internal control system), management must be careful when analyzing the cost involved for the necessary internal control to prevent exposure. The auditor evaluates this problem by determining a cost-effectiveness analysis, through the use of such standards as those found in the Statement on Auditing Standards. Five diagrams are shown with various cost-effectiveness methodologies. (RH)

This section of the AICPA Professional Standards is concerned with the overall international guidelines associated with computer-assisted auditing, commonly referred to as CAAT. The section discusses the techniques when using a computer as an audit tool in such cases as the software, test data, uses of CAAT and the overall effectiveness of CAAT in evaluating audit data. Information is given as to procedures the auditor can and should maintain in controlling CAAT applications. (RH)


An evaluation of internal control systems is an important part of auditing responsibility. An independent auditor may be required to render an opinion on internal controls as well as on the financial statements. Auditors have not yet accepted mathematical models for control. A linguistic model is suggested. It uses the theory of fuzzy sets to aggregate common linguistic values and returns a linguistic aggregate evaluation of the control system. An example is given and a bibliography with references.


A sophisticated MCS, such as Burroughs GEMCOS, can be organized into general areas of functional responsibility. The MCS is viewed here as a single process in the mainframe. The MESSAGE must identify its action, format, and routing. A transaction is a set of data base changes by a transaction processor (TP) that occur in transaction state. A simple message causes a single transaction in the TP, while a complex message causes more than one transaction state. The unit of MCS AUDIT, the outbound message interface to the TP, becomes the level and sequence of the reprocessing phase of recovery. Normally only messages which require changes to the data base are audited. (Article includes diagram showing three examples of the interface from the SCREEN in the MCS to the TRANSACTION in the TP and back.)

An EDP audit risk model used by Marriott Corporation provides a means of assessing EDP risks in a dynamic, rapidly changing environment. The EDP audit attempts to determine a company's hardware, applications, and where the risks are. The present model is based on a survey of hardware and applications. Each device and application is assigned risk points based on specific criteria. From this, risks for the entire system can be calculated and vulnerable areas detected. In addition to risk analysis, the model affords a database of hardware and applications and provides a basis for other audits and user surveys. Tables illustrating risk calculation logic and results of hypothetical analyses are included.


Systems audits are a somewhat new field for auditing. Most technical services departments have never undergone a thorough audit. Nine tips are discussed for preparing and undergoing a systems audit. After the first audit, the rest are easier.


Audit products which automate the bank audit process the work of internal and external auditors and are more comprehensive than manual systems. Electronic data processing (EDP) auditors, who examine data access and security, and system usage, backup, and updating, may use some of the same products. Audit products include complete audit systems, function specific programs, and security devices, all with the purpose of supporting the reliability of a bank's financial data.


Although each office automation audit is tailored to the specific organization, there are general features common to any audit. A variety of factors are reviewed in an audit, including the use of standards, the physical layout, storage facilities, disaster recovery plans, CPU protection, daily procedures, equipment utilization, strategic planning, software adequacy, staff training/skill levels, and staff adequacy. After gathering all the required information, the
The postimplementation audit evaluates the actual performance of a system. It should take place after the system has been in operation for about six to nine months. The evaluation includes a comparison of objectives with actual system outputs. In addition, it includes an assessment of user satisfaction, system efficiency, data accuracy, security, back-up and recovery, and system documentation. The audit report should include a description of changes from original objectives, problems discovered during the audit, plans for solving known problems, and recommendations.

Peat, Marwick, Mitchell & Co. has developed Controls for Application System Evaluation (CASE), a methodology to set management priorities for controls of computerized information systems. Management users, systems developers and auditors, using CASE, can participate in an in-depth evaluation of application controls and establish priorities in four major areas - Input, Processing, Operations, and Output and document more than 350 control concerns in the process. Each of the major areas is further broken down into four to six subdivisions, and examples of completed worksheets are shown, and their development, and usefulness discussed.


EDP audits follow the same basic concepts as regular audits. The audits need to be planned, executed and controlled. The planning aspect covers the scope of the audit, the impact it will have on departments and the environment of the audit. The execution phase requires adequate staffing and the use of various auditing tools. The audit reviews the controls over operations and data being used. The audit itself needs to be limited as to how it affects the company's operations.


An information systems audit can be productive if the auditor is qualified and if the MIS manager cooperates with and follows the auditor's recommendations. A qualified auditor should have extensive DP management experience and good interpersonal skills. A complete audit should cover personnel, hardware/software, applications development, data center operations, user relations, and management policies and practices.


Using a Victor 9000 microcomputer and a SuperCalc spreadsheet, a mathematical model is built to help Omark Industries plan its audit of forty-two locations in a three-year period. A priority list is established using a Weighted Index Value (WIV) for each audit type at each location. The WIV is a composite index based on relative weights assigned
to four factors of which the Relative Materiality Index (RMI) has the highest weight. The RMI is based on relevant financial criteria. It includes data elements applicable to cycle audits of Expenditure, Revenue Production, Capital Expenditures, Payroll and EDP.


Operational audits measure record-keeping management. Detailed planning is necessary before an audit can be conducted. An important question is whether the files should be brought to a central location or whether the audit should be conducted at the file locations. Representational sampling is advisable. All relevant personnel should be notified that an audit is taking place. Standardized forms with accession numbers and space for comments should be used. It is vital that the reliability and validity of the data are maintained. Includes bibliography. This is the second of a three-part series.


The Snohomish County Public Utility District, Number One, found that careful planning for its first operational audit in 1981 minimized the number of contingencies and their impact. Phase I involved discussion of goals and objectives by the audit team. In Phase II, the team selected a population, drew a 'map' of the filing system, and developed active filing system standards. In Phase III, six data collection forms were designed and tested. They were a file station audit data sheet, data summary sheet, worksheet, audit evaluation, master data sheet, and organizational grid. In Phase IV, the data was analyzed for validity and reliability. Examples of the six data collection forms are shown. This is the first of a three-part series.

60. Gunther, M. and Lang, B. "Analysis and Interpretation of Data from an Operational Audit of Active Files." Records Management Quarterly, Vol. 18, January 1984, p. 5-8, 10-12.

An operational audit is a nonfinancial audit meant to determine a company's managerial efficiency. Statistical tools and techniques such as arrays, measures of central tendency, partitions, scaling, and indexes were used to analyze the performance of file stations at the Snohomish County Public Utility District in Everett, WA. Data about
the District's 1481 cubic feet of records was collected on tally sheets and analyzed. Nine tables illustrate various statistical measures, means, partitions, and frequencies; two graphs show frequencies of record volume by type of filing cabinet. This is the last of a three-part series. Include references, tables and graphs.


A Guideline Series report from the American Institute of Certified Public Accountants (AICPA) indicates that an on-line environment does not change the types of errors and irregularities encountered during an audit. The advantages obtained through the use of an on-line system are access to data files and reduction in risks that are encountered in manual and batch procedures. Several factors to consider when auditing on-line are: occurrence of certain types of irregularities and errors, changes in the nature and extent of controls, and changes in the nature of the audit trail and sources of audit evidence.


The advent of the distributed system creates a new environment in which the EDP auditor must work. He must deal with multiple copies of a database and understand the access and reliability controls needed to maintain their integrity. These controls plus audit techniques and requirements are all discussed. Specific subjects discussed are general audit concerns, protection/recovery considerations, software provisions, performance and reliability, concurrent auditing techniques and the audit trail.


In preparing for the auditing of his automated accounting system, the DP manager should be aware that DP auditors are performing their audits through the computer system - verifying I/O controls, and internal processing functions of the computer. The best preparation for the audit is to design in input controls, processing controls, and output controls before the system is actually implemented. A list of such controls is provided.

The internal auditor should understand and participate in the development life cycle of an on-line distributed system to insure adequate controls are built into the system. New audit procedures may be required to verify the controls after the system has been implemented. A diagram of a simple distributed system is included.


Manufacturing control systems differ from financial systems in their focus and components. Most auditors are not familiar with auditing manufacturing control systems. The typical subsystems of manufacturing control systems are described. Auditing procedures can be used to identify and verify the control points of the system. Different auditing procedures are applicable in various subsystems.


Viewed as a service and a competitive edge, Price Waterhouse has embraced computer applications. It uses computers as a part of the auditing service and provides computer application and installation reviews for clients. The firm is tackling communications problems and is reviewing its information technology strategy. Personal computers play an important role. Portable computers must be IBM compatible, have a hard disk, and run LOTUS 1-2-3. The company handles security with IBM DES standard encryption and dongles, small plug-in devices required to operate microcomputers. It also conducts computer training and uses computers to keep up with the Inland Revenue.


Two kinds of errors occur in personnel data bases. One is simply that the data was entered improperly. The second error is that the data is not updated. The symptoms of both problems can be quickly detected. The symptoms, however, must be recognized. Some deal with accuracy and completeness. Others deal with standard reports and ad hoc reports. Audit steps which can be taken to detect problems are listed.
As more applications systems become computerized, audit efforts also increase. One company has addressed the problem by forming an Audit Information Center (AIC). The aim of the AIC is to increase effectiveness and efficiency of the audit staff. It is a menu-driven system which offers flexibility in testing and running audit programs. The implementation effort for AIC was minor.

The object on an audit has not changed, but auditing techniques have. An auditor must check the general and applications controls of a computer system and review manual and automated aspects of a business. Auditors may use packaged software or write their own programs to test client data. Programs are used to test data; test data validates a program. Personal computers perform many routine audit functions.

Two techniques for auditing on-line systems are compared. Parallel simulation is a common auditing technique for batch environments. Its reliability depends on the subset of transactions being audited. Continuous and Intermittent Simulation (CIS) audits transactions as they are processed. It does not audit immaterial transactions. If a problem arises while CIS is in operation, all the necessary information is immediately available. Guidelines are given for when to select which technique.

The Integrated Test Facility (ITF) is a computer auditing technique considered to be the most comprehensive technique available. Among the advantages of ITF is that it fulfills the objectives of a security audit. One of its drawbacks is the effect the auditor's transactions have on the data base. The concept of using differential files to facilitate an ITF
audit is discussed. Use of differential files can reduce the cost of the audit. The integrity of the data base is not affected when an audit is done using differential files.


The operational audit is concerned with the appraisal of company effectiveness, identifying operations which are open to improvement. The history of the operational audit and its relationship to other types of audit are discussed. The scope of the operational audit is discussed and so is the manner in which assignments are typically conducted. Two case studies, one in a sales company and the other in a production company, are presented. Details of the results are provided. The relationship of operational research to operational audit is reviewed. The benefits of including operational researchers in audit teams are pointed out. Organization charts for the case studies are included.


Before computerizing an integrated accounting system, a requirements analysis should be done to determine which aspects of the company's accounting activities justify computerization. Not all integrated accounting packages perform the same functions. For transaction processing, an essential feature is a good audit trail. Another essential ingredient is error checking before processing. The decision between open-item accounts or balance-forward accounts must be made before choosing a sales ledger program. A purchase ledger system that prints checks may not be required by a smaller company. The nominal ledger program should produce a listing of each account with transactions and a trial balance printout which can be used as input for a profit and loss statement. Before computerizing any accounting system, an accountant should be consulted. The wrong integrated accounting system is worse than no computerized system. A diagram of the various account balances in an accounting system is included.


The advent of real-time systems has introduced new problems regarding controls. The responsibility for completeness and accuracy of information should be with the users of the
information, but most often is with those who input it. 
Real-time processing also creates difficulties because the 
physical order of processing is not controlled and complex 
recovery procedures are involved. Control of the tables used 
for access controls is often inadequate. In addition, it is 
difficult to demonstrate the ongoing correctness of data 
because batch totals or master file date checks are no 
longer appropriate. Methods must be developed to verify and 
authorize critical data after they are input but before they 
are used.

75. Mar, S. "Future EDP Audit Function And Scope." EDPACS, Vol. 10, 

Many companies have established EDP audit departments. The 
time has come to address future developments in EDP 
auditing. A large bank in Seattle is reviewing its auditing 
division as to future requirements. It is anticipated that 
the planning aspects of auditing will double by 1990. 
Several research projects are underway to study future 
developments such as changes in laws and regulations. Audit 
functions are reviewed and new priorities established when 
needed.

76. Mautz, R.K., Morton, A.G. and Severance, D.G. "Corporate 
Computer Control Guide." Financial Executive, Vol. 52, 
June 1984, p. 25-36.

The Corporate Computer Control Guide is divided into three 
parts. Part One discusses the results of a survey with 350 
corporate executives in relation to electronic data 
processing. Computer failure and abuse are discussed, along 
with a table of potential disasters and competitive 
disadvantage concerns as presented by senior management. 
Part Two provides sets of questions designed to initiate 
discussions within an organization. The questions were 
divided into four categories: questions for Senior 
Management, questions for User Management, questions for the 
Chief Information Officer, and questions for the Director of 
Internal Auditing. Most management problems are, in reality, 
people problems. Often these are caused by a failure to 
define responsibilities. Part Three lists the 
responsibilities of the Line Management, Chief Information 
Officer, and the Internal Auditor.

77. McKeown, B. "Audit and Control in the HP3000/IMAGE 

The author has written a detailed evaluation of an audit of 
the HP/3000/IMAGE minicomputer system used by Weyerhaeuser.
Discussion includes distributed processing and database controls. The audit involves key risks and control techniques unique to the HP3000's MPE IV operating system, its subsystems, the IMAGE database management system, the DS 3000 telecommunication system, transaction logging systems and the data dictionary. A conclusion is given as to the adequacy of controls in data security, disaster recovery, database locking, database internal integrity checks, access to programs and utilities and operating systems control. (RH)


A data center audit can prove to be a productive experience. It can be used to improve operational controls in application systems. Auditors can assist with automating the tape library. They can assist with training and upgrading data center staff. A well performed audit will also highlight security issues and bring those issues to the attention of upper-level management.


This is the ninth chapter in the course. The auditing of computers is covered. Auditing is becoming more difficult as the complexity of computer systems increases. A recent approach to auditing computers is dynamic auditing. This is auditing that happens every time processing occurs. Auditing must be systemwide. Auditors must make sure that the audit trail is maintained. Auditing must be conducted through the computer. Auditors should participate in system design, implementation and postimplementation as well as dynamic auditing. A productive relationship must exist between the auditors and the EDP personnel. The role of the auditor includes observation, confirmation, inquiry, system inspection and operations analysis.


Preparation is seen as the key to surviving an audit, a regular occurrence in data processing organizations. The three general phases of an audit explained in the article are the planning, performance and review phases. Procedures that data processors can take to facilitate an audit are also detailed. Use of audits is recommended for remedying situations which are unfavorable to the company and as a conduit for promoting worthwhile proposals.

The B 1000 DMSII data base is composed of options, parameters, audit trail, data sets and sets. By employing specific techniques for describing and using these components a more efficient data base may be developed. The KEYCOMPARE option should always be on because it requires minimal overhead and insures set integrity. SYNCPOINT minimum values should equal the number of update programs running. Audit trail buffer size should be between 1800 and 3500 bytes. Further suggestions concerning DMSII will be published in articles in June and July 1984.


Rahn, a data professional, gives steps that are necessary for auditing a computer system. First, be more effective by defining the auditors' role in an operational review. Second, seek objectives by contacting those affected, a sometimes difficult and thankless task. The author also gives points on how these two objectives can be attained as well as what the EDP operational audit should veer away from. Guidelines are given for auditors to follow and to whom and when they are to be reiterated. (RH)


Concurrent Auditing Techniques (CAT) is an auditing process. CAT is defined as a process which employs specific techniques to collect evidence concurrently with the occurrence of application system processing. These techniques provide for timely evidence collection and evidence evaluation during the audit. Each technique is described and includes Integrated Test Facility (ITAF), Test Decks, Tagging and Tracing (TT), Snapshot/Extended Record and System Control Audit Review File (SCARF). After listing the advantages and disadvantages of CAT, it is concluded that CAT is a viable, useful tool for auditing.


Peat Marwick uses the Apple Macintosh for annual audits under a program called Systems Evaluation Approach—Computerized Audit Support (SeaCas). SeaCas was introduced
in late 1982 with the Apple III. Currently the company has 4,000 personal computers for more than 7,000 employees. The applications include System 2190 proprietary software and its Financial Statement Subsystem for data retrieval on IBM and Burroughs mainframes and Microsoft's Multiplan, Chart, and File, Macwrite, Macpaint, and Macterminal personal computer software. The audit staff receives in-house training; a personal computer and printer go on every audit.


Senator William Roth, chairman of the Senate Governmental Affairs Committee, has criticized the Pentagon's contract audit policies. Roth says the Defense Contract Audit Agency (DCAA) does not properly audit contract price proposals. He cited the following DCAA deficiencies: an undue regard for the concerns of contractors; a lack of support for field auditors' positions; and delayed processing of incidents of fraud.


The first step in optimizing resources used by a DMSII database system during on-line processing is a system performance audit. The audit begins at the hardware and system software level and proceeds to the environmental software implementation. The final step is the evaluation of the application software implementation. The audit deals with optimization in the areas of memory utilization, processor utilization, and input/output utilization. DMSII access routines are an interface between user programs and the data base. The main function of SYSTEM/COPY AUDIT is to copy a DMSII audit file from one media to another. The DMSII UTILITY program has two principal functions: dumping data bases to tape for back-up purposes and initiating data base recovery programs. Diagrams illustrating the function of each of these DMSII components are included.


As computing systems become larger and more complex, conventional after-the-fact auditing techniques become impractical. However, these techniques continue to be used by many organizations until they install a new system. A survey was conducted of three hundred organizations about the auditing techniques that they use and that they prefer.
The results of the survey are presented and discussed. Recommendations are made concerning establishing audit procedures for advanced systems. The survey questionnaire is included.


The IRS has begun using its computers and new sources of data to snare tax evaders who would previously only have been identified through an individual audit. In 1984 IRS computers generated 3.9 million notices questioning discrepancies between 1982 returns and income records; $1.5 billion in added taxes was assessed. A number of the notices, however, contain errors according to accountants, and these may take several rounds of correspondence to resolve.


Due to the sophistication of microcomputer-based systems auditors must enhance their approach to the traditional audit, the use of the PC does not end the need for extended audit testing. Thirteen objectives are discussed in outlining the evaluation of a PC-based system, a micro environment checklist is given, as well as the five stages of personal computer systems integration. (RH)


Peat Marwick Mitchell will be using the Apple Macintosh for its Systems Evaluation Approach Computerized Audit Support, the latest technology based system. The company has been using microcomputers since 1979. It uses computers for its own internal operations and its work with clients. Over half of its consultants work in the computer area and the company created Systems Development Group, a systems house. Peat Marwick has Prime minicomputers and a new network. It is involved in a Wang system report processing pilot project. Microcomputers have been used extensively for auditing, modeling and forecasting.
MESPIS, the imaginary maintenance equipment spare parts inventory system, will need past event records. Data fields will include the date, name and quantity so an audit trail is possible. A serial number sort is a necessity. A flow diagram shows the simplest way to handle the past record data.

The implementation of the database in the project is now at the point of auditing. Consultants are chosen on the basis of cost and benefits. The reporting by the consultants took the form of staff interviews, and checking the data models, entity and function diagrams, and all the information in the data dictionary. The specifications were then related to the database as it exists. The report pointed out the necessity for clarification in several areas, and the lack of a function dependency analysis. Physical evaluation of the database covered general system efficiency and long term flexibility. Problems at this time on the project concern additional programming and data conversion but the link and system testing plans have been firmed.

The Federal Aviation Administration's planned $3.2 billion advanced automation system (AAS) poses huge risks, mostly as a result of projected cost overruns and insufficient system testing, according to an auditing report by the General Accounting Office (GAO). The government agency's procurement program is based on two stages, the design competition and the award, and this method of awarding government contracts is insufficient because it omits the lengthy testing requirements which will uncover a defect, according to the GAO report. Full production of the most expensive elements of the AAS, including the controller workstation, occurs simultaneously with the development of the advanced hardware and software elements. Usually, large purchases have a separate testing and development stage which occurs before the commitment to complete production, however the FAA wants to make its decision for production based on computer model simulations of system design and performance trade-off analysis.
Product Evaluation Archives and records can be kept off paper for the use of the librarian and the auditor in performing their daily functions. Although microfilm and video disks have been used, Philips Megadoc has aimed to explore the systems problem of record handling. Viewing is an improvement over microfilm, and the product interconnects with telephone and data networks, thereby eliminating paper.

Coopers & Lybrand is now offering its Handbook of EDP Auditing for sale. The book is the result of eleven years of planning by the company's computer audit assistance group and is over 1,100 pages in length. It is designed to help businesses that are becoming increasingly automated develop appropriate auditing procedures.

This publication deals principally with the audit of EDP systems and not the results produced from the systems: focus is more on the internal control structure. Auditing concepts, typical terminology and flowcharts are presented.

The Association of Data Processing Organizations (ADAPSO) will admit Price Waterhouse & Co. and Arthur Anderson & Co. to the organization. Though there are some critical ADAPSO members who claim there is a conflict of interest in auditing firms which provide MIS services, ADAPSO has sanctioned the companies' legitimacy in the computer services market. The organization has historically maintained that the auditing companies contracted by customers to recommend services or software decisions would recommend services provided by themselves.

The Independent Computer Consultant Association (ICCA) is critical of the Big Eight accounting firms that recommend
computer systems to clients while also performing audits of the same companies. There are two major issues involved. First, an accounting firm should maintain independence in order to conduct an accurate audit. The second issue concerns fairness and competition. One solution would be to bar accounting firms from performing audits on companies for which they have provided consulting services.


The merging of the fields of auditing and management information systems (MIS) is explored with respect to the Audit Command Language (ACL). ACL is a prototype language to aid in developing a single standard language for auditing. Several issues are dealt with. The idea behind ACL as well as its design characteristics are discussed. Various functions and commands of ACL are discussed as well the ACL supervisor and monitor. The impact of ACL on the MIS environment is covered as well as some recommendations for research into the development of a standard auditing language.


Information Resource Management (IRM) concentrates on managing information as an organizational resource and is a synthesis of several approaches to handling information: general management (resource handling), computer systems management, library science, policy making, and planning approaches. Among the many benefits of IRM are improved support of information security, privacy, and auditing efforts. This article discusses these benefits while emphasizing the key role a corporation-wide data dictionary plays in IRM.


Changes in software in a computer environment can affect more than the immediate program being changed. When they are made without proper controls, the entire system may be exposed to new risks. A change control review system can oversee and minimize potential risks. The review should include authorization and documentation of changes as well as a comparison of audits before and after the changes. Changes should be implemented by someone other than the one programming the change.
Most of the information published about EDP auditing deals with auditing methodologies. An EDP audit depends on more than methodology to be successful. It also needs effective management functioning. A successful manager is one who sets objectives, organizes, motivates, measures results and develops staff. An effective EDP audit is a result of the manager.

MICROCOMPUTERS


Discussed in this article are the many uses of the computer in the auditing process. Comments are given as to the usefulness of the personal computer as a management tool in developing the annual audit plan in terms of scope, location, time budgets and reports. Further discussion includes the use of microcomputers in training for computer-assisted instruction, as a word processor in generating correspondence, reports and as an audit aid in the use of financial and operational audits. (RH)


Two myths associated with the use of microcomputers are identified, (1) that the computer is always right and (2) you don't audit calculators. More detail is given to spreadsheet verification as an audit test in the use of microcomputers. Six very helpful points are stated as additional check points in tracking microcomputer errors. (RH)


Microcomputer technology development, though solving many business problems, seems to have little internal control concerns. To circumvent this problem the establishment of a position entitled microcomputer coordinator/facilitator (MCF) would have the task of analyzing the micro system.
This analysis of said system would entail checking internal controls in the areas of software, hardware, training, and staff use of accessible data. (RH)


Many first-time users of computers should base their decision to purchase on crucial software and vendor support. The company auditor should be a key figure. The extent to which operator errors are detected and prevented is the test of a superior system.


Microcomputers present a challenge to internal auditors. The challenge is to understand control procedures applicable to the new software so auditors can effectively advise management. The value obtained from a well-equipped microcomputer is described. The experience an internal auditing department had in the initial year of using a microcomputer is discussed. The following categories of software are considered useful: electronic worksheet programs; calendar or reminder programs; and special purpose applications. Relevant topics are discussed including control approaches and guidelines for the use of distributed computer. Hands-on experience should be obtained.


Made up of diagrams with a one page introduction. A presentation is given showing the examples of microtechnology use in the audit environment. (RH)


Due to the flexibility and accessibility of microcomputers, auditing techniques and audit independence have greatly improved. This article presents the microcomputer as an essential audit tool in improving audit productivity and quality due to its various uses in the audit environment. Attention is given to the benefits received by the audit team as well as the training and requirements involved in implementing its use as an audit tool. (RH)

A survey among the members and recipients of EDP Auditor Update, on the use of microcomputers in EDP auditing. Background is given on the respondents and a discussion on the survey results. (RH)


A portable audit micro is the most advanced tool that an auditor can rely on for his work. The system accumulates all hours and makes a summary of work-completed-to-date and estimated-time-to-completion. All sample data and the work performed on them and the test evaluation results are recorded on electronic work papers for the review. At the year's end, all the analyses of transactions and balances are carried out by extracting the data from the client's computer system.


Arthur Young & Company, one of the eight largest accounting firms in the country, uses a Macintosh computer network to do auditing work. The system consists of 62 Macintoshes, seven Sunol hard disks, seven Macintosh XLs, five LaserWriters, and the AppleTalk network. The AppleTalk networks at Arthur Young will be limited to twelve Macintoshes each, however, due to the network's relatively slow transmission speed.


When the Big Eight accounting firm of Peat, Marwick Mitchell & Co. decided to automate its auditing practice, it chose the Apple Macintosh, primarily because of its friendly user interface. In January 1984, the company announced plans to purchase over 4,000 Macs. Peat Marwick has specified three company goals for its Mac automation effort: to increase staff productivity and audit quality, to shift the burden of mundane clerical tasks from the auditor to the micro, and to enhance the company's image by employing state-of-the-art technology.
An evaluation and comparison is presented between mainframes and the microcomputer. The concerns listed illustrate the use of the micros in an administrative capacity. A checklist for planning and policy guidelines is presented for the use of the non-EDP-oriented auditor. A second checklist is presented pertaining to EDP auditing control and security. (RH)

The pro-active approach is one of the DP managers exercising a degree of control over the integration of corporate micros. Requirements needed by the DP manager in order to achieve better DP control are: a focus on the user, knowledge of the capabilities of microcomputer hardware and software, and training and support in microcomputer integration. All of the previous stated skills will tend to smoother DP control for the organization along with excellent professional and career opportunities for the DP manager. (RH)

The Arthur Young Audit Computer consists of an Apple III CPU with 256K RAM, a hard disk with 20M bytes of storage, and eight-inch floppy disk drives. It also has communications capabilities. The three main applications for the Audit Computer are discussed: analytical review procedures, audit administration, and data testing.

The microcomputer, seen as a new phenomenon, introduces numerous uses for the auditor. Among these uses incorporated into the auditing process are microcomputerizing where working paper formats are input for ready access by other team members of the auditing team, thereby being able to constantly revise the previous input. New "integrated programs" are mentioned as a way of making the system more flexible and versatile. The microcomputer and its use in "audit decision support systems" cover such
areas as internal controls and audit testing on the micro. Long term auditing techniques are discussed as future trends in the auditing process. (RH)


Sobol discusses the use of establishing certain policies and procedures needed to provide control within the microcomputer environment. Issues touched upon include acquisition of microcomputers within the audit department, central clearing houses, volume purchasing, data entry, usage limitations and security. Approached from a management point of view emphasis is given to the auditor as a needed force in the control of the microcomputers' use in today's ongoing technology.


The EDP auditor can increase audit productivity and reduce costs with a microcomputer. Many businesses are installing microcomputer systems which can be audited with a microcomputer. Some audits of mainframe systems can be done with a microcomputer terminal. In selecting a microcomputer for audit purposes, the hardware and software features are a consideration. Guidelines are given for establishing needs. As microcomputers become more portable, the auditor can become more productive.


Peat Marwick Mitchell & Co., one of the nation's Big Eight accounting firms, has purchased almost 5,000 Apple Macintoshes for use in its audit departments. User response is generally enthusiastic. Some offices, in fact, report that demand has outstripped supply. A typical configuration includes 128K RAM, an external disk drive, a 1200 bit/sec modem, a numeric keypad, and bundled software.


Microcomputer acquisition by the federal government's Office of Technology Plus stores has been inefficient and costly, according to auditors for the General Accounting Office (GAO). The government agency is in favor of a more competitive procurement process for the roughly $50 million
per year market. The GAO said the government could save money by forming an award schedule made up of computer store retailers, to support the more limited use of the OTP outlets, which are operated by the General Services Administration. The report also suggests cutting the maximum order limit of the existing OTP outlets to $50,000 from $100,000. A GAO report released in 1985 said the government-operated stores were selling software which was priced 22 percent higher than the software sold on the open market, and that the microcomputers sold under multiple-award schedules were priced 15 percent higher than commercial market prices of the same equipment.


This study was done to show the growing use and evolution of micro computer technology in association with the auditing processes of GAO evaluators. The guidelines cover a range of subjects, from data management, review, verification and indexing, to referencing and information storage, with an entire chapter on documenting workpapers in the audit process. Designed principally for evaluators these guidelines were accomplished through the assimilation of other papers and a previous paper entitled Microcomputer Do's and Don'ts.


The microcomputer as an audit tool is discussed in four phases of operation. The four phases, automating the audit process, basic auditing functions, advanced auditing functions, and audit module functions are all discussed as a ways of realizing significant improvements in efficiency and effectiveness in working with financial data and audit records. included is a discussion of the significance of the microcomputer in the future and the entire auditing profession. (RH)
PORTABLE COMPUTERS


Citicorp Bank utilizes a network of fifty IBM PCs and thirty-five IBM-compatible Compaq portables for its worldwide auditing activities. The network's principle purpose is to provide intelligent terminal-to-mainframe capabilities, although it is used for stand-alone processing and for uploading and downloading files. The micro network, called Audinet, is linked to Citicorp's Global Telecommunications Network (GTN), a private leased line network.


Portable computers are now being used to help perform auditing functions. The President's Council on Integrity and Efficiency (PCIE) is using Compass computers to help prevent abuse in agency programs. The PCIE chose the Compass because of its terminal emulation capacity and its ability to access a large number of centralized applications programs. The PCIE has already more than paid for the computers in a sense when it discovered $1.5 million in underpayments by oil and gas companies to the Department of Interior. The General Services Administration has established a training center in order to teach the auditors/investigators how to use the computers as auditing tools.


IRS auditors in the Boston area are using Grid Systems' Compass portable computers for on-site tax analysis. The Compass systems are equipped with 512K RAM, 348K of bubble memory, and 128K ROM, expandable to 512K. The goal of the project, which will involve all auditors by September 1985, is to eliminate the use of hand-held calculators and speed up the audit process. Using the computers, audit times have reportedly been reduced from three to four hours to fifteen to twenty minutes.


The Internal Revenue Service will incorporate the Grid Compass portable computer into its auditing procedures. Available to all agents, the portable computer will speed up
procedures, reduce the margin of error and exchange data with a host minicomputer. Presently, the agency is seeking competitive bidding for an examination system, leading to a fully integrated program by 1987.


The Internal Revenue Service (IRS) is going to equip sixteen field agents in Massachusetts with Grid Compass portable computers. This is being done to test how portable computers can speed up the process of conducting faster, more thorough audits. The goal of the program is to begin computerizing revenue agent reports. The IRS is planning to purchase 12,000 to 17,000 portable computers for its agents by September 1985.


Evaluators at GAO's Seattle Regional Office selected 100 lapsize computers from 16 manufacturers to determine advantages and disadvantages of their computers in an audit environment. Lapsize computers were defined as portable computers weighing 20 pounds or less. Revealed was the knowledge that lapsize computers would fill many of the GAO traveling audit needs. Some of these needs included text processing, data entry and analysis, and communications. Essentially all of the lapsize computers tested are compatible with LOTUS 1-2-3, PeachText, WordPerfect, and Crosstalk. To ascertain the advantages and disadvantages of those tested they were divided into three major groups for discussion with a summation table of the results. Appendices are included giving a profile of the 16 manufacturers and their products. (RH)


Peat, Marwick, Mitchell & Co. bought 120 Apple Macintosh portable computers from Apple Computer Australia. The hardware will be used to computerize audits at the office of the client. Microsoft Multiplan will be used along with other internally developed programs.

The IRS is starting a mass project to provide 15,000 tax auditors with portable computers to automate functions that will reduce routine tasks, reduce overhead costs, and increase accuracy. The computers will be used primarily for spreadsheet analysis and word processing. Arthur Andersen & Company, Washington, D.C., received the contract to design an Automated Examination System. Portable computers from Grid System Corp. are the hardware of choice in a pilot project of the IRS.


Sixteen federal revenue agents in the Worcester and Springfield, Massachusetts offices of the Internal Revenue Service's (IRS) Boston district are using Grid Compass portable computers. The on-site tax auditors use the portables for spreadsheet analysis, word processing and other applications. The IRS is also developing the Automated Examination System which is a network of fixed and portable computers.


Texas Instruments has announced a portable computer which is compatible with its desktop Professional. An extensive amount of software and hardware options are available. The new portable can be used to conduct on-site analyses, word processing, and auditing. Lotus 1-2-3 and TC's Naturalink are compatible with this hardware.

SECURITY


A roster of computer crime types and techniques is listed and described, based on a report done for the Department of Justice by SRI, a security consulting firm. The criminal techniques and types identified are the "Data Diddler," the "Trojan Horse," the "Salami Slicer," "Logic Bombers," the "Scavenger," the "Leak Catcher," "Piggybackers," "Impersonators," "Simulators," and "Modelers." Some techniques effective against computer criminals are offered.
Risk analysis should be conducted to determine what risks a specific company may face and how to reduce them. One specific individual can be chosen to manage data security. Security policies should be written and issued to employees. Frequent unannounced audits should be conducted. All tapes and disks should be kept in secure storage, and files should be classified according to sensitivity. A user log of all personnel using a system should be maintained, and a carefully designed password system should be established.


Computer surveillance systems at the National Association of Securities Dealers (NASD) and the New York Stock Exchange (NYSE) produced an audit trail that led to the arrest of Dennis B. Levine. Levine is accused of trading stock on at least 54 companies about which he had inside information concerning mergers and acquisitions, leading to a personal profit of some $12.6 million. NYSE has a system called Intermarket Surveillance Information System which analyzes records of all exchanges and connects with another Sperry mainframe in Trumbull, Connecticut. Whenever unusual interest in a company is seen on the market, a signal is given, and last year the signal was sounded 11,800 times. After a media survey to see if there was public knowledge to prompt the interest, about 388 of the instances were actually investigated and about 100 were referred to a NASD office to press charges.


The U.S. Office of the Comptroller of the Currency (OCC) has ordered an unidentified firm that provides EDP services to financial institutions to cease its unsafe and unsound practices. More specifically, the unnamed firm has been ordered to provide timely and audited information to the OCC, implement a contingency plan for service disruptions, and provide adequate liquidity in advance when operating losses are identified.


In March 1985, the Inspector General of the Department of the Interior cited the Bureau of Land Management's (BLM) Denver computer center for inadequate controls over passwords, a lack of
audit trails, and faulty operating procedures. As a result of the inadequate security, the inspector could not vouch for the integrity of the BLM's computerized lottery, which is used to award drilling rights for federal land tracks. It could not be determined whether the lottery had been manipulated in favor of any particular energy companies.


The government is set to begin auditing the telephone calls of federal employees, reportedly to prevent employees from making unauthorized long distance calls. Critics in Congress argue, however, that the auditing could be used to catch government whistle-blowers and to generally squelch legitimate dissent. Government officials claim the audit will save $50 million in long distance bills.


Elaborate computer security is worthless if users are not adequately trained. An adequate computer security training program should cover physical security; logical security, such as access controls, encryption, and audit trails; administrative security; and the legal and social aspects of security, such as copyright laws, privacy legislation, and DP liability insurance. There are three sources of security training programs: seminars and workshops, media-based courses such as videotape, and printed materials.


A former Pentagon auditor told the House Energy and Commerce Subcommittee that Pratt & Whitney Aircraft Group's West Palm Beach plant billed the government for tuxedo rentals, shipping crates for ski clothes, firewood, and sports tickets. The House subcommittee, which is investigating allegations of fraudulent conduct in the weapons industry, is responsible for the freeze on government payments to General Dynamics Corporation. The Defense Criminal Investigative Service has begun an investigation into gifts given to Defense Department officials by General Dynamics.
Congressional committee hearings will begin in February 1985 to investigate possible conflict of interest when accounting firms audit corporations for whom they also supply software and management consulting services. The Association for Data Processing Service Organizations (ADAPSO) has also been investigating this issue, but has found no evidence of impropriety. The Big Eight accounting firms maintain that no conflict of interest exists.

A computer crime involves the use of a computer to perform an illegal activity or the theft of computer resources. Many large companies are concerned with the use of computer-based systems for electronic embezzlement. High quality audits and controls are required to prevent computer-assisted embezzlements. The first chapter of the Computer Auditor's Society has been established in New Zealand. This society, which is comprised of larger financial institutions, has developed a code of ethics regarding the use of computers for its members.

Through the use of EDP auditing Richard A. Stimson, the Defense Department's director of industrial productivity, has disclosed plans to conduct two audits of prime defense contractors. Contractors will be investigated to ensure that incoming materials are tested properly. The second audit will determine if contractors are ensuring that the semiconductors they buy conform to specifications. Other steps aimed at improving weapons quality are briefly described.

Brown discusses the use of the minicomputer in a small EDP organization. Control procedures involved with installation of the minicomputer include numerous internal controls consisting of: assignment responsibility, documented procedures, clear separation of programming and operating responsibilities, management and users' involvement in the design, testing and installation of the computer, computer
operation logs, authorized program changes, and a review of the control procedures. Additional discussion includes control of data when stored in a centralized data base, cost of implementing controls, whether or not the EDP system is auditable, steps involved in auditing the minicomputer and the detection of computer crime or fraud. A diagram appears at the end of the article showing audit objectives. (RH)


Computer security encompasses both the physical security of the installation and the integrity of the data. As microcomputers, word processors, data networks, and people able to use computers proliferate in companies, the threat of increased tampering with computer data banks and programs rises dramatically. Auditing can play an important role in checking the internal control of computer security. For some companies, it may be useful to expand the role of the audit committee of the board, reevaluate measures of audit performance, and involve auditors more in important decisions. Risk analysis can be a useful tool in helping to make choices about computer security.


In 1982, Computer Sciences Corp. was awarded a $58.2 million contract for an automated financial system for the Navy's industrial fund installations. Government auditors have now ruled that the firm did not intentionally underbid this contract. The auditors cited similar bids by two other bidders. The total cost of this system is now expected to reach $129 million.


A survey of fifty randomly selected DPMA chapters covered six data security areas. The DPMA members ranked security concerns, in order of concern from highest to lowest, as access to facilities and equipment, backup and recovery, programming errors and omissions, disaster protection, embezzlement and fraud, and auditing. The overall effectiveness ratings in the installations were 'good to excellent' except for auditing, which was rated 'poor'. Most methods of security were used in the majority of installations except for separate control groups for
software testing, procedures for locating the data processing site, formal contingency master plans, and auditing. Tables show the results of the survey.


One tool of security auditors is software which compares object codes of programs. Source code can be understood and reviewed by an auditor without a great deal of difficulty. Object code is more difficult to understand. Several ways are discussed of ensuring that the object code in use accurately reflects the source code presented. The verification process for auditing is reviewed.


The widespread use of personal computers in business creates a problem of maintaining data integrity during uploading and downloading operations. As information is sent through layers or locations within an organization, changes could be made without the original sender being aware of them. Two parallel and independent audit trails, one of the traditional type and the other through data processing, should help preserve data integrity. Small businesses should safeguard against the loss of data; adequate back-up is a must. Also, a back-up operator may be necessary. This ensures that more than one person knows how to operate the small business' computer system. A list of some computer security system sources is included.


While no computer system is absolutely secure, there are specific steps that can be taken to reduce the risk. Among these are: assigning a manager to deal specifically with security, issuing a written policy on security, instituting regular and unannounced DP audits, and developing security teams that involve the entire organization, not only the DP department. The Research Institute of America recommends the following procedures: files should be classified according to their degree of sensitivity, DP managers should control the number of personal computer users, and passwords should be carefully designed and controlled. A partial listing of available hardware and software security products is given.

Proposed legislation in England requires that users of systems dealing with personal data register with the government and have a privacy audit on their systems. A study has been conducted to determine the impact of privacy audits on six businesses. The results indicate the inspections would be less costly if done as part of a financial audit. Thirteen privacy principles based on the Younger Report were used in assessing the organizations. The procedures and findings of the inspections are given.


The operating systems of computers need to undergo auditing along with other aspects of computer facilities. The operating system itself oversees the execution of other software. It needs to have controls to limit its exposure to system abuses. The audit of an operating system should review the procedures for making modifications and the security the system provides for programs and data. The audit program should test the system's integrity and access controls. Certain tests can indicate security hazards.


The authors approach micro security from three points, (1) physical security of hardware, (2) physical security of data and software and (3) data integrity. A discussion follows as to necessary procedures needed to alleviate unnecessary risks in exposing secured data or theft of data, hardware and software involved. A partial listing is attached naming software and hardware available for micros. (RH)


A new security-oriented software package has been withdrawn from the market at the request of law enforcement agencies such as the FBI and Interpol. The Audit program, which monitors all input and output of a system, has been deemed 'too powerful' for ordinary users. A stripped-down version will be marketed commercially and the regular version will go to the legal agencies. The Audit program, from Clyde Digital Systems, runs on DEC VAX minicomputers.

Alert/CICS is a security system for IBM mainframes running CICS. It is from Goal Systems International Inc. Audit trails, the facility for not displaying fields, no need to change user programs, and facilitation of the implementation of a complete security hierarchy in an on-line environment are its features.


General Electric Information Services Co. (Geisco), a computer time-sharing company, has employed a consultant to test the security of their Mark III and IBM-based Mark 3000 systems. The consultant is provided with firm manuals and descriptions to provide him with enough information about these systems to break security. An outside audit firm is also employed to insure that the passwords of ex-employees and invalid users are locked out of the systems.


'General' controls, as opposed to application controls, are reviewed. The types of on-line systems described are 1. data entry, 2. data collection, 3. message switching, and 4. file updating. Physical safeguards (guards, locks, passwords and identification control) and logical controls (management control logs, level and type of user controls, selective file access and update) initiate timely reports to the auditor. Other controls described in detail are audit trails, transmission error control, data file controls, output controls, system failure and recovery methods. These changes in the approach to testing (an auditing technique) are suggested- 1. Tagging, 2. Real-Time Notification, 3. Audit Log, 4. Extended Records and Monitoring, and 5. Integrated Test Facility.


Law and Business Inc. offers pointers to determine whether there might be abuse or collusion by data processing personnel. Dramatic changes in life style may indicate that there is a problem. An official audit is always urged if there is reason for concern. Caution must be exercised before any personnel are confronted or accused.
The second article in a three-part series on data security deals with passwords and audits. Three basic methods for password management are central issue, local issue and individually chosen passwords. In each case, some procedure is needed to ensure the user and the system know the new password and that others do not. An examination of the elements of the system is needed to determine effective password procedures. Some method is needed to allow auditing of the system without compromising password integrity.

Some data processing shops are not as secure as they should be. While a computer system may be impenetrable from without, often programmers within a shop may have unnecessary access to the computer and its software. Furthermore, auditing is sometimes ineffective.

The use of computers in small businesses can reduce costs and capital investments, lower staff numbers and cut down on fraud. At the same time, businesses give up direct accounting control. A business must work with dealers and select a software system, which may not exactly fit the company's needs and may not have enough security. Physical, administrative and technical controls must be implemented to reduce the danger of fraud. Of all the types of fraud, the most spectacular is data and program alteration by systems programmers. Small businesses should be wary of system programmer applicants. Applications programmers cannot change operations systems, but can change data processing programs. Companies need audit controls to stop this.

The activities of computer hackers threaten to undermine the confidence of citizens and corporations in the ability of the government to maintain computer security. The General Accounting Office informed a Senate subcommittee that serious problems exist in all aspects of government
information security including policy gaps, management deficiencies, and inadequate internal audit capabilities causing accidental and intentional information losses.


A distributed data processing (DDP) environment can be thought of as a tree structure, where low-level nodes communicate with higher nodes. A typical DDP environment can have exposures leading to potential losses of information if adequate controls are not implemented. A survey of DDP auditors has been conducted on the security aspects of DDP environments. Specific areas of exposure potentials and the impacts they might have on auditing were ranked. Control measures to limit exposure were ranked in relation to their effect on auditing and cost of implementation.


Both the Department of the Treasury and the Department of Defense recently issued directives requiring all institutions handling government funds or sensitive data to implement approved security systems. Any adequate security system, in its hardware or its software must incorporate five basic functions: communications encryption, file encryption, access guarding, user and terminal authentication, and transaction authentication with audit trails. Organizations should realize that failure to implement available security techniques could result in the filing of negligence law suits.


The key to network security is access control. There are several security methods that should be utilized, including passwords, audit trails, and encryption. To make certain the security controls are functioning properly, it is advisable to conduct frequent mock penetration attacks on the system.


Public attention to computer crime is leading hardware and software vendors to include security features such as audit
trailing, secure operating system kernels and encryption of data in their products. This security must foil the efforts of hackers and criminals alike. The best security systems have access control in many different areas.


Working together, EDP security and EDP audit achieve shared benefits including: improved security controls, increased information resources, system security, sharing of knowledge and a mutual support system. Difficulties arising out of this control system can include users confusion of EDP security and EDP audit, emotional resentment by EDP security when reviewed by the EDP audit staff, and possibly even disagreements on job projects. Case studies are presented to illustrate difficulties when EDP security and EDP audit lack understanding of the other function. A hierarchical scheme shows how an effective operation can be attained. (RH)


Communications networks provide a security advantage for multi-site organizations with distributed data processing because widely scattered facilities are less vulnerable to power outage, natural disaster, and attack than one central facility. Security officers should consider data security policy, risk vulnerability assessment, access control and authorization, data encryption, and audit and reporting. Lack of security policy may prevent prosecution of accused computer abusers. The computer equipment surrounding the network must be in a protected environment. The security of the entire information system, including the network, must be thoroughly audited by qualified personnel.


The state of technology concerning audit, control and security is more advanced than the application of that technology. In part, the lag results from lack of knowledge about the new technologies. Advances in shared storage, addressability, states of privilege, shared registers, authorization mechanisms, journals and logs, end-user
authentication, external controls, cryptography, transaction-driven systems and application development are summarized. Each can be used in audit, control and security applications.


Omni Marketing Concepts announced the Micro-Guard, a new expansion board for complete security in IBM personal Computers. Audit tracking of users will be available with the product.


Information stored in computers is a valuable resource and the proliferation of microcomputers has brought new problems in protecting this information and computer systems. Automated aids to systems penetration, scanning, using microcomputers and modems can easily foil some of the largest systems. Password security is commonly used, but often can be easily broken. Trojan horses simulating the log-in program can provide trespassers with access to privileged areas of the system. Computer systems also can be penetrated using trap doors. Controls and cross-checking are used to detect crimes where data is modified even before entering the computer. Audit trails aid in tracking computer criminals. Such sophisticated investigation techniques are difficult for the average police officer and often cause complicated legal problems. Complicated security systems are available, but often are not used because they diminish the user-friendliness of the system. Sixteen specific computer crime incidents are reported. A diagram illustrates the vulnerability of modern computer systems. A table shows types and perpetrators of crimes, and a graph illustrates the growing incidence of such crimes. Includes graphs, diagrams, and tables.


Illegal copying and selling of mainframe computer software is increasing. The only people who can usually copy mainframe software are high-ranking MIS personnel. It can be very difficult for corporations to prevent software piracy due to the level of responsibility enjoyed by these
individuals. An audit trail can be used to collect incriminating evidence of illegal copying and thus will act as a deterrent.

173. "Propose NBS R&D Program to Help Guard Gov't CPU's." 

Representatives Jack Brooks and Dan Glickman have proposed legislation calling for the National Bureau of Standards to study the security of government computer installations. All federal agencies would be required to train their employees in computer security. A Government Operations Committee report says that federal computer systems lack internal security controls and audit checks.


Testimony was presented to the Subcommittee on Transportation, Aviation, and Materials, House Committee on Science & Technology discussing information security. The discussion is divided into four areas: (1) information security, affect on automated systems and their telecommunication networks today, (2) legislation, policy, management and auditing in relation to information security, (3) problems contributing to information security due to audit findings of the last 7 years in relation to the factors of legislation, policy, management, etc. and (4) federal findings that could impact the previously stated problems. Ample testimony is given on the seriousness of computer security vulnerabilities. A five page attachment is included that lists GAO reports covering major information security and federal computer matching efforts. (RH)


The increase in the use of microcomputer systems in offices is creating a greater need for security. Many companies do not view security as a high-priority issue. Major security risks focus upon areas such as unauthorized access to data bases, data integrity, hackers, disaster recovery, vandalism, movement of data off-site and physical safety of hardware and software. Several factors that must be considered are education of end users, controls regarding the purchase of hardware and software, audit of data to insure integrity of government regulations, and computer crime bills. (RH)

Westinghouse Electric Corp. has refused to supply the Defense Department with subpoenaed internal audits. The Defense Department has turned the case over to the Justice Department. The Pentagon is seeking these records in order to verify that it was not overcharged on several contracts with Westinghouse. The government has previously been denied access to confidential corporate records.


Computer crime is discussed in detail from two perspectives, access controls and communication controls. The need for a stricter level of controls is presented as being essential in computer technology, especially in the areas of accounting information systems (AIS) and electronic data processing (EDP). Given are the primary objectives of controls in information transactions and in the detection of exposure reduction. Three categories of exposure reduction are given and discussed: (1) preventive, (2) detective and (3) corrective measures. (RH)


While the data processing security officer and the data processing auditor of an organization approach their tasks differently, they seek a similar goal: protecting the assets of the organization from intrusion. The security officer reaches for potential weaknesses in computer security and the auditor reaches for actual weaknesses in computer security. The security officer provides recommendations to reduce the weaknesses and the auditor provides recommendations for decreasing the weaknesses.


Microcomputers, especially hooked up to modems, offer a security risk. Unauthorized users may access protected data or may accidentally destroy data on a disk. Four danger areas are cited: theft of the actual computer or a part; theft or misuse of data; software piracy; and malicious damage. Firms are also open to problems via their communication systems, if protection isn't adequate.
Passwords, data encryption and audit trails are three methods suggested for protection. Various anecdotes are included that point out security risks.


Several factors may jeopardize control of accounting applications: (1) less segregation of duties, (2) reduced processing controls, and (3) unrestricted access to data stored in mainframe systems. These have become significant security risks as a result of the growing number of micros. Controls in a microcomputer environment include the following: an audit trail, proper labeling of files, backups of all files and programs, full documentation of the system, and cross-training of employees. Minimization of risks can be achieved by: (1) designation of certain personnel authorizing microcomputer access to the central data base, (2) passwords, (3) read-only access, and (4) a log of who accesses and extracts information from the central system, and what information is taken.


The Data Protection Bill proposed in England requires that systems dealing with automatic processing of personal data register with the government and undergo a privacy audit. Financial auditors have been suggested to carry out the inspections. An alternative idea has been suggested that computer professionals are more qualified to conduct such inspections.


Control Data Australia Pty. Ltd. and the Institute of Internal Auditors have formed a joint venture to produce courseware that would help detect computer fraud. The two groups will use a CDC 110 microcomputer along with the Plato authorizing system. This combination will allow a computer simulation of fraud to be produced and give auditors experience in detecting what the variables are in the simulation as compared to the real world situations.
Tandem Computers has agreed to allow the Securities & Exchange Commission to inspect its books for the next three years. The agreement follows SEC charges that Tandem claimed revenues in 1982 which should have been credited to fiscal 1983. Following an Arthur Anderson audit, Tandem lowered its stated 1982 revenues from $37.2 million to $29.9 million.

**SOFTWARE**


A client accounting package, the Glows Audit and Write-up system, has been introduced by Orion Microsystem. It is a multi-user system, allowing for up to sixty-four interactive terminals. It includes General Ledger, Fixed Asset Reporting and an Audit package. The package runs under Unix and Xenix.


This is a listing of GAO publications prior to 1982 covering a listing of ADP software related subjects, of which, auditing is included. It was prepared for the Panel "Breaking the Software Bottleneck" at the Federal Computer Conference, Washington, D.C. September 20 1984. (RH)


Many audit software packages are available on the market. Often auditors are not aware of packages which could help them in auditing. A directory of audit programs is presented.


Bridge Communications' NCS 150 network control server provides complete records of session-level activities for Ethernet local-area networks. It provides audit trails on-
line or in hard copy. In the event of system overload, contention backup, or if printer thresholds are exceeded, the NCS 150 will sound an alarm.

188. Briggs, G. "Carleton Auditec Pkg. to Fit Honeywell CPU." MIS Week, Vol. 6, No. 28, July 17, 1985, p. 82.

Carleton Corp. has adapted its Auditec reporting and auditing software package to run on Honeywell's DPS8, DPS 88, and DPS 90 mainframes. The machines run the proprietary GCOS operating system. Auditec allows users to use English commands in its COBOL-74 programs. The package consists of an administrative program, a dictionary maintenance program, and a program generator. It was designed to run on IBM machines.


The Reveal Portfolio and Client Management System is designed for brokers and is used primarily as a client management system. The package is ideal for maintaining an audit trail for SEC requirements. The package is easy to use and contains all necessary client data. The package offers a variety of reporting features as well as a calendar. It will even handle the difficult problem of stock splits. The documentation is good. The package runs on an IBM PC.


The Financial Management Software Series from Computer Associates International, Inc. is complete with the release of CA-Asset Management. The on-line, interactive accounting package supports tracking capital equipment and depreciation projection, and it provides a complete audit trail.


American Management Systems' Auditing and Financial System (AFS) is helping the Mineral Management Service (MMS) of the U.S. Department of the Interior better manage its royalty accounting and collection system. The package allows MMS to deposit between $12 million and $15 million in additional interest into the U.S. Treasury each year.

Software products from the ICP Software Information Database are described. Products include audit programs and modeling systems for financial analysis. Product descriptions by vendor, prices, operating environments and ordering information are provided for each product. Alpha index in chart form is included.


Data Securities International (DSI) has initiated a new software protection service called Post. Under the service, DSI, as an independent third party, holds a developer's source code design specifications, and any software modifications in an account. It provides physical protection for the software and maintains an audit trail.


This index to utility software, including data/file management, graphics, query languages, security/auditing, and sort/merge packages, is grouped under the following operating system types: AOS/VS, CMS, DOS, DOS/US, DOS/USE, EDX, MCP, MPE, MUS, OS/US, PRIMOS, RSTS/E, RSX-11M, RT-11, RTE, SSP, UNIX, VM/CMS, VRX, and Other Operating Systems. Within each category, the following information is included: vendor, package, package type, and the page number on which the product listing can be found. Product listings follow the index and are listed alphabetically by vendor under each product type. Each listing provides the following information: specific application, system requirements, operating system, memory required, source language, source code availability, purchase terms, price, number installed, and date first installed.


Since installing Value Computing's SMF Express software package, the systems management facility (SMF) inventory at Reliance Insurance Co. runs to 125 volumes of tape for fifteen months. Previously, the firm accumulated 250 SMF tapes per month. In addition, the SMF package has eliminated
losses due to human error. It is used for job accounting, charge-back, capacity planning, security system monitoring, resource auditing, and performance measurement.


The technical procedures for auditing and controlling the updating of IBM DOS/VSE systems are covered. The functions of the Interactive Programming Facility (IPF), the Maintenance System History Program (MSHP), and some of the commands that are invoked, such as BACKUP and RESTORE, are described. Brief steps are given to update the system, either through a change in a program product (software package) or an application program. The approval of a change and a suggested form are covered. Steps used by the technical services staff to apply maintenance are described, together with the seven IBM library sets. Testing procedures and updating controls are discussed. A list of suggested minimum audit documentation is included.


Easy and Pulsar are both British software accounting systems with full audit trails that allow the records required by customs and excise value added tax (VAT) purposes. The modules for these systems are independent or integrated; both have modules for nominal sales and purchase ledgers, stock control and invoicing. Pulsar, with additional modules, is more comprehensive, useful for a larger company with an accounts department. Easy has an easy-to-use manual and is ideal for a small business and first-time user. The two programs are reviewed with capabilities listed and screens displayed. Operating systems are PC DOS 1.10; PC DOS 2.00.


Top accounting firms are developing their own financial software in order to help them deliver services to clients. Peat, Marwick, Mitchell & Co. offers tax packages, custom systems development and the Government Information Management System. Arthur Young & Co. offers government accounting programs, tax software and general accounting software which are sold along with their consulting services. Coopers & Lybrand offers auditing software. Deloitte, Haskins and Sells are marketing financial software for specialized areas.
In preparation for an IRS audit, a Macintosh user organized his mass of receipts, checks, and notations into a database program. This was accomplished in a few days with the help of Overvue, an information manager for the Macintosh computer. The IRS auditor was very impressed with the database and was able to get a clear picture of the scope and nature of the claims. As a result all deductions were allowed, including an additional $500 found during the input session. The negative side of all this organization is the possibility of privacy invasion.

An evaluation and review is given of three Macintosh-compatible accounting software programs: Back to Basics from Peachtree Software, Symposium from Symposium, Inc., and Rags to Riches from Chang Labs. Specific details of the systems are compared summarizing the similarities as well as the drawbacks of each.

An audit of software used as a tax shelter is performed by XXCAL for the IRS. The company sees to software products that are overvalued by the publishers, determines the proper valuation, uncovers shortcomings in design or documentation, and offers suggestions on a product's marketing. The findings are reported to the IRS which decides what action to take. The review process takes about forty to eighty hours, and about one-hundred products are reviewed a month at XXCAL.

Errors in creating spreadsheet models can cause serious problems that are difficult to detect. Two new spreadsheet auditing packages can help spot errors. The Spreadsheet Auditor from Consumer Software sells for $99 and runs with Lotus 1-2-3, Visicalc, and Supercalc. Docucalc is from Micro Decision Systems and runs with Lotus 1-2-3, Symphony,
VisiCalc, and SuperCalc. Docucalc comes in French and English. The Spreadsheet Auditor reportedly is easier to use.


CableKey, a stand-alone automated funds transfer cable test and verification product for banks which are not associated with a funds transfer network, provided seven status reports and a detailed audit trail as part of verification. CableKey operates on IBM PCs with hard disk and printer. The program is distributed by Bankers Trust Information Services, New York, NY.


The Spreadsheet Auditor helps the user design, program, test, and debug a spreadsheet. This package, designed by Consumers' Software of Vancouver, BC, consists of four utility programs: auditor, cross-reference, macroanalysis and sideprint. The Spreadsheet Auditor is described as a productive tool to be used in conjunction with LOTUS 1-2-3, Symphony or SuperCalc.


A new software package, MRP II Software Audits has been introduced by Manufacturing Software Systems, Inc. This new Audits system is designed to help evaluate MRP software for implementation. Audits will compare a company's requirements with the functions a software package can do.


POST from Data Securities Int'l (DSI) allows the establishment of protection through the states of program design, development, marketing and sales. An audit trail of transactions is also generated. POST ensures product delivery with documentation of the software development cycle and assures end users controlled access to source code.
Choosing an accounting system for a microcomputer requires knowledge of accounting, business operations and computers. Certified public accountants do not generally have enough understanding of computers to give advice on software. There is little correlation between the quality of packaging, cost of a package, number of features and the suitability of a package for a particular business. Criteria to consider are documentation, audit trails, expandability and size limitations. The best way to choose accounting software is with the aid of an independent professional consultant.

Microcomputers have enabled many companies to have in-house computerized accounting systems. General ledger is considered a good starting place. It offers companies both day-to-day control over their bookkeeping and evaluative techniques for financial reports. Characteristics of general ledger packages are reviewed, including what to look for in a package. These include financial reports, thorough audit trails, ease of use, ease of upgrading and degree of modularity, so programs can work together. An insert discusses accounting software used by CPAs. Photographs and profiles are included for two users. A chart lists forty vendors and ranks their products on twenty-seven characteristics.

Cooper Industries is a Fortune 500 manufacturing company with fifteen independent divisions, each using its own data processing system. The company's internal auditors needed a report writer software package which could run on any IBM mainframe operating system and interface with both Cullinet Software, Inc.'s IDMS and Cincom Systems, Inc.'s Total data base management system, so that the software could be used throughout the company's various divisions. Carleton Corp.'s report writer Auditec met these criteria, so it was selected by the company. Cooper has expressed great satisfaction with the product, because it is easy for all auditors, not just DP auditors, to use and offers the portability needed for performing quick field audits at any company installation.

Audit is a generalized report writing system that allows customization of forms and use of preprinted forms, and it produces required reports and calculates interest. Audit may be purchased from Shaw Systems Associates, Inc., and works on the IBM 370, 43xx, 303x, and 308x.


Computer auditors are responsible for the accuracy and efficiency of a company's data processing systems and software. A variety of companies, including large conglomerates, banks, manufacturers, and insurance companies, have acquired auditing software that has greatly improved efficiency and decreased dependency on programmers. Auditing packages save time in setting up and reviewing application software and most packages require little programming experience. A chart lists fourteen auditing packages with their vendor, requirements, and price.


An auditing package can help to eliminate stress in a DP manager's life. These packages can assist auditors in locating potential problems. The same system that gives the auditor independence from the programming staff can also be used by the MIS manager to prove expenditures. As more information becomes automated, auditing packages become more of a requirement.


Advanced Computer Techniques Corporation (ACT) has a network processor (NP) software package that permits a Honeywell DPS/ Level 6 processor to handle communications functions. Some features of NP are: message routing, multiple host, audit trail, remote console operation, and local disk storage for communications functions. Future versions of NP will feature gateways, local area network, electronic mail, word processor communication between similar and dissimilar equipment, and protocol format.

NCRMDB Symplex Systems has announced release 2.0 of its menu generator, security system called EASYMENU. It is designed for NCR's IMOS, IRX and ITX users. New features on this release of the security and audit system include: the sign on password, access codes that establish what a user can run at a particular terminal, a ten-character audit code that can be defined for a password and the menu system manager that can now define four eighty character lines on the enter password screen.


Audit System's new, enhanced version will produce documents interesting to bank managers as well as auditors, including deposit and loan payment schedules. Audit System is flexible, allowing customized reports and easy data retrieval.


The Bank Audit System recalculates savings account and loan interest and balance for reliability checking against a bank's records. The fifteen program system is used by both internal and external auditors and requires some EDP training. The mainframe based COBOL system runs on all DOS or OS IBM and Burroughs machines.


Design/1, from Arthur Anderson, supports design teams that work on development projects for the IBM PC and PC/XT. Pre-defined structure charts, automatic cross referencing and audit capabilities are some of the features.


Randall Smith, production control manager at the Denver-based Affiliated Bank Services Co. (ABSC), was shopping for a utility that would help the internal auditors compare two versions of one program and allow programmers to perform
data comparisons. The utility had to be capable of running on the company's IBM 3083 mainframe under MVS. Smith found what he wanted in Sterling Software Marketing's Comparex package. It has a test mode that synchronizes by lines and a data mode that synchronizes by fields. The package can handle all file organizations, including VSAM, ISAM, and partition data sets (PDS). The programmers of ABSC are pleased with the utility.


This directory of security/auditing software is listed alphabetically by vendor. It is divided into two categories: large systems software and microcomputer software. Each product description includes the package name, the specific application and/or industry for which the package is designed, the hardware and/or operating system on which the package runs, the amount of memory required, the source language, the availability of source code, the purchase terms, the price, the date first installed, and the number installed. Following the product listings is a product locator index, also divided into large system and micro applications. The index provides the name of the package, its price, and the page number on which the complete product description can be found.


There are many factors to consider when selecting a software package for a particular application or function. One very important selection which is often overlooked is the question of control and audibility. Control refers to the screening of data, such as business transactions, and the correction or rejection of this data, while audibility refers to the need for an audit function to be performed on results produced by a computer, mainly when a company's financial statements are involved. By giving these two areas high priority when selecting a software package, purchasers
can eliminate many potential problems, though until software certification standards are established, buyers must consider carefully their specific data processing needs.


Audit software programs provide greater security than alternative tools for auditing. The software falls into two primary categories: auditing data and comparing source notes. The programs grant auditors the freedom to work independently of the data processing staff. Audit programs sample and calculate data, perform financial analysis and trend line analysis, and provide frequency distributions and histograms.


In order to obtain higher quality in their audits, the First Tennessee Bank in Memphis decided to train their financial auditors to write their own software. The ability of auditors to write their own software resulted in increased creativity, and more time for EDP staff to concentrate on tasks beyond that of the routine audit tasks.