1977

Management, control, and audit of advanced EDP systems; Computer services guidelines

American Institute of Certified Public Accountants. Auditing Advanced EDP Systems Task Force

COMPUTER SERVICES GUIDELINES

Management, Control and Audit of Advanced EDP Systems

American Institute of Certified Public Accountants AICPA

Notice to Readers

Computer services guidelines are published to assist members in understanding and utilizing various aspects of data processing. These guidelines represent the recommendations of the computer services executive committee on the various topics covered.

Prepared by

Auditing Advanced EDP Systems Task Force

Everett C. Johnson, *Chairman*
Burton J. Cohen
Richard Gnospelius
Leslie J. Hellenack
William E. Perry
Kenneth A. Pollock
Larry D. Van Horn

Paul Levine, *Manager*

Approved by

Computer Services Executive Committee (1975-76)

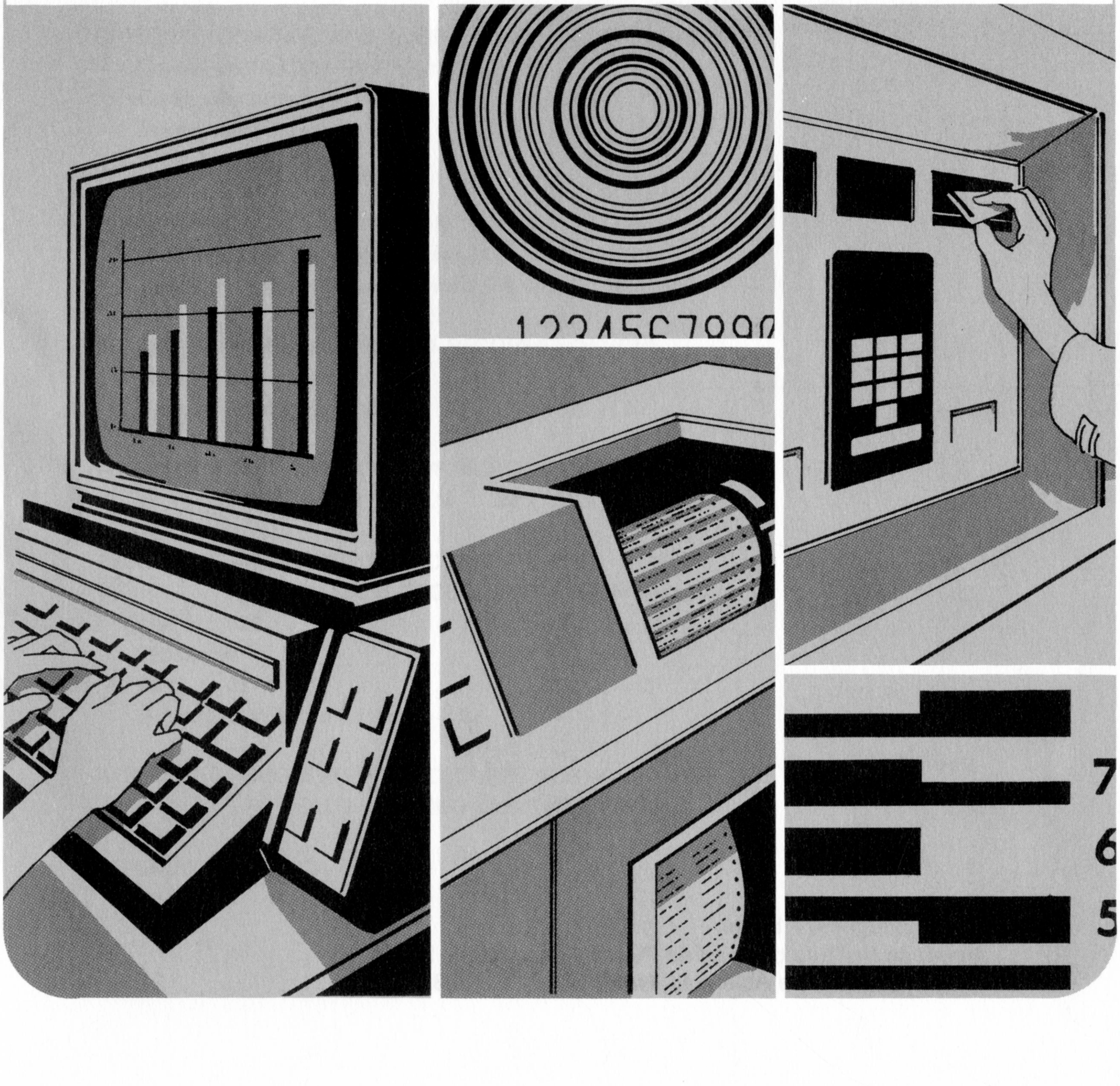
Richard J. Guiltinan, *Chairman*
John C. Broderick
Michael Carrozza, Jr.
John P. Harrison
James K. Loebbecke
Lawrence J. McDonald
John W. Nuxall
William E. Perry
Howard M. Schnoll
Paul B. Woodfin

Donald L. Adams, *Managing Director*
Paul Levine, *Manager*

COMPUTER SERVICES GUIDELINES

Management, Control and Audit of Advanced EDP Systems

American Institute of Certified Public Accountants AICPA



1211 Avenue of the Americas, New York, N.Y. 10036

Contents

Preface

For a variety of reasons control usually takes a back seat to other objectives in the development of innovative electronic data processing applications. The pressure to bring a new application "on the air" by its scheduled date often causes desirable control objectives to be overlooked or not implemented. This, in turn, may result in the need to retrofit control mechanisms—usually at considerable expense—after the application has been operating for a time.

In addition, consideration of audit approaches often is deferred until a new system has been operational for some time. Therefore, opportunities to use cost effective EDP audit techniques may be lost.

Adequate control mechanisms have been devised for many present-day systems, but technological developments are leading to more system changes. Advanced systems are now a reality. If the hardware for these systems does not provide adequate controls, or if operating systems do not have the processing integrity to assure proper treatment of all transactions by application programs, controlling and auditing these systems after they have begun operations will be unnecessarily costly and perhaps less successful.

It is to help prevent such serious and expensive mistakes that this report has been prepared.

Chapter 1

Introduction

New data processing concepts in large-scale systems, increased capabilities of minicomputer systems, and the linking of communications and data processing are bringing sophisticated information systems to large and small users alike. In the future virtually all business activities will interact in some way with EDP systems. Control and auditability are paramount considerations in the design of these systems. Since traditional control and auditing techniques may not be responsive to such systems, new techniques may be required.

The scope of this report includes the areas of management and auditor concern about advanced EDP systems, the identification of specific problems, and some proposed solutions to these problems. Basic control and audit features for advanced EDP systems are presented and possible audit approaches are considered. Also, certain of these applications are relevant to today's systems.

Most importantly, this report is intended to stimulate discussion and research in advanced systems technology by computer hardware manufacturers, software developers, EDP personnel, management, users, and auditors. This report defines or identifies problems, but does not provide final conclusions or solutions. Hopefully, it may provide a portion of the impetus needed to launch the study, research, and experimentation that will be required to develop sound management, control, and audit techniques applicable to advanced systems. The matters addressed herein should be considered in the design and development of advanced EDP systems to assure that such systems meet all of managements' needs and can be audited at a reasonable cost.

Objectives and Concerns

EDP systems are now being designed to achieve some of the following objectives:

1. Derive maximum benefit from the capability of linking high-speed computing with high-speed communications.
2. Bring the system closer to the user. Users may include employees, customers, vendors, and others.
3. Automate the decision-making process as it relates to established management objectives.
4. Provide a single reliable source of information regarding the enterprise, and eliminate duplication of record-keeping by replacing previously separate systems with one integrated system.
5. Eliminate the printing of large amounts of detail and the use of large amounts of paperwork to support transactions and other activity.

Advanced EDP systems developed to meet these objectives will use new processing concepts; thus, new management skills and techniques will be needed to manage these systems. New control procedures will be required to maintain the integrity of the systems, and auditors will require new skills and techniques to audit these systems effectively.

This report reflects the concerns of auditors with advanced EDP systems and has been prepared for the consideration of management, hardware manufacturers, systems designers, and developers, as well as auditors. The principal concerns discussed in this report can be summarized as follows.

Internal Accounting Control

- □ Control features and procedures must be provided for communication-based networks and other systems in which accounting information can be accessed or changed from remote locations.
- □ Authorization systems are required to control access to and the processing of accounting information and to maintain a separation of employee functions.
- □ Programmed system controls must be provided since a manual review of input by employees will no longer be applicable when accounting transactions are generated and processed automatically by the system.

□ Provisions for tracing the historical flow of accounting transactions should be provided in systems having accounting significance.

□ Provisions should be made for timely and economical reconstruction of accounting information in the event of its destruction.

□ Management, auditors, and others should be provided with feedback on the performance and integrity of advanced EDP systems.

Auditability

□ Increased audit reliance will be placed on controls in advanced EDP systems.

□ The availability of traditional hard-copy documents and other audit evidence is decreased and the acceptability of system produced audit evidence will become highly dependent on the adequacy of system controls.

□ Requirements for effective audit techniques and audit timing considerations need to be addressed.

□ Auditors need to participate in the system design and development process to a greater extent than they have in the past.

□ Audit cost is significantly affected by the design of the system, the usefulness of system documentation, and the effectiveness of control of accounting applications processed on advanced systems.

EDP Technical Proficiency

□ Higher levels of EDP technical knowledge will be necessary for management, users, and auditors.

Summary

Cooperation between auditors, management, users, hardware manufacturers, and software developers will help ensure that advanced systems provide the advantages they are capable of providing without introducing serious internal accounting control deficiencies. This paper categorizes the areas that require additional control techniques and suggests the following approaches:

1. Techniques and procedures for identification of users.
2. Authorization concepts for validating user requests prior to processing.
3. Techniques to ensure timely processing of authorized transactions, recording of user and process activity, and retrieval of historical data.
4. Tools and techniques for auditing advanced systems.

Organization of the Report

Chapter 2 describes the nature and scope of the audit process as it relates to EDP systems for readers unfamiliar with this area. Chapter 3 introduces the characteristics of advanced EDP systems, discusses their control implications, and raises various concerns and questions addressed to management. Chapter 4 presents recommended features for effective control and auditing of advanced EDP systems and is addressed to hardware manufacturers and software designers as well as management. Chapter 5 discusses audit approaches to advanced EDP systems and describes various audit tools and techniques. Chapter 6 , summarizes the report, provides conclusions, and makes recommendations.

The report contains four appendixes. Appendix 1 contains an illustration of an "advanced" EDP system that might some day exist in a mythical organization called Ultimate Corporation. Appendix 2 presents certain authorization concepts related to information processing systems. Suggested auditor procedures that might be performed during system design are presented in Appendix 3. Appendix 4 is a brief glossary.

Chapter 2

Nature of the Audit Process

Audit Objectives and General Nature of the Audit Process

"The objective of the ordinary examination of financial statements by the independent auditor is the expression of an opinion on the fairness with which they present the financial position, results of operations, and changes in financial position in conformity with generally accepted accounting principles."[1] Although specific audit procedures may differ, the auditor's objective does not change when EDP is utilized in the accounting process.

Independent audits include two broad categories of procedures designed to determine the reliability of accounting data and financial reports produced by the system. The first category includes procedures for the study and evaluation of internal control. The second category includes procedures, called substantive tests, designed to assist the auditor in formulating an opinion about the validity and the reasonableness of transactions and the propriety of accounting treatment of transactions and balances. In an advanced system environment both categories of procedures can require audit techniques that use or involve the computer.

Study and Evaluation of Internal Control

An understanding of the process by which accounting information flows through an accounting system is fundamental to the auditor's evaluation of internal accounting controls and to the design of auditing procedures. The ability to follow the flow of accounting information through the system, normally called an *audit trail,* or *management trail,* is of particular concern to the auditor. The basic components of this flow are the company's transactions covering the exchange of assets or services with parties outside of the company as well as internal transfers within it.

The independent auditor is interested principally in internal accounting controls, which are concerned with the safeguarding of assets and the reliability of financial records. Controls, such as those concerned with operational efficiency, personnel practices, and so forth are called administrative controls and usually concern the independent auditor only indirectly.[2] However, internal auditors, that is, professional auditors employed by the enterprise as distinguished from independent or "external" auditors, frequently are very interested in administrative controls.

The use of EDP in an accounting system requires appropriate procedures to assure effective internal accounting control. Typically, many internal accounting control functions, which were once performed by separate individuals in a manual system, have now become concentrated in an EDP system; thus, basic accounting records frequently lose their visibility and can be altered without leaving a trace. These records may be accessible to programmers, operators, systems personnel, and, in some situations, to users over whose actions these records may be used to maintain accountability.

The auditor identifies internal accounting controls upon which reliance can be placed as a basis for restricting substantive tests. The auditor then performs tests of compliance, which provide reasonable assurance that accounting control procedures are functioning as prescribed.

In a manual system the auditor examines evidence, such as indications of approval and cancellations, that indicates whether the control

[1] Statement on Auditing Standards (SAS) no. 1 (New York: AICPA, 1972), Sec. 110.01.

[2] See SAS no. 1, Sec. 320, for a definition and discussion of accounting controls.

procedures were in fact functioning as prescribed during the period covered by the financial statements being examined. Similarly, in an EDP system the auditor seeks assurance that control procedures have functioned throughout that period. Such assurance, however, is frequently obtained in different ways. Programmed EDP accounting control procedures designed to detect erroneous data frequently leave no visible evidence indicating that the procedures were performed. The auditor can test these controls by reviewing processed transactions to determine whether unacceptable conditions existed and were detected. For example, a computer program developed and run under the auditor's control may be utilized to review a file of sales transactions for the year in order to detect variations from a company's stated credit policy.

In an advanced EDP system the auditor may use the client's computer system to perform tests of compliance. The auditor, in effect, then becomes dependent on the integrity of the system while performing these tests and should follow additional procedures to gain assurance regarding integrity over audit processing.

The auditor then considers the nature of the accounting system, the adequacy of prescribed accounting controls, and the degree of compliance with those controls and determines the extent to which substantive testing procedures can be restricted. Some substantive testing is always required, since auditing standards do not permit the auditor to place complete reliance on internal control to the exclusion of substantive auditing procedures with respect to material amounts in the financial statements.[3]

Substantive Procedures

Substantive audit procedures are directed at obtaining evidence as to the validity and the propriety of accounting treatment of transactions and balances and may include inspection, observation, inquiry, and confirmation.

Evidence supporting the financial statements obtained through these procedures consists of the underlying accounting data and all corroborating information. This includes documentary material such as checks, invoices, contracts, and minutes of meetings, confirmations and other written representations by knowledgeable people, information obtained by the auditor from inquiry, observation, inspection, and physical examination, and other information developed by, or available to, the auditor that permits reaching conclusions through valid reasoning.[4]

The traditional independent evidence, such as copies of invoices and purchase orders, is often replaced by computer prepared records. The records usually are in machine-sensible form and can be inspected only by using EDP techniques. Without adequate controls over access to preclude unauthorized changes, these records may provide little evidence for audit purposes.

The effect of advanced systems on the audit process discussed in this chapter is explored in greater depth in chapter 5.

[3] SAS no. 1, Sec. 320.71.

[4] SAS no. 1, Sec. 330.03 and 330.05.

Chapter 3

Characteristics and Implications of Advanced Systems

Early computer applications tended to be single-purpose systems dealing with one component of the organization, such as, payroll or billing. Advanced applications now transcend departmental boundaries and perform multiple functions simultaneously. Advanced systems are beginning to encompass most or all of the activities within a business enterprise and interact directly with the advanced systems of other firms. These systems may lead to more efficient and effective information management, but they will introduce different control and audit problems.

Automatic interactions among various elements of an advanced system may leave no visible audit trail. Such systems should ordinarily be designed to provide some form of an audit trail. System interaction with persons or systems external to the enterprise will present control problems. Such features will likely become more widespread and more complex as technology advances.

Such sophistication frequently makes it impracticable to use traditional control and audit techniques developed for, and appropriate to, earlier systems. Batch control techniques, for example, are unsuitable for systems in which files are immediately updated as each transaction is entered from various geographic locations.

Characteristics of Advanced Systems

Advanced EDP systems can be large or small. Many "mini-computer systems" incorporate advanced system characteristics. For purposes of this report, advanced EDP systems are those systems (large or small) that possess one or more of the following characteristics:

□ Data communications

□ Data integration

□ Automatic transaction initiation

□ Unconventional or temporary audit trail

Each of these features is discussed below together with a summary of its control implications.

Data communications. Data communications, in this context, is the linking of electronic communications with electronic data processing. The complexity of data communications systems ranges from a simple remote teletype terminal linking a small computer, to a complex network of computers and terminals. Data communication facilities provide the processing linkages for time sharing, on-line, real-time, remote job entry, and distributed processing systems. Information in these systems, including programs, transactions, decision rules, and so forth, can be introduced, modified, or accessed at sites distant from the data processing installation. This is a marked change from most early EDP systems in which all access, input, processing, and output was physically accomplished and controlled at the computer center.

Data communications capability may be illustrated by an airlines reservation system. A national terminal network is used to communicate with a central computer system to reserve seating space, cancel reservations, and inquire about the booking status and passengers on any flight.

Systems of this type frequently are termed *transaction-driven* or *event-driven* because each transaction is entered into the system individually and immediately processed against all files it will affect. This contrasts with earlier systems in which input was frequently collected and batched for subsequent processing.

Data communications also makes distributed processing possible. For example, a network of small computers, usually used for local processing, can be linked to large central computers such that sharing of information and processing can occur throughout the network. Such networks also provide large scale computing capability to the user of small computers.

Traditional computer systems usually require information to be entered on special forms, subjected to control total checking, reviewed and approved by responsible employees, and processed in batches by computer department employees. Advanced systems eliminate many of these procedures and may accomplish equivalent functions in different ways. When data communications capability is used to provide direct interaction with outsiders, intervention and review by employees may be eliminated. For example, bank currency dispensers or automated teller terminals are now common in many areas of the country. A bank customer inserts a special card, enters a special identification code number, and depresses keys to indicate the amount and type of transactions being consummated. Cash is dispensed, transferred between accounts, applied to loans, or deposited. The information is recorded electronically without the action or even the presence of a bank employee.

Implications. Controls at all locations accessing the system are essential. Control at terminal sites is important because computerized information may be subject to alteration from any terminal in the absence of such controls. Procedures for identification and authorization of users are necessary. When several computers or terminals at different locations are used in a system, weak controls at one location may compromise the effectiveness of controls elsewhere in the system.

Distributed systems also need carefully designed controls; not only to properly handle the data transmitted, but also to manage the operation of each individual computer. As with terminals accessing a central computer, distributed systems computers at various points in the network can modify or access information at other locations.

Data Integration. Data integration can lead to more effective use of the computer. Essentially, it minimizes redundant record-keeping which usually arises when separate applications each use their own separate files. For example, application-oriented files may contain identical information for each employee, as shown in the table below.

Recording identical data elements in more than one file may waste computer resources since additional file space must be allocated in order to record the same information in multiple locations; additional processing is required to modify the information in each file when changes occur.

Periodic review must be made of identical elements in multiple files to make certain the values in each file are the same and to correct wrong values. In an integrated system, it is often cost-effective to record most information elements only once and automatically retrieve them when desired for processing.

The data in the previous example could be physically recorded in a data base system as follows: One area of storage would contain the employee number, name, address, and other personnel information; another storage area might contain all manufacturing history transactions in job number sequence (those transaction records containing labor information would not contain any employee information, rather, they would contain an identifier, called a *pointer,* specifying where that information could be found); a third area might contain payroll disbursement information that might consist of only date paid, gross pay, withholding, and net pay amounts with pointers to the related manufacturing history and personnel records.

	File		
Data Element	**Payroll**	**Personnel**	**Manufacturing History**
1. Name	X	X	X
2. Employee number	X	X	X
3. Social security number	X	X	
4. Home address and city	X	X	
5. Rate of pay	X	X	X
6. Withholding information	X	X	
7. Job assignment	X	X	X
8. Other skills		X	
9. Education		X	
10. Employee history		X	
11. Next of kin, beneficiaries		X	
12. Job hour charges			X
13. Job number			X
14. Date charged			X
15. Operation code			X

The data base management system makes the logical connections between these various data elements by using the pointers and produces the equivalents of each of the three flies described in the table on page 6.

Implications. Today's systems frequently have features or controls that restrict access to data files to authorized persons for authorized purposes. Because data base information may be available to the system at all times, different authorization procedures will be required. A carefully constructed system of authorization for access to each data element in the system should be established to prevent improper access or manipulation by persons having no legitimate purpose for accessing the information. Thus, authorized employees in the personnel department might be able to access and change pay rate information but would be precluded from accessing or changing manufacturing data. It is only through such an authorization system that the concept of segregation of functions—a concept fundamental to adequate internal accounting control—can be maintained in an integrated system.

Responsibility for each data element in the data base should be established. For example, only one department should be able to add names to the customer file, assign numbers, and maintain addresses for each customer even though this data is accessed by many users.

An auditor needing information in a data base will require appropriate tools to access it in an independent manner. Such access may present control, timing, and auditor training problems.

Automatic Transaction Initiation. Automatic transaction initiation is present in many systems today, and its use will increase in advanced systems. Already many systems automatically generate invoices, checks, or orders to ship, produce, or purchase goods—actions frequently are taken without human review of their correctness. An inventory control system will serve to illustrate the situation.

In early EDP systems, when on-hand balances reached certain predetermined levels, the computer may have produced a reorder notice. This notice would be reviewed by an employee and, if appropriate, a purchase order would be prepared. Advanced systems have economic order quantity information in the system and not only detect reorder points but also produce the purchase order for resupply in the most economic lot size. Issuance of such purchase orders without human review has become common and may become more widespread when purchase orders are transmitted directly to vendor systems by data communications. In some cases, where automatic transaction initiation uses sensor-based data collection methods and/or data communications, hard-copy documents may not be produced, although the supporting data would be retained in machine-sensible form and would be available for recall. (See Appendix 1 for an example of such a system.)

Implications. These systems frequently do not use hard-copy source documents to support transactions other than the action documents created by the system. In the case of the automatically generated purchase order systems cited above, there may be no manually reviewable output to permit an evaluation of the proposed action. In the absence of a readable document showing a history of usage, planned requirements, present balances, and amounts already on order, the correctness of the automatically initiated document may be difficult to judge.

Here again, system controls assume great importance and it behooves both management and auditors to assure themselves that such controls are designed into the systems and cannot be circumvented. For example, one such control for the automatically generated purchase orders might be to print out supporting information for all purchase orders over a given amount and for a specified percentage of smaller purchase orders. This supporting information could be manually reviewed before the order is released and should be retained for audit review purposes. Where possible, controls should be incorporated into systems of this kind to validate the genuineness and reasonableness of automatically initiated transactions and to prevent or detect erroneous transactions.

Unconventional or Temporary Audit Trail. Most EDP systems today generate a trail of transaction activity used by both management and auditors. This information is frequently printed in detail, making it readily available for use. These printouts are gradually being discontinued as systems evolve, although the information may be retained in machine-sensible form. Auditors have developed and presently use generalized audit retrieval packages, or computer programs, to access such information.

All systems should possess audit trail capabilities, but some advanced systems may produce a machine-sensible audit trail whose retention period may be relatively short. The short retention may result from the expense of preserving the information for an extended period of time in machine-sensible form compared to lower cost alternatives, such as microfiche.

In some cases transaction documents are microfilmed and the documents themselves destroyed shortly after origination. The magnetic media on which the data was entered may be "scratched" (electronically erased) and used for other purposes. To follow the audit trail may necessitate the use of a microfilm reader. Although high-speed microfilm retrieval systems are available, the use of generalized audit retrieval packages is precluded.

A backup copy or "dump" of the data base poses particular problems for auditors, who will need to be knowledgeable about the technical and complex structure of such material in order to be able to deal with it effectively. Such dumps may be of limited value for audit purposes.

Implications. If original documents of the kind used by auditors are no longer available for indefinite periods of time, certain audit procedures will change. External auditors, for example, may have to alter both the timing of their auditing procedures and the procedures themselves. The organization's internal auditors may provide assistance to the external auditors by coordinating with them on the selection and testing of specific kinds of critical transactions. This would require the external auditor to become more involved in the work of the internal auditor.[1] Management also requires the ability to investigate reported results and frequently uses auditing techniques for this purpose. Suitable audit capabilities and the requisite technical proficiency to deal with such situations must be developed.

Management Implications of Advanced EDP Systems

Management implements advanced systems when it believes they offer potential for enhancing the organization's competitive position, improving cost control, and facilitating operations in general. Management should consider the total impact of such systems.

Changing Environment. As EDP evolves from individual applications to those that completely encompass operating and planning functions, it is very probable that some organizational structures will change. As management recognizes information for what it is, that is, an organizational resource, the need for appropriately controlling and managing it becomes obvious. Proper channels of information, both within the organization and between it and its environment, will cut across traditional boundaries and may promote restructuring of the organization to help achieve management objectives.

The continued computerization and integration of functions into a unified system also raises considerations for management; among them are the following:

1. Data bases in advanced systems may contain very sensitive corporate data, such as strategies, goals, and forecasts. Special safeguards will be needed restricting access to this data to authorized users only.
2. In most of today's systems, certain individuals are responsible for passwords and similar controls and therefore can access any file, program, or table, and make untraceable changes. This capability could extend to anyone obtaining the appropriate passwords. Control procedures over the actions of those who are responsible for access controls are needed.
3. Training of personnel who will interact with the system can be a major undertaking and will involve managers, users, designers, programmers, operators, auditors, customers, suppliers, and government agencies.

As advanced systems evolve, there will be a reduction in human intervention in the processing of information. Since criteria for decision-making will be incorporated in the computer systems they should be applied consistently. Such systems will require effective control mechanisms to preclude the entry and processing of erroneous information.

Data may be entered from remote terminals without manual review. The result is that operating personnel and outsiders will directly interact with the computer. Such interaction requires control mechanisms to strictly monitor and enforce authorization and transaction processing rules.

Erroneous input accepted by the system may remain undetected and cause additional errors. Designers of these advanced systems should

[1] See Statement on Auditing Standards no. 9, *The Effect of an Internal Audit Function on the Scope of the Independent Auditor's Examination* (New York: AICPA, 1975).

provide adequate controls to allow only authorized use of the system, to detect erroneous data, and to prevent such data from being processed.

Control seems to follow innovation in EDP systems. Early punched card systems used the same controls as manual systems until it was found that a card could too easily disappear either accidentally or intentionally. Control totals or "hash" totals were introduced to validate the accuracy and completeness of a file.

When magnetic tape files were developed, those same concepts were transferred to tape labels until it was found that they, too, could be bypassed easily. With the development of magnetic disc files, hardware vendors corrected the control weakness of bypassing labels by forcing the user to create a label for every disc file used.

Facilities will be needed for control in integrated data bases and communication-based systems. Procedures should be established to maximize the opportunity for those control facilities to keep pace with future innovation rather than lag behind.

If the possible difficulties and risks of advanced EDP systems are not properly analyzed, evaluated, and considered and countered in planning by management, a single adverse occurrence could seriously affect a firm's business. Controls must provide for a high level of system integrity. Management and auditors will need an ongoing capability to determine that system integrity is being maintained.

Audit Implications for Management. Early EDP systems had both hard-copy source documents and detailed printed output. Many audit objectives could be achieved without auditor involvement with the computer system. As these documents and outputs are eliminated the auditor's approach will change. This may impact audit cost—a subject of management concern. In an advanced system environment, audit cost may be considered a component of system cost. Factors substantially affecting audit cost in this environment are quality of system documentation, effectiveness of controls, ease of locating, retrieving, and testing information, and audit methodology.

The auditor reviews system documentation to understand the system and choose efficient audit procedures to accomplish the audit objectives. Audit cost is greatly increased if adequate documentation is not available.

A poorly controlled system could also greatly increase audit cost because substantive audit tests cannot be reduced. In some of these situations audit testing may become impossible. Management should consider the effect on audit efficiency when considering control costs and making decisions on the control system techniques to be employed. Auditors and management have a commonality of interest in effective control. Prudent management will, therefore, request auditor involvement during the system design process. This should result in significant subsequent audit economies and should provide management with additional confidence that a well controlled system will be produced.

The availability of effective tools and techniques for audit retrieval and testing can often help improve audit effectiveness and reduce audit cost. Therefore, alternative audit methods and related tools should be considered during systems design.

Chapter 4

Effective Control and Audit of Advanced EDP Systems

This chapter, which sets forth control and auditing objectives for advanced EDP systems, is directed to management and to the designers and developers of hardware and software.

Suggested control and auditability features are set forth together with some practical methodology for meeting these requirements.

Control and Auditability Objectives

Internal control and auditability objectives in advanced EDP systems cannot be achieved by the auditor alone. Control and auditability features must be designed into advanced systems by both hardware manufacturers and system and application software designers.

Control Objectives

□ *Access to assets* is permitted only in accordance with management's policy and objectives. Obviously, certain individuals will require access. The number of persons having such access should be limited and there should be a segregation of functions between the EDP department and users.

□ *Transactions are initiated* in accordance with management's authorizations. Transactions may include accounting transactions, system or program changes, authorization table changes, and so forth, and may originate externally or within the system.

□ *All transactions are promptly recorded* (1) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and (2) to maintain accountability for assets.

□ *Accountability records are compared* periodically with the actual assets or other resources and appropriate action is taken with respect to any differences.

Auditability Objectives

□ *Audit trails* should identify what detail transactions are included in summarized results. An audit trail should consist of information about who performed what, when, in what sequence, and the results thereof.

□ *Audit evidence* should be controlled and protected from loss, alteration, or destruction.

□ *Audit control* should result from achieving the above control objectives such that the auditor can obtain assurance that the audit processing integrity is maintained.

□ *Audit tools* are provided to permit the auditor to interface with systems and information in an independent and cost effective manner.

Advanced computer systems may be unauditable unless these requirements are properly understood and implemented. One of the primary purposes of this paper is to identify those features that are necessary for effective control and provision of auditability in an advanced EDP systems environment.

Control Features

To achieve the control objectives in an advanced EDP systems environment, the system should be designed to provide the following features:

1. *User Identification.* The system should have the capability to uniquely identify each of the specific persons using the system.
2. *Request Authorization.* The system should be able to determine if the processing or information request of a user is authorized.
3. *Process Integrity.* The system should be capable of controlling and processing all validated user requests in an appropriate time frame.
4. *Activity Logging.* The system should be capable of recording all user activity, such as the number of attempted log-ons, request type, and the like, as well as recording information about the processes executed.

User Identification. A cornerstone of any control system is the determination of who is authorized to do what. Therefore, the system should be able to determine with whom it is interacting. The system must be able to identify each user or set of users. It should be capable of responding to a wide variety of requests ranging from a chief executive officer who needs information related to competitors, industry trends, executive performance, and so forth, to clerical personnel who may only need detail transaction information.

Currently, most interactive systems identify a specific subset of users by password and/or by terminal location. Thus, anyone who knows the password and who has access to the terminal location can access system files. Some systems carry this process a step further and allow users to name and identify their own files. Thus, even though one user can access the system, another user's files cannot be accessed unless the file names are known. However, most of these interactive systems have an "administrative user" who is responsible for issuance and control of user identity codes and passwords and can theoretically access all of the information contained within the system. Any user who can obtain the administrative user's password can do the same.

There are some specific techniques under development that would allow a system to uniquely identify a given user. The use of voice print, thumb print, or similar technology may become common in the future. Future systems should be able to specifically identify users as a requisite to any effective user control scheme.

The identification methodology implemented must allow an enterprise to classify users so that all specific subgroups or single users can be identified by the system. For example, a system could allow all accounting clerks access to the system through specific terminals, but allow the financial vice president access through any terminal. The identification of users is the precursor to the authorization of user actions.

Request Authorization. Once the user has been identified the system should provide the capability to determine precisely what information can be accessed and what processes can be performed by that user. Although some terminal-based systems presently incorporate access authorization and activity/security routines, this capability does not effectively exist in many systems today. For example, in the absence of effective request authorization procedures, application programmers or system programmers could obtain unauthorized access to stored data or programs. These individuals frequently possess the necessary ability to obtain such access.

Advanced systems may contain a wide range of sensitive information and should be able to restrict users to only the data they are authorized to access. Naturally, this requires the enterprise to identify and maintain some type of formal authorization procedure. This could be in the form of an authorization table that would relate users to the types of transactions they could process against specific data elements.

Once the system has identified a specific user or class of users an authorization control routine could determine, by interrogating the authorization table, if the user has been authorized to process the transaction entered and to access the information or data required. The authorization routines should be flexible so that factors such as the time of day, terminal input location, day of the year, and so forth, can be factored into the process. When a user request passes all applicable authorization tests, the appropriate application program then would be executed and the output routed directly to the user or wherever designated.

Although a comprehensive authorization process with all these capabilities probably could not be implemented with present-day technology, neither auditors nor system designers should be limited to thinking in terms of present-day technology. For example, data dictionary/directories, which identify each data element and its relationship to other data elements and programs, are being implemented in many of today's more advanced computer systems. This is a trend that will continue and that could be expanded to provide authorization table capabilities. Future computer systems could have expanded dictionary/directories or other mechanisms that relate users to authorized input requests, processes, and information. This kind of linkage would allow the auditor to determine the processes executed for a given type of input request. For example, the typical process steps associated with the entry of a sales transaction are as follows:

- Preparation of shipping documents.
- Preparation of sales invoice.
- Update of the appropriate accounts receivable data elements.
- Update of appropriate product inventory data elements.
- Explosion of products sold into component parts and/or raw material requirements.
- Test for reorder point for all components and/or raw materials affected.
- Update the appropriate sales registers.
- Update the appropriate sales commission data elements.
- Update any appropriate royalty data elements.
- Update the appropriate contingent liability data elements if product is guaranteed or warranteed.
- Update the other appropriate data elements.

In a conventional system, most of these are treated as separate transactions and are handled by such departments as sales, accounting, or shipping. Each step would require some form of authorization procedure. Application systems have been and are being developed that would have the capability to perform all of the above steps and update all appropriate information elements whenever a sales transaction is entered into the system. The auditor will no longer be able to walk through a typical transaction to understand the process steps involved; he may, however, be required to analyze the contents of the dictionary/directory to determine the path that a specific type of request follows through the system and the authorization procedures related thereto.

Process Integrity. Currently, as programs are executed in either a batch or interactive mode, hardware controls and operating system controls maintain program integrity. These controls are acceptable now, but should be expanded to meet advanced system needs for program and data integrity.

In an advanced systems environment a wide variety of users will be interacting with the system and executing the same or different processes simultaneously. Typical processes can include compiling a program, updating data elements, validating a user's password, and so forth. Once a system has determined that a user has been authorized to execute a specific process, the system must be able to complete that process within the time constraints required by the user.

To accomplish this the system must schedule each user process and permit multiple users to access many of the same information elements almost simultaneously. As a practical matter, the system must be able to maintain the status of each data element and control the sequence of access and update.

Specific system controls are required to maintain process integrity and consistency, and to permit reconstruction of events and recovery in the event of system failure. These controls may require the use of high-speed memory to record the status of all programs being executed and data accessed or a similar technique that allows definitive boundaries to be drawn around processes and their effects.

The results of any given process activity may necessitate a system generated response to computer operations, managers, auditors, or others within the enterprise. For example, an operations officer in a bank may want to be notified when and by whom a transaction greater than a stipulated dollar amount was processed, or an auditor may want to know when a transaction affecting a dormant account was processed—the system could provide this information.

Other control features will be required if advanced systems have the capability to analyze the results of each processing step or program execution and dynamically generate, eliminate, or resequence the steps in the queue awaiting processing.

Activity Logging. Once a specific step in a process has been completed, the system should have the capability to record or log who executed what process step and what data elements were affected. The system must be able to record this data on a file accessible only to specific personnel. This data should not be accessible to those persons over whom accountability has been recorded. As an example, the activity log that records password changes made by authorized personnel should not be accessible to those personnel. Similarly, the activity log that records the auditor's access to the data base must not be accessible to the auditor.

Although the primary purpose of the activity log would be for control, it would be useful to management in reviewing compliance with stated policies and procedures and for other audit purposes.

An entry in this log need not be generated each time a user enters a transaction, or each time a process step is executed. Rather, it is up to the enterprise to identify specific users, kinds of transactions, and process steps that require logging. For example, the activity log might contain the following information:

□ Identity of the user
□ Process(es) requested
□ Time and date of request
□ Process(es) performed
□ Results obtained

The generating and logging of the foregoing information will allow the auditor or others to effectively monitor who is accessing what information within the enterprise.

Auditability Features

The features desirable in advanced EDP systems to ensure that the systems are generally auditable are the same features desirable for effective management of the information system. A possible exception might be the form and period for retention of information for audit purposes. Previously stated auditability objectives relate to audit trails, audit evidence, audit control, and audit tools. These auditability objectives might be met if the control features previously stated are implemented into advanced computer systems. For example, one of the auditability objectives is audit control; that is, the auditor requires the capability to audit the system without being wholly dependent on it. In the past this has meant that the auditor might copy files related to financial applications and process them on a separate computer system with specially written audit programs. However, when systems have the high level of control achievable with the recommended control features in this chapter, the auditor might gain assurance regarding the independence of audit processing by reviewing activity logs that cover periods during which the audit processing was performed.

The authorization control concept alone will provide all auditors of advanced systems with potentially much greater independence than is available today.

Audit Tools

Audit tools provide flexible information retrieval and testing capabilities for the auditor. These capabilities are outlined below and in chapter 5.

Advanced EDP systems should include an easy-to-learn declarative language that will allow auditors to interrogate a data base, perform mathematical operations on data base elements, format output files, generate reports, and so forth.

Naturally, auditors should be able to perform these operations using compound selection criteria such that a specific subset of information could be generated without involved programming. For example, an auditor in a banking environment may want to select only those employee accounts with account balances greater than $1,000 that had more than ten transactions in a biweekly period.

The system should provide this kind of capability and provide users with special purpose routines such as statistical sampling, regression analysis, model-building modules, and the like to aid in the audit effort. With these routines the auditor would be able to statistically select random samples for testing and perform analytical audit procedures.

Additionally, the auditor should be provided with the capability to specify which kinds of user requests should be automatically logged onto an audit file. The auditor should be able to specify that all requests, a stipulated percentage of all requests, or those that meet a given criteria, be written to the "audit log" file. This capability is different from an activity log that documents who performed what request. The audit log provides the auditor with an audit trail of the transactions that were processed against specific information elements. For example, the auditor would be able to specify that all transactions affecting a particular cash general ledger account or that all employee balance accounts be automatically logged.

Advanced systems should be designed with "audit hooks" that would allow the auditor's programs to be integrated into the normal process activities associated with specific transactions. This feature would provide the auditor with the capability to monitor processing activity and select specific transactions for exception reporting or audit testing. This capability could be used in various ways. For example, the audit department could be notified "on-line" when a user request of a specific kind was entered into the system. This type of routine could be used to monitor transactions involving dormant accounts in a banking environment. Systems and applications program changes could be similarly monitored.

Today, portable computers that can process in a "stand-alone" environment, or communicate with a large computer system are a reality. The auditor could access the information system, select financial transactions for testing, and transfer these transactions to a separate "auditor's computer" for analysis. This approach is fast becoming cost effective in today's environment. Advances in technology will surely make this approach even more cost effective tomorrow.

The information system schematic (exhibit 4-1) depicts the control features described in the previous sections.

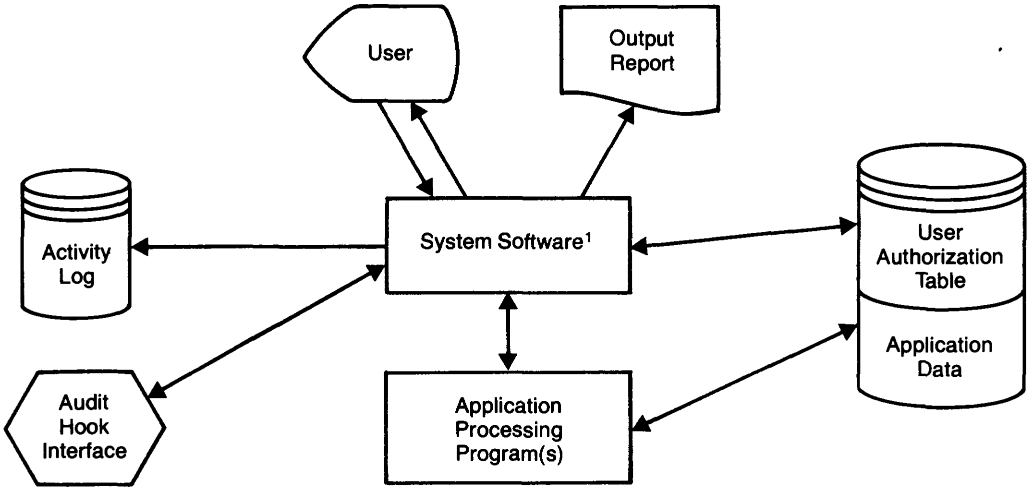
Users who have terminal equipment access the information system, and the authorization control routine accesses the authorization table and determines whether or not a user's identification or sign-on parameters are acceptable to the system. If they are, user entered data related to transaction type are validated against appropriate entries in the authorization table.

If all criteria are met, the processing program(s) are then called and control is passed to them. When processing is complete, control is passed back to the authorization control routine and appropriate activity logs created.

The purpose of this schematic is to present on a conceptual level the control features that auditors believe are necessary in an advanced systems environment—it is not a proposed solution. These features will permit the control objectives relating to access to assets, transaction initiation and recording, and comparison of records of accountability to be achieved.

All of these capabilities can be incorporated into an advanced system. If they are, they will provide management and the auditor with much needed control and auditability features.

EXHIBIT 4—1 INFORMATION SYSTEM SCHEMATIC



[1] Includes the following routines:

Input/output
Authorization control
Data management
Audit hook
System management

Chapter 5

Audit Approaches for Advanced EDP Systems

This chapter relates advanced EDP systems to the audit process described in chapter 2 and presents potential problem areas with their related audit considerations and suggested tools and techniques for auditors. This chapter provides the auditor with a starting point for considering the effect of an advanced EDP system on the audit process. The material is directed to the independent or external auditor; but, many of the audit techniques and approaches may be suited for use by internal auditors. This chapter also has the secondary purpose of providing information to management and EDP personnel regarding auditing considerations relevant to their advanced EDP systems.

The principal objective of the independent auditor is the expression of an opinion on the fairness of the financial statements of the enterprise in conformity with generally accepted accounting principles or with a comprehensive basis of accounting other than generally accepted accounting principles. The study and evaluation of internal accounting control is an intermediate step in the audit process. The term "auditing advanced EDP systems" refers to those auditing procedures that relate to the understanding or testing of such systems or the results produced therefrom. Such understanding and testing is not an end in itself, but a part of the audit process.

Many accounting control techniques in advanced EDP systems will differ markedly from those in present conventional EDP systems. Nonetheless, the review and evaluation approach to EDP accounting controls followed by an auditor will most likely continue to be along the lines set forth in the AICPA audit and accounting guide on that subject.[1]

When auditing advanced EDP systems, the auditor will likely place a high degree of reliance on advanced EDP systems controls and may use the system to perform compliance and substantive testing procedures described in chapter 2. Therefore, audit review of the design and development of an advanced EDP system can help assure that control and auditability are adequately considered. The audit considerations during the systems design stage are outlined in this chapter.

Auditing Advanced EDP Systems—Some Differences

The areas of difference between conventional EDP systems and advanced EDP systems, from an auditing point of view, include the following:

1. Complexity
2. Nature of evidential matter
3. Relationship between accounting controls and evidential matter
4. Nature of audit control
5. Audit trail considerations
6. Techniques required for access to information
7. Timing of audit procedures

Each of these is discussed below with their attendant audit concerns.

Complexity. One of the most significant problems facing the auditor of an advanced EDP system is understanding the flow of accounting information through what may be a very complex series of processing steps that frequently interact with each other and with those in other systems. The auditor's preliminary objectives are to identify (1) how transactions are initiated

[1] See AICPA Audit and Accounting Guide, *The Auditor's Study and Evaluation of Internal Control in EDP Systems* (New York: AICPA, 1977).

and flow into the financial statements, (2) the relationship between the EDP and manual portions of the system, and (3) the basic structure of accounting control.

Proper documentation, audit review during system design, and effective internal audit reviews of advanced EDP systems can all significantly reduce the time and, consequently, the cost of this phase of the audit. Standardization of systems (such as operating systems and application systems) by their developers, together with an approach similar to the "third party auditor review,"[2] could also reduce audit cost. Under this suggested approach, an auditing firm might obtain a system description suitable for audit use, review and test the standardized system, and provide a report directed to other auditors describing the results of these procedures and suggest tests that an auditor might perform on such a system.

Nature of Evidential Matter. The auditor needs sufficient competent evidential matter to afford a reasonable basis for an opinion regarding the financial statements under examination.[3] In manual systems and some EDP systems, this evidence includes documents evidencing actions (for example, approvals), transactions, assets, or obligations, which the auditor can examine or confirm with independent parties.

Machine-sensible evidence can be changed without leaving a trace. Today, auditors frequently compare items selected from machine-sensible records to appropriate source documents to obtain satisfaction that transactions have been properly recorded. These approaches may not be feasible in some advanced EDP systems because independent or supporting documents may not be available. Other techniques will be required to provide and control the evidential matter needed by the auditor.

Relationship Between Accounting Controls and Evidential Matter. In applying a traditional audit approach, the auditor seeks to identify accounting controls upon which reliance may be placed. The auditor then tests compliance with these control procedures to obtain satisfaction that they are operating as prescribed. Whenever these controls appear to be functioning effectively, the auditor may be in a position to rely on them as a basis for appropriately restricting the extent of substantive auditing procedures. Alternatively, if the auditor chooses not to rely upon accounting controls, compliance testing is not necessary, although substantive testing cannot be reduced.

In advanced EDP systems the alternative of not relying upon accounting controls may not exist. The auditor may be required to understand and test for compliance those controls that effect the following:

1. Affect the validity or integrity of system controlled or initiated audit evidence.
2. Restrict the ability to alter evidence in machine-sensible form.
3. Provide a basis for effective audit control when the auditor relies on the system for testing purposes.

For example, most bank currency dispensers produce a transaction record, one copy of which is provided to the customer. A second copy is retained within the dispensing device and is used to support the daily transactions, such as the cash disbursed. This transaction record copy might provide useful evidence for audit purposes if the controls over the initiation of transactions and over the creation and handling of these documents are effective. If these controls are not effective, the traditional audit approach of extending the testing of these documents would not be effective. In such a situation, the auditor would have to consider whether alternative procedures, such as confirmation with the bank's customers, could provide satisfactory audit evidence, or whether controls are so lacking that it is unlikely that any conclusions can be made from further audit testing.

In order to audit effectively in an advanced systems environment, the auditor will probably place a high degree of reliance upon the controls in the system. Effective accounting controls are requisite to such reliance. The auditor, therefore, may be required to understand and test these controls. In the absence of these controls, the auditor may be unable to audit at a reasonable cost.

Nature of Audit Control. All audit testing, whether manual or involving EDP systems, must be performed with independence and objectivity. Whenever client personnel provide assistance in the performance of audit procedures, an accepted practice is to supervise, review, and test this work before placing reliance upon it.

[2] See AICPA Audit and Accounting Guide, *Audits of Service-Center-Produced Records* (New York: AICPA, 1974), wherein the concept of a review of an accounting system in use at a service center is made by a "third party auditor" and relied upon by auditors of the customers of the service center.

[3] See SAS no. 1, Sec. 330.

When the auditor performs tests in an EDP environment, certain client provided programs frequently are used. For example, if the auditor were to prepare, test, and process a program to make statistical selections from files maintained on a client EDP system, the auditor usually will be required to use the client's operating system, data management system, or similar programs. In order to obtain satisfaction that audit reliance can be appropriately placed on those programs and that the integrity of the audit testing has not been compromised, the auditor should obtain reasonable satisfaction that those elements of the system being used are properly functioning.

In an advanced systems environment this reliance may be more difficult to obtain. Effective and auditable controls over access to systems programs, such as the operating system and the data base management system, could provide a basis for reliance for audit purposes. In the absence of such controls, the auditor may be required to use an independent computer system or use more costly alternative procedures that provide the degree of independence required.

Whenever audit testing is to be performed using EDP techniques in an advanced systems environment, the following general procedures are suggested:

1. Consider which of the following elements of the client's system are being relied upon for the audit tests to be performed:
   a. Operating system
   b. Data base management system
   c. Data communications system
   d. Application programs
2. Consider whether appropriate controls exist to provide a satisfactory basis for relying upon each of the above identified elements.
3. Identify how compliance with these control procedures can be tested to the extent deemed necessary if reliance is to be placed on such control procedures.
4. Process the audit application and consider some method of independent verification of the audit processing results.

Audit Trail Considerations. One of the characteristics of advanced systems is the use of unconventional or temporary audit trails. Audit trails in the form of transaction listings and the like may not exist in these systems. More likely, the audit trail will exist in machine-sensible form for limited periods of time. Microfilm, microfiche, and highly condensed printouts and summaries of information will likely constitute more permanent forms of audit trail information. Documents supporting transactions may not be centrally filed and, in many cases, may not exist.

A typical audit trail environment might be as follows: The accounts receivable system is designed to retain microfiche copies of customers' statements for audit trail purposes. This information is also retained in machine-sensible form on the data base system for approximately two months, after which time it is destroyed. In order to audit efficiently, the auditor will require access to the machine-readable records. Otherwise, the auditor may be forced into the uneconomical alternative of reviewing large volumes of microfiche records and applying essentially manual audit procedures to them.

Machine-sensible audit trails may exist for shorter times (as little as a few hours) in some systems. The auditor may choose to access this information directly from the data base. This approach is discussed below. Another approach is to use one or more of the tools and techniques discussed in the last section of this chapter. These techniques may enable the auditor to create "selective audit trails" based upon transaction type, transaction amount, time of day, or any other criteria.

Techniques Required for Access to Information. As more and more information is integrated into advanced EDP systems, computer-assisted auditing techniques will likely become the most economical method to access this information for audit purposes. The auditor will require tools to access information contained in a data base and to access control information relating to advanced EDP systems. This capability will be fundamental to performing an effective audit.

In a traditional EDP system, information usually is stored or recorded (physical form) in a manner that represents the logical or conceptual view (logical form) of the file. For example, an accounts receivable file may contain one or more records for each customer with balances due. Each record might contain the customer number, name, and related information pertaining to that customer's account. These records are normally ordered in customer number sequence.

In a modern data base system, information is physically recorded in a manner that bears little resemblance to its logical form. For example, the logical form of the previous example would be unchanged. The physical form might be to record on one area of a disc the customer number, name, address, and so forth. Another disc area might contain all sales transactions in date and invoice number sequence. These transaction records would not contain any customer information, rather, they would contain a pointer to the information in the customer disc area. A third disc area might contain customer remittance information. This might consist of only date received, amount, and pointers to the related sales transaction records. The data base management system makes the predefined logical connection between these respective physical data elements and would be used to produce the logical equivalent of the balance due file described in the previous paragraph.

Obviously, the auditor accessing information in such a data base ordinarily will have to use the data base management system to make the necessary logical connections between physical data elements. In that case, the auditor should consider the audit control implications of such use. Independent computer audit programs could be developed as an alternative to placing reliance on the data base management system. Such programs have not become widely used, principally because of the complexity of developing a generalized approach to accessing data in physical form from a variety of data base formats.

Generally, data base information must be at a static point in order to be useful for audit purposes. An interactive system that operates on a twenty-four-hour basis may not be suitable for audit use unless a proper cutoff can be established.

Timing of Auditing Procedures. The auditor traditionally has performed audit testing some time after transactions have occurred. In an advanced EDP systems environment, certain auditing procedures will be performed immediately following transaction occurrence. In some situations, auditing procedures may be performed before transaction processing is complete. This may be accomplished by auditor controlled computer audit programs that are "embedded" in the system. Unscheduled visits or testing initiated from remote terminals are other techniques applicable for this environment. Ideally, the auditor will become involved during the systems design process to ensure that necessary accounting controls, audit routines, and the like are incorporated into the system.

Auditing Approaches to Advanced Systems

The auditor of an organization using advanced EDP systems will need to possess adequate knowledge and experience of EDP in addition to that required in accounting, auditing, taxation, and related subjects. Many situations will require the auditor to utilize, supervise, and review the work of EDP audit specialists.

Technical Proficiency. Some of the functional areas of skill and proficiency that will be necessary for these auditors and EDP audit specialists include the following:

1. Data processing functions
   a. Data entry techniques
   b. Computer configurations (for example, minicomputers and communication networks)
   c. Operating environments (for example, multiprocessing and virtual storage)
   d. File organization and updating (for example, random processing, integrated data base processing, and shared files)
   e. Processing environments (for example, batch-mode and real-time)
2. EDP auditing tools and techniques
3. EDP control concepts

Although the "general" auditor will obviously not require an in-depth knowledge in all these areas, some knowledge at the conceptual level will be necessary in order to properly supervise and review the work of those EDP audit specialists possessing such in-depth knowledge.[4]

The Auditor's Participation During Systems Design. The auditor is concerned with the following kinds of questions during the design of advanced EDP systems:

- What control procedures should be included in the system to provide for effective accounting control?
- What is the best approach for auditing the system in a cost effective manner?
- What audit capabilities should be incorporated into the system?
- What degree of audit control should be provided over audit programs and data files?

The auditor has the best opportunity to assure that these issues are satisfactorily

[4] See Elise G. Jancura, "Technical Proficiency for Auditing Computer Processed Accounting Records." *Journal of Accountancy*, October 1975.

resolved by reviewing systems during the design stage. Frequently, the auditor may suggest that additional control procedures be incorporated into the system, that certain unnecessary control procedures be eliminated, or that additional records or testing capabilities be provided for audit purposes. Such controls may result in more efficient operation of the system. Modifications are more easily made during systems design rather than after the system has become operational. Changes to an operational system can be extremely costly and will most likely be met with a great deal of resistance. While this approach is applicable to all EDP systems, it is much more important in advanced EDP systems.

The general steps that an auditor might take during the systems design stage are set forth in Appendix 3.

Review and Evaluation of Accounting Controls. Because of the complexity of some advanced systems, a first-time review of accounting controls may be time consuming. This review, which may be substantially completed during the systems design stage, should be followed by subsequent review and testing procedures. Audits at a later time may require repeating these procedures.

The first review of a proposed or an existing system should be directed at gaining an understanding of the system, identifying accounting controls and the audit trails, determining the potential degree of reliance to be placed on the controls, and developing an effective audit approach. The procedures to be applied during the systems design stage, which are discussed in the preceding section and in Appendix 3, can be adapted to meet the objectives of a first review of an existing system.

Subsequent procedures are those necessary to complete the review, perform compliance testing, evaluate the accounting controls in the system, and determine the nature, timing, and extent of substantive testing. These procedures also are outlined in Appendix 3.

General Controls. General controls include those that relate to more than one application. They include such procedures as segregation of functions, and controls over access to data and programs. In an advanced systems environment, a high degree of reliance upon general controls will be necessary. The general controls incorporated into operating systems, data base management systems, data communication systems, and similar systems can be key elements that contribute to effective accounting control.

Since general controls span application boundaries, the activities of personnel responsible for these controls should be subject to close supervision and control. For example, systems programmers, who are responsible for maintaining the programs in the operating system, which controls the functioning of all other programs, could disable a key control feature, such as the necessity for passwords to access data, thereby rendering many other controls in the system ineffective. An effective procedure for review and approval of all changes to operating system programs could be used to mitigate this possibility. For example, a program is presently available that creates a log of all modifications applied to the operating system. This could prove to be a useful management and audit tool.

The auditor should consider the effect that controls at other locations may have on those at the location being evaluated. For example, in a distributed system, poor controls at one location could compromise otherwise effective controls elsewhere.

Application Controls. Application controls are those that apply to a single application. For example, the control procedures that would be used in an automatic inventory reordering system would be unique to that application. Examples of application control procedures include those designed to allow (1) only authorized input to be accepted for processing, (2) the review and control of correction and resubmission of errors detected by the system, and (3) processing results to be subjected to limit and reasonableness checks. Application controls, to be effective, depend upon effective general controls.

The trend in systems development appears to be toward greater use of "general" systems, for example, data base systems, where possible, and is moving away from systems that handle only a single application. Hence, a greater emphasis will be required on the review and understanding of general controls as a requisite to the evaluation of application controls.

Audit Testing—Advanced System Considerations. Audit testing can be classified into two types of tests:

1. Substantive tests of the validity of data underlying transactions and balances.
2. Compliance tests designed to provide assurance that the controls being relied upon are functioning properly.

The auditing problems discussed earlier in this chapter, particularly those related to evidential matter and reliance on controls, should be considered when applying testing techniques to advanced EDP systems. The balance of this chapter will discuss audit testing in an advanced systems environment and will discuss the considerations for designing such tests together with some tools and techniques which may be useful for such testing.

Substantive Testing. The auditor should consider the problems raised under evidential matter earlier in this chapter when designing substantive tests. Specifically, the availability of independent evidence, the dependence upon the proper functioning of controls and their relationship to the acceptability of this evidence, and the susceptibility of unauthorized changes to this evidence should all be considered by the auditor. Close integration between compliance testing and substantive testing may be required.

Compliance Testing. A general approach to designing and developing compliance tests could be as follows:

1. Identify the control procedures being relied upon in the following areas:
   a. To place reliance upon the controls over system produced evidence used for substantive testing.
   b. To reduce the extent of substantive testing.
   c. To place reliance upon system controls or system programs while performing other tests.
2. Identify the appropriate time periods to be covered by the test. In audit situations substantially all of the period being audited is preferable.
3. Identify which kinds of transactions, logs, or other records of compliance are available for testing.
4. Consider the extent to which each of the identified records might be used for other audit purposes.
5. Design and apply the particular compliance test.
6. Determine the effect of the testing results upon the controls being evaluated.

Compliance testing can be performed using either actual transactions, such as live or historical data, or simulated transactions, such as dummy data.

When the auditor elects to test actual transactions, they are usually tested for evidence that control or system features being relied upon by the auditor have functioned properly. Transactions, as viewed in this context, could include accounting transactions or systems transactions, such as program or system changes. Compliance tests are intended to provide assurance about the controls, but not about the validity of the underlying accounting transactions.

Actual transactions can be tested manually or can be tested during computer-assisted audit techniques. Live data includes actual transactions as they are being processed. Historical data, on the other hand, includes transactions that have been processed completely.

Testing with simulated or dummy transactions involves the use of auditor introduced test transactions in an attempt to ascertain whether a control operates as prescribed on these transactions. The system being tested in this manner could be the actual system operating in a live mode, or it could be a copy of the system or particular program of concern. In situations where a copy is utilized, the auditor needs to obtain reasonable assurance that the program and changes tested represented a copy of those actually used throughout the period covered by the audit procedure. While it may be difficult to obtain evidential matter about which programs were used, librarian systems that maintain a record of all program modifications can prove to be helpful.

Audit Testing—Tools and Techniques. This section discusses some tools and software-based techniques applicable to auditing in an advanced systems environment. The tools and techniques can be divided into the following three general categories: (1) those that operate on live data on a real-time basis, (2) those that operate on historical data, and (3) those that utilize simulated or dummy data.

The techniques matrix at the end of this chapter summarizes the information discussed in the following sections. The following is not intended to be an exhaustive list or teaching guide, but rather serves to familiarize the reader with some advanced auditing techniques.

Techniques Using Live Data. *Techniques* in this category usually require that all data relating to the particular test to be performed be subjected to an audit selection step before or during normal processing. This selection step identifies specific transactions of audit interest. The identification would usually be based on auditor determined criteria such as dollar amount, transaction type, authorization code, statistical sampling considerations, and so forth. In most situations all transactions of interest would be processed through an audit program or "audit module," which performs the requested identification. Audit modules could be a part of the vendor supplied operating system, the application programs, or some other system component.

Audit hooks are points in a system that allow audit modules or programs to be integrated into the normal processing activities. Audit hooks can be described as "windows" into the system and audit modules could "look through" these windows and select transactions as they are being processed. Audit hook capabilities should be provided by systems designers at certain points in the operating system, data communications system, data base management system, and application system. Also audit hooks should be provided by the vendors of computer hardware so that certain types of hardware control operations could be subjected to audit testing. Audit hook capability, once incorporated, should be carefully controlled.

Once the particular transaction of audit interest has been identified, it is available for analysis by the auditor and could be retained in machine-sensible form or printed for subsequent audit followup. Each of the techniques below is illustrative of one type of processing of these identified transactions.

"Tagging" transactions—A "tag" or indicator is affixed to "identified transactions" early in the processing cycle. The auditor is then provided with a complete trail of all paths followed by the tagged transaction in the application system. This trail can be in machine-sensible form or printed so it can be analyzed by the auditor. Other data with which the tagged transaction interacts at each significant processing step can be captured and displayed for the auditor as well.

For example, all sales transactions over a certain amount or any of a predetermined list of customers could be tagged. Transaction data, credit limit, current unpaid balance due, delinquent amounts due, and so forth, could be retained to permit the auditor to analyze the credit approval process.

This technique could be useful for compliance testing purposes. The auditor might place more reliance on the results because actual transactions are used in the processing. The flow of transactions through the system can be portrayed in a manner that will greatly enhance the auditor's understanding of the system. In some situations, transaction tagging may prove to be an acceptable alternative to a complete audit trail for all transactions.

The capability of capturing and displaying audit information for previously tagged transactions should be considered and incorporated at the time a system is designed. Attempts to apply such an approach to a previously designed and programmed system can be extremely costly.

Real-time notification—Real-time notification is the continual review of previously identified transaction types for audit purposes. This review could be implemented by using an audit hook approach. Transactions having certain audit significance can be printed immediately on an auditor's terminal or listed for audit follow-up at a later point in time. Specific transactions could be analyzed, and if they meet specific criteria (that is, if the transaction was of a certain kind, the transaction amount was greater or less than a given value, and so forth), a message indicating the type of transaction would be forwarded to the attention of the security officer or other appropriate authority and, if appropriate, to the auditor. In some cases, a response from the security department or other appropriate authority would be necessary before the transaction could be completed. In other cases, no response would be necessary. The normal audit use of this kind of data would be to check compliance to policy by reviewing exceptions.

This technique might be particularly useful for significant transactions such as those of very large dollar amount or those having potentially widespread control implications, for example, changes to key portions of operating system programs. The live data can be normal accounting transactions, requests for system resources, such as access to certain files, or nonaccounting activity, such as program changes.

Audit log—The audit log is used to provide a record or log of certain data processing activities whenever they occur. The previously identified transaction types are written into a record or file that should be available only to the auditor. In some data base systems, the audit log contains a record of every transaction processed. The auditor could later print or use other techniques to analyze these records and make further tests as considered appropriate.

An audit log normally would record events as they occurred at a specific point in a system. Examples include attempts to access a particularly sensitive file—including an auditor's file—change certain passwords, override certain approval criteria, and so forth. Since it can be used to focus attention at control points within the system, this technique is probably useful as a part of compliance testing.

Monitoring systems activity information—Monitoring is the use of hardware and/or software to analyze the activity within a computer system. While the prime objective in many of the approaches in use today is to determine the efficiency of use of hardware and software resources by applications, they do offer the auditor the data with which to review actual systems activity.

The live data to be monitored normally would include program initiations, data file accesses, hardware allocations, and so forth. Financial transactions usually would be excluded. The monitors generally use data about the functioning of the system and tend to answer the questions of who uses the system and what system resources are used.

Applications of this technique could be expanded to include control functions performed by the hardware and by systems software.

Techniques Using Historical Data. These techniques generally are designed to provide the auditor with the capability of working with previously processed data in machine-sensible form. This data would include accounting transactions, systems data, and summary level information. Also, data captured during processing by one of the previously discussed techniques could be considered historical data if analyzed at a later time. Audit hooks, as described above, are not necessary to apply these techniques because data has already been processed.

Audit languages and programs—If an easy-to-learn audit language was available, auditors could interrogate data base files, perform mathematical operations on historical data base elements, and format output files or reports based on compound selection criteria without the need for special programs. Auditors could use this language for most of their needs, but the system should allow them the capability to add their own special-purpose modules such as statistical sampling, regression analysis, or business modeling.

Auditors should have available a library of generalized programs to perform audit tasks under their control. These programs could be used in compliance and substantive testing.

The capabilities afforded by these languages and audit programs also can be utilized by management and should be provided by both hardware and software vendors.

Simulation—Another method of determining the accuracy of processed data is for the auditor to reprocess it and compare the results obtained with those generated by the company's processing. This technique, called simulation or reprocessing, can be applied with auditor developed programs, an audit language, or by an auditor review of authenticated copies of the company's programs. The following example might best illustrate the use of this technique.

At the beginning of the year, the auditor requests copies of all application programs of interest. At various times during the year, the auditor may appear at the client's office and request processing of, say, yesterday's transactions against the auditor's copy of the program. Results can then be compared with the company's results to gain some assurance that processing is in accordance with company policy. The degree of such testing would depend on the existence and operation of a variety of controls at the installation. Input material for many applications is "scratched" shortly after use; therefore, such testing usually cannot wait until the end of the fiscal year. This approach can be most effective when done on a surprise basis.

Because of its potential costliness, the auditor may devise methods of duplicating only certain portions or modules of the client's program and still obtain the required assurance. Another technique would be to use an audit language for simulation purposes.

Extended records—Under the extended records technique, additional information is retained in each record so that a complete audit trail can be maintained. For example, a customer name and address record might be designed so that prior versions of the address will be maintained as part of the record. Thus, a complete audit trail of all address changes within a particular account would be available at any time. Since this approach increases the required amount of storage capacity, it could become quite expensive. Until advances in technology reduce storage costs, the extended records technique may be used where the availability of this kind of audit trail warrants the cost.

Other Techniques. This category of techniques includes those that use simulated or dummy data and those that analyze programs by other means. Since actual transactions are not used, these techniques can provide assurance only as to compliance.

Integrated test facility (ITF)—The integrated test facility is a means of introducing dummy data into a live application system to see whether it is properly handled. The data is introduced as though it were live data and must be removed at some point during the application.

For example, a dummy customer account may be set up against which the auditor could issue purchase orders, receive goods from the company, return goods, pay for them, and so forth. These dummy transactions are entered along with the real transactions of the day with no distinction between them. The auditors can observe the treatment accorded the transaction on the company's records and have some assurance that prescribed controls are, or are not, functioning properly. Exceptional transactions can be attempted—taking unwarranted discounts, ordering in excess of credit limits, returning more goods than purchased, and so forth—to verify compliance with stated policy.

Close control of all ITF transactions entered should be maintained to assure that the financial statements have not been inadvertently distorted by the processing of test transactions. If this technique is in use by internal auditors, the firm's independent auditors should verify that all ITF transactions have been backed out properly or otherwise controlled.

Program analysis techniques—Some auditors believe that a review of the detailed program steps is a useful approach to understanding and evaluating accounting controls. This approach may be appropriate when there is no practicable alternative to gaining an understanding of the controls or processing steps in a program. Although there are tools available to assist the auditor with such a review, this approach can be quite complex, time-consuming, and require a detailed systems and programming knowledge. This approach should be viewed as a part of the review of the system; it provides little or no assurance as to compliance. Once a program has been reviewed, it should be tested as appropriate for the kind of compliance assurance desired.

Program analysis techniques permit the auditor to analyze the functioning of a computer program or series of programs. Transaction data is not used in the process. Rather, the rules by which the transaction will be or has been processed are analyzed.

In the process of *tracing,* using a special program, the computer is made to print out each client program step as it is performed. The auditor could determine by reviewing the printout whether processing has been completed in accordance with his understanding of the program logic. The auditor may acquire a better understanding of the application and become aware of unused portions of the program (which may be potential problem areas). It is, however, a costly technique and should be used only when it is necessary to review detailed code and detailed execution.

Mapping is basically a subset of tracing. Instead of printing every step, the review program prints out only the steps related to decision points in the client program. The auditor could again determine if certain parts of the program were not used and could investigate to find out if this was appropriate. If the selected steps were in fact performed properly, the auditor has some assurance that the programmed controls are operating.

In the process of *recompiling and comparing,* the auditor obtains and reviews a control copy of client programs of interest at the start of the audit period. At a later time, the auditor obtains a copy of the current version of that program and compares the current copy with the control copy. If there are no differences, the auditor has some assurance that the program has continued to process properly—having previously been satisfied as to its correctness. If there are differences between the two, the approved changes made to the program should be reviewed. This technique might be used in conjunction with tracing or mapping. This can be a laborious and time-consuming method, especially if programs are relatively volatile. It requires a relatively comprehensive programming knowledge on the part of the auditor.

There are a series of other tools and techniques available to auditors for certain situations. These include the following:

- Various *flowcharting packages* which enable the auditor to produce a flowchart of the computer program logic. The auditor starts with a program source code which is processed by the flowcharting package producing the flowchart.
- *Decision table analysis packages* which can produce the logic of the program in decision table format. Some of these packages can use a decision table as input to generate a program that can be used to simulate the processing of the program to be tested.
- *Cross-reference systems* which can provide listings that show every occurrence of each name used in a program. Such a listing can be a valuable aid in the review of a program.
- *Performance analysis packages* which can be used to detect unused portions of a program. This can be useful for identifying program instructions that are triggered by special or unusual circumstances or events.
- *Test data generators* which can quickly create files containing valid and/or invalid data that can be used to perform high volume, comprehensive tests. This can facilitate a "test file" approach for complex advanced systems analogous to the "test deck" approach used by auditors in punched card systems.

Many of these techniques can be used together to provide highly effective audit capabilities. For example, the use of a test data generator, coupled with a performance analysis package, can provide an extremely effective testing technique. After the test data has been created, it can be processed through the program to be tested under the control of a

TECHNIQUES MATRIX

Technique	Capability Supplied by	Used by	Data Used	Purpose	Advantages	Disadvantages
Transaction tagging	Vendor or application system designer	Auditors and managers	Live accounting	Compliance and substantive test	Full range of selectivity	Adds to overhead of system, special programming
Real time notification	Systems programmer or vendor	Auditors and managers	Live accounting and system	Compliance test and control	Control and timeliness	Cost
Audit log	System designer	Auditors and control personnel	Live accounting and system	Compliance and substantive test	Specified transactions logged for audit review	Cost
Monitoring	Vendor	Auditors and managers	Live system	Review actual system activity	Shows what has happened	Requires technical knowledge to interpret
Audit language and programs	Vendor and system designer, software house, manufacturer or audit firm	Auditors and managers	Historical and live	Compliance and substantive test. Perform wide variety of audit tests	Retrieves data for audit purposes. Relatively easy to use, not expensive	Requires some programming knowledge by auditor. Presently limited to types of files that can be accessed.
Simulation	Auditors, internal and external with program copy	Auditors	Historical	Determine accuracy of data processed	Permits comparison with real processing	Extensive use can be large consumer of machine resources
Extended records	Design of client applications	Auditors and managers	Historical	Provide complete trail for audit and management purposes	Provides complete account history	Very costly use of machine resources at present
Integrated test facility	Auditors, mostly internal	Auditors	Dummy	Compliance test	Relatively inexpensive	Must be "backed out" very carefully
Program analysis techniques	Special software, contractor or vendor	Auditors and programmers	Usually dummy	Authentication of program operation. Check of key points in program execution	Gives better understanding of application; gives assurance controls are functioning	Needs auditor knowledge of programming, may be expensive; useful only in certain circumstances.

performance analysis package. This test,among other things, will produce a list of program instructions that were not tested. Test data can then be modified or expanded to produce a test file that will exercise every instruction in the program.

Potential Techniques. It is obvious from the pace at which computer technology is advancing that current computer techniques may not be sufficient to satisfy the auditor's requirements in the future. Two techniques that may help satisfy these requirements are program certification and independent computers used for audit purposes.

Certification of programs would permit auditors to rely on the processing of standard audit software packages, such as data base managers, compilers, and other retrieval packages.

Auditors could use an independent computer interconnected to a client's advanced EDP system to facilitate various modelling, simulation and testing techniques for determining the reasonableness of overall record-keeping. These computers also could be used to retrieve live data and to analyze and test systems software with relatively little reliance on the client's system.

Chapter 6

Summary, Conclusions, and Recommendations

Continued change in data processing capabilities and approaches will impact the business enterprise and its managerial style. The auditor's role, while not having changed objectives, will involve significantly altered methods.

The principal purpose of this report was to bring to the attention of various interested parties the thinking of auditors who have already been affected by some of these changes. The long-range potential and the need for careful planning so as to take advantage of these changes, while still effecting adequate control of the resultant systems, has been emphasized.

Conclusions

Development of this report has highlighted the need for communicating the following messages to the indicated parties.

Systems Designers and Providers of EDP Hardware/Software. Advanced products will be used to develop systems for business or other organizations. Such products should provide hardware and systems software features, such as the audit hook capability described in chapter 4, that will permit well controlled and auditable application systems to be designed. If these capabilities are not built into the equipment and the manufacturer-supplied software, individual purchasers may be forced to invest substantial portions of their data processing budgets to provide, through other means, the controls which could have been integrated into your products at substantially lower cost.

Systems developed using advanced hardware and concepts will be subjected to audits. It is better to be aware of the auditor's specific needs at the time advanced systems are developed, rather than attempt to retrofit such requirements after systems are operational. When user requirements are defined, include the auditor's requirements and be prepared to utilize the control capabilities built into the hardware.

Management. Auditors, through their knowledge of control concepts and their experience in audit situations, can make constructive and cost effective contributions to systems of the future. Their inputs may ,be significant not only as to initial system design but as to the operational environment as well.

Auditors. Technical proficiency will be put to a most severe test working in advanced environments such as those discussed in this paper. Audit skills should be kept continuously current through a well-conceived, meticulously operated education and training program encompassing changing technology. By making others aware of the auditor's expertise, auditors will have a greater opportunity to assume a more active role in defining appropriate audit requirements and controls for future systems.

Recommendations

The following recommendations are offered.

Systems Designers and Providers of Hardware/Software. Communicate with auditors to consider their needs, and use their control expertise as a complement in development of new systems.

Consider the auditors' requirements to perform the attest function on an independent basis and their desire to perform it using effective and economical methods.

Provide information about current and future developments in advanced systems.

Management. The goals of management parallel and support those of auditors. Therefore, management should maintain an awareness of significant changes in EDP systems in order to evaluate the resulting impact on the business environment and the need to define and install appropriate accounting controls. Further, management should consider the need to conduct a continuing dialogue with auditors to keep them informed about planned changes in data processing application systems.

Management should take the initiative in obtaining sufficient auditor involvement in the design and installation of advanced EDP systems to foster the implementation of internal accounting controls.

Management should retain the final voice in the implementation of recommended controls, weighing the cost of such controls against the relative risk of not implementing them.

Auditors. Continue to obtain education regarding changes in EDP systems and assist in defining and implementing new and effective controls, and new and effective audit tools and techniques so as to assist in the beneficial use of such systems.

Communicate with management, systems designers, and hardware/software manufacturers. Acquaint them with audit requirements and the desirability of various controls.

Take the initiative in communicating to interested parties about the expertise of auditors in defining and implementing controls.

The AICPA should consider sponsoring, perhaps on a joint basis with other interested organizations, the following types of activities:

1. Establishing a continuing dialogue with major EDP vendors and suppliers to make them aware of the auditors' concerns and requirements in regard to hardware/software audit and control capabilities. This effort should encompass operating systems and other systems software developed by such manufacturers and by others.
2. Devoting additional effort to defining the requirements for a generalized software package capable of interfacing with a data base management system. Consider the feasibility of including, within computer hardware, features that would support the basic objectives of management control and auditability.
3. Identifying and defining attributes, controls, and development procedures that would facilitate a "third party" audit review of software would be extremely helpful, particularly in regard to systems software. The development of applicable standards for such a review should also be considered.
4. Developing a continuing education program to train auditors in the technical and audit considerations involved in advanced EDP systems.

APPENDIX 1

Ultimate Corporation—A Future Advanced System

Ultimate Corporation is a hypothetical example of an advanced EDP system that could be designed in the future. Ultimate is intended to provide a useful illustration of the auditing problems that such systems can present.

Ultimate Corporation is in the business of processing and formulating liquid chemicals. Inventories of raw chemicals are maintained in large vats. These vats are equipped with a sensing device which signals Ultimate's computer system, called UAS (Ultimate Advanced System), when the inventory level falls below the reorder point.

UAS then analyzes the future inventory requirements and economic order quantities to determine the amount to be ordered from one of Ultimate's four major vendors. UAS can connect itself by data communication facilities to each of the four vendor's computers. This capability is used to query the vendor's computers to determine the availability and best price for each item to be ordered. The actual order is transmitted to the selected vendor computer from UAS by data communications and given a common order/shipper number. No traditional purchase order document is prepared.

The vendor's computer then processes the order for delivery. Liquid chemicals are delivered through a direct pipeline connecting the vendor to Ultimate. Ultimate has a sensing device on this pipeline which meters the amount of chemical received and transmits that directly to UAS.

When Ultimate has received the ordered amount, UAS then communicates directly to its bank's computer. Payment for the chemicals received is made by an electronic fund transfer system (EFTS) from Ultimate's bank account to the vendor's bank account. The vendor's computer acknowledges receipt of payment directly to Ultimate's computer. No traditional check evidences this payment.

Ultimate Corporation obviously presents some unique and interesting auditing problems. A number of events have taken place during this transaction cycle. None of these events have been evidenced by any form of traditional documents as we know them. There are no purchase orders, receiving reports, vendor invoices, canceled checks, accounts payable, or other documents or transactions, either internal or external. The integrity of Ultimate's processing is dependent upon the effectiveness of controls in very advanced EDP systems.

Specifically, the problems facing the auditor of Ultimate's financial statements are these:

1. Absence of available independent evidence supporting transactions.
2. Lack of a clear audit trail.
3. Lack of evidence of authorization for transactions.
4. The need to place heavy reliance upon the system of internal control, such as those over authorization and recording of transactions.
5. The need to understand the flow of information through the processing cycle and its relationship to controls.
6. The need to test the controls being relied upon.
7. The need for auditor's hardware or software to be incorporated into this system.

One audit approach to this system might suggest the use of an auditor's sensor on the pipeline and the inventory vats. The auditor could request a machine-sensible file of all electronic fund transfer transactions from the bank and, from each vendor, a file containing their records of all transactions with Ultimate. This information could then be used to verify independently, either on a test basis or completely, Ultimate's transactions with its major vendors which were processed by this system. This approach would require hardware (such as sensors) and software tools and techniques to collect, analyze, and evaluate this information.

The Ultimate Advanced System conceivably could be extended to apply to transactions with Ultimate's customers as well as its vendors. Ultimate could become connected to its customers by a direct pipeline as well. In this environment, one can envision an entirely automated process within Ultimate Corporation. Financial statements could be produced daily and the auditor's opinion thereon might be rendered within hours.

Obviously, this example is somewhat simplified and futuristic. However, portions of the Ultimate systems are in use today. For example, the chemical and petroleum industries both use sensor/computer-based "process control" systems for production purposes. The popularity of electronic funds transfer systems has been growing significantly. The use of data communications between customers and vendors, or even between competitors, as is the case in the airline industry, is also a growing practice.

These systems provide significant audit challenges today and these challenges surely will grow in the future.

APPENDIX 2

Authorization Concepts for Information Processing Systems

This appendix illustrates one view of an information system and has been developed to attempt to clarify one of the key controls—authorization—that auditors believe is necessary in an advanced systems environment. The information processing system described is indicative of those that will exist in the developing generation of systems.

The major elements of an information processing system are these:

1. *Users*—These are internal personnel at all levels and outsiders who prepare and require information through interaction with the system. This information consists of data related to past or future events presented in a format that is understandable and meaningful to the specific user.
2. *Processes*—The techniques, procedures, programs, microcode, or other steps that translate the user's "request" into the information required to perform a given job function.
3. *Data*—The stored representation of the events, records, plans, policies, procedures, programs, and decision criteria of the enterprise. Two broad classifications of data are static data and dynamic data. Static data consists of the records which relate to information that is relatively fixed within the enterprise such as names and addresses of employees, physical plant locations, major customer names and addresses, product descriptions, and so forth. Dynamic data consists of the data associated with the events of the enterprise that change or fluctuate on a daily or periodic basis. This would include, but not be limited to, the data related to the number and value of a given product sold within a limited time span, such as an hour or a day. Essentially, dynamic data is the data associated with a single event which has little meaning in and of itself. Usually, it is only after that data has been summarized for a specific period or set of events that it becomes meaningful information to members of the enterprise.

These three elements or major components of an information system will be discussed in detail in the following sections.

Users

To further an understanding of information systems, it is advantageous to classify users into the following categories:

- *Management* consists of general, functional, or operational employees whose primary purpose it is to direct others and to achieve end results through others. This category of users is primarily involved in the planning and control aspects of the enterprise.
- *Operations personnel* are the employees or others who are primarily concerned with entering, updating, retrieving, and processing data.
- *Auditors* are either the internal or external auditors of the enterprise.
- *Application programmers* are the employees primarily involved in the development of application software who specify, in computer terms, the processes that translate the data into the information required for planning, control, and operational purposes.
- *System programmers* are the employees primarily concerned with generating, updating, modifying, and controlling the general systems software normally furnished by the hardware vendor.
- *EDP control* involves the EDP personnel who are responsible for safeguarding the EDP environment including the creation and changes to the enterprise data base.
- *Computer operators* are the EDP department personnel primarily concerned with monitoring and controlling the computer hardware.

These users may interact with an information system either directly, through terminals or other kinds of input, or indirectly, through predefined processes that are a part of another computer system that is in direct contact with the primary computer system.

Naturally, this is a generalized overview of the possible users within any enterprise, and the groupings are relatively arbitrary to enable us to discuss the concepts related to EDP control and auditability.

Processes

Normally, users request that specific processes be performed by previously written application programs on either data stored within the EDP system, input data or data entered by the user, or a combination of both stored and input data. In some cases, a generalized information retrieval system may be used to produce the information required for a given user, or the user may even develop a program to generate information of interest.

Whether a given user utilizes a set of programs developed for a specific application by the application programmer or whether the user is the application programmer who is performing the task of developing an application program, there are three basic ways in which users can communicate with the EDP System:

1. *Batch.* Users assemble related transactions or requests that are subsequently processed against the appropriate combination of stored and/or input data to produce the results required, which are then made available to users.
2. *On-line Data Entry.* Using data entry devices such as teletypes (TTY), keyboard/video display units (VDU), or other users enter transaction data under program control. This is either stored on temporary files for subsequent batch updating, or is used to update appropriate data elements and return results to users immediately.
3. *Interactive.* Using data communication terminals, users interact with the EDP system to develop application programs and/or modify existing data base elements, and summarize or otherwise manipulate data.

Regardless of how users communicate with EDP systems, there are only two basic functions they can perform on the stored data base:

1. *Retrieve or scan data.* Users can access the stored data and present it in a form meaningful to the enterprise.
2. *Change data.* Users can access the data base and modify the form, value, location, length, character type, derivation alogorithm, or any of the other attributes of specific data elements as well as add or delete data from the data base.

Currently, one of the key control weaknesses of many of the present EDP systems is the ease with which the stored data can be accessed, manipulated, or inadvertently destroyed by one or more of the various types of users. For example, "application programmers" making changes to an existing application system frequently have complete access to the production (live) version of the data associated with the system. Naturally, only copies of live data should be used in testing program changes, and the application programmer should not, in most situations, have access to live data. System programmers also could very easily develop subroutines to modify live data if they are allowed access to application system documentation. This can be done through the "supervisor call" feature associated with many operating systems or by other techniques. Since the operating system normally does all of the input/output, a system programmer could develop a subroutine that would determine when particular records within a specific application system were processed and modify these records as desired. Thus, it is imperative that advanced systems limit the application programmer's and system programmer's access to data that would impact the financial statements.

Data

Although the kind, nature, and variety of data related to any specific enterprise is unique, for the purpose of this discussion it has been arbitrarily classified into the following categories:

1. *Transaction data.* Data associated with the events of the enterprise. For example, a sale, a new employee, a new purchase order, and so forth. Specific accounting related events are cash disbursements, cash receipts,

sales, shipments of material, and so forth. Specific data associated with the initiation or recording of an event must be maintained for audit purposes.

2. *Historical data.* This is data related to the current and historical status of the enterprise. Specifically, it can consist of summary data related to any function, such as the sale of a product for a year, the production capacities of one or more plants, the names and addresses of employees, and so forth. Accounting related historical data consists of the ledgers, journals, and audit trail data that support the financial statements, and the records related to perpetual inventory, accounts receivable, cash receipts, and payments that support asset accountability.
3. *Identifying data and decision criteria.* These are the static data associated with the policies, procedures, and operation of the enterprise. Typically, these would include plant location codes and the related addresses, product codes and product descriptions, and other similar data. Specific accounting related tables would include credit limits, discounts, inventory reorder levels, and so forth.
4. *Application software.* These are the computer programs developed by the application programmers that transform users' requests into viable information. Specifically, accounting related application software impacts accounts payable inventory control, general ledger, sales, accounts receivable, cash management, and so forth.
5. *General systems software.* These are the computer programs related to the operating system, language compilers, such as COBOL and FORTRAN, data base management systems, data communication systems, and various utility programs.
6. *System control software.* These are the computer programs used to control and record the access to all other stored data. This data would include program status and change logs, password control or authorization tables, and system authorization tables.
7. *Audit software.* These are the computer programs used or developed by the auditor to retrieve and process data, simulate application software programs, generate statistical samples, and so forth.
8. *Systems tables.* These are the static data related to the use of the computer hardware systems and could include tables which describe or specify the resources available, such as terminals, printers, readers, storage devices, and communication lines which describe the number, type, characteristics, and attributes of these devices.
9. *Authorization tables.* These are the data which relate users to the processes they can perform and to the specific data they can access as well as relating certain restricted devices to the central processing unit.

Authorization Table Concept

The authorization table (exhibit A) depicts the relationship between users, the method used to communicate with EDP systems, the processes performed, and the enterprise data accessed.

Exhibit A attempts to highlight what could be considered typical relationships common to most business enterprises. For example, it shows that management would normally just be interested in scanning the transaction and historical data. On the other hand, application programmers would want to communicate with the EDP system in any of the three modes, but should have the capability to both scan and modify only the data related to application programs.

The system programmer would also be able to communicate with the EDP system in any of the three modes but would be restricted to systems data, such as the operating system programs or COBOL language compiler programs. The auditor, on the other hand, would be able to communicate with the system in any of the three modes and be allowed to scan the entire data base but would not be able to modify or change any of the data elements except those that were specifically related to audit programs.

EXHIBIT A

AUTHORIZATION TABLE

	Authorized to Communicate by			Authorized Processing		Authorized Information to be Accessed								
Users	**Batch**	**Data Entry**	**Inter-active**	**Read**	**Update**	**Transaction Data**	**History Data**	**Decision Criteria**	**Application Software**	**General Systems Software**	**Systems Control Software**	**Audit Software**	**Systems Resource Data**	**Authorization Control Tables**
Management	X	X	X	X	X	X	X	X						
Operations	X	X		X	X	X	X						X	
Auditor	X	X	X	X		X	X	X	X	X	X	X	X	X
Application programmer	X		X	X	X				X					
Systems programmer	X		X	X	X					X			X	
EDP control	X	X	X	X	X						X			X
Computer operators			X	X						X			X	

APPENDIX 3

Suggested Procedures for Auditors to Follow During Systems Design

This appendix includes some suggested procedures that might be followed by an auditor in reviewing the systems design stage of an EDP system and contains subsequent procedures that could be followed for reviewing and evaluating accounting controls once such a system becomes operational.

While a rėview of systems design is considered to be an important factor in furthering the implementation of adequate internal accounting controls in significant financial EDP applications, it is not a requirement. The absence of such a review would not preclude the auditor from rendering an opinion on the financial statements. A particular system might incorporate other user-oriented controls that would obviate the need for controls that might have been recommended if the auditor had reviewed the application during its design and implementation.

Auditor Participation in Systems Design. The general steps that an auditor might take during the systems design stage of an advanced EDP system are outlined below.

1. Review the objectives of the proposed system and the overall approach taken to achieve those objectives.

2. Determine the impact that the system will have on the financial statements and whether errors in the system might have a material effect on those statements. (See Statement on Auditing Standards No. 1 (New York: AICPA, 1972), Secs. 320.28 and 320.65.)

3. Review the prescribed practices and standards for documenting the system. The documentation should be completed in a timely manner, approved by management at each stage of system development, and should contain, among other things, clear descriptions of the accounting controls and information flow through the system.

4. Determine the control philosophy to be followed in the system, for example, which controls are the basic responsibility of the user vis-à-vis the data processing department, and the principal input, processing, and output control procedures to be followed. Potential weaknesses should be identified and additional controls suggested.

A. Since advantages of advanced systems will lie in the immediacy of processing, it might be tempting to eliminate some traditional supporting operations, such as hard-copy documentations of input.

B. Advanced EDP systems will be larger and more complex, linking the many interrelationships between segments of a business. This creates the need for more stringent controls on input and the operation of the system, especially editing and validating as part of the initial entry process.

C. In those advanced EDP systems that have remote processing capabilities there should be adequate distinction between update and systems that only provide inquiry. The following controls may be implemented:

- Inquiry system controls should emphasize identifying users and the data they are authorized to access.
- Update system controls, in addition to the above control, should concentrate on the verification and editing of input since most advanced systems will use destructive update techniques on direct access devices that process one transaction and update one master record at a time. Destructive updating requires periodic copies of master and transaction files for reconstruction if the current master is lost.

5. Identify the audit trails in the system. Audit trails should provide evidence that principal control procedures are functioning, or that no errors were encountered, and evidence as to how transactions were processed. The availability of this information will significantly affect the audit approach to be used. In real time systems the audit trail should provide feedback at the terminal location and at the central computer identifying—

Users
System used
Information sent and/or received
Time of entry and/or processing
Place of entry and/or processing
Error messages

6. Determine the nature of the audit evidence that will be available to support

transactions processed. Consider the reliability and acceptability of this evidence, particularly if it is system generated. The availability of independent corroborative evidence should also be considered; for example, can significant transactions be independently confirmed?

Many installations maintain a log of all transactions accepted by the system. Such a log is usually maintained in the order of acceptance of transactions and contains all the detail necessary for complete reprocessing of the transactions in the event of data loss or equipment failure.

In those instances where the system generates a transaction, as in the automatic reorder function in an inventory control system, it is important that the system document the existence of that machine-generated transaction by producing some hard-copy memorandum that can be verified by an independent check of the activity.

7. Review the programming and testing practices to be followed. These can significantly affect the effectiveness of the control in the system. Consider whether the users will conduct tests of the system and whether audit testing before the system becomes operational would be appropriate.

In addition to testing all the alternate processing paths that can exist in an ordinary program, live data tests should be considered. All of the interrelationships, terminal polling, message queuing, and program selection that should exist to accommodate an advanced system application should be tested along with the processing.

8. The auditor should review the proposed procedures and controls during the conversion of the existing system. The lack of adequate controls during conversion could result in the failure to detect significant errors.

Examples of errors that could occur during the conversion process are—

A. Complete or partial deletion of a file.

B. Introduction of erroneous data, such as incorrect identifying numbers or incorrect amounts.

C. Incorrect processing or summarization of data if programs have not been adequately paralleled and compared with similar information procession by previously adequate systems.

9. Consider various audit approaches including procedures for reviewing, testing, and evaluating the accounting controls and procedures for substantive testing of the results of processing. Determine the nature of any special programming required for audit purposes under each approach. Select an approach that provides for effective audit testing at a reasonable cost. The auditor's examination of systems documentation can be used to develop a preliminary opinion as to the adequacy of procedures and to provide an indication to the auditor of those controls whose existence should be verified and whose effectiveness should be evaluated.

The auditor should check on the progress of the system through the design, programming, testing, conversion, and operational stages to assure that changes do not adversely affect the effectiveness of controls or the audit approach.

Monitoring client operations over a period of time is another technique for observing and subsequently evaluating actual systems performance, although it provides no evidence regarding those controls or procedures that are not called upon during the particular period under observation.

Subsequent Review of Accounting Controls. Once a system has become operational the auditor should evaluate the actual effectiveness of the accounting controls in the system. This evaluation should be repeated during each audit of an advanced system, at a minimum annually, or at more frequent intervals if warranted.

APPENDIX 4

Glossary

Application programmer is a person who is authorized to code and maintain applications programs such as accounts payable, inventory control, financial reporting programs, and so forth.

Auditability determines the characteristics of a system that permit data to be reviewed for validity and accuracy, and that permit controls to be tested for integrity and reliability. These characteristics are important in obtaining assurance that the following conditions have been accomplished:

1. Uniform handling of all data has been performed as authorized.
2. Data has been completely and correctly processed.
3. Data has been recorded in a manner that allows it to be traced from origination, through subsequent processing, to ultimate disposition—and in the opposite direction.

Auditor's computer is a specially designed computer having the capability of interfacing with other computers to test the propriety and integrity of their software and file structures. It has the ability to perform various other audit functions on an independent basis from the computer system being audited.

Audit control is the means for obtaining assurance regarding the integrity of audit testing in circumstances in which the auditor places reliance on certain client programs, such as operating systems, data base management systems, and so forth, in order to perform such testing.

Audit hooks are the capabilities incorporated into the hardware, systems software, and applications software that will allow auditor developed software or testing criteria to be fully integrated into normal processing activities. Audit hooks would provide auditors with the capability to capture any transaction being processed by the system and take whatever action is required.

Audit trail is a means for identifying the actions taken in processing input data or in preparing an output such that data on a source document can be traced forward to an output, for example, a report, and an output can be traced back to the source items from which it is derived. Note that the audit trail can also be termed an inquiry or a management trail because it is used as a reference trail for internal operations and management as well as for audit tests.

Computer audit software is generalized software developed or used by an auditor for file interrogation, performance of arithmetic calculations, and development of reports. Currently, such software is normally limited to accessing files with standard sequential or indexed sequential structures.

Data base is a collection of data items related to all or only a portion of enterprise activity. Today, the term implies a structured collection of data items that are related to an enterprise's operations, such as the financial data base, a customer data base, or similar operation.

Data base management system (DBMS) is a set of integrated software routines developed to create, maintain, and allow access to an organized and structured collection of related data items. The DBMS handles the mechanics of storing, updating, and accessing the data, thereby allowing the application programmer to view a logical collection of data elements as a file and reducing the programmer's concern with the physical form or structure of these data items.

Data base administrator is the individual authorized to define the rules which govern and control access of data and the method of physical storage of the data. The function is handled via a descriptive data base language which performs the following:

1. Defines and describes the data.
2. Defines the logical relationship and interrelationship of the various segments of data.
3. Defines the physical storage of the data and its attributes.
4. Defines and describes the logical view of the data as it may be seen by the application programmer and the interrelationship of the logical views to the data structure.
5. Defines the security measures applicable to each user and to the data base.

Data communications pertains to the transmission of data over distances, such as by telegraph, telephone, radio, directly to electronic data processing devices.

Data dictionary/directory is a structured collection of information elements that define and describe the data elements associated with one or more data bases. Ideally, the dictionary/directory defines each data base and describes its attributes related to identification, representation, relationship, security, integrity, and so forth.

Distributed systems include two or more computers physically separated, but linked together with a communication network that allows any site to utilize the resources within the network. For example, a small computer at a plant site could use the power of a larger computer in the network to manipulate and solve a linear program alogorithm related to plant scheduling.

Integrated test facility (ITF) is a means of introducing dummy data into a live application system to see whether it is properly handled. The data is introduced as though it were live data and must be removed at some point during the application's operation.

Internal control in a broad sense has two elements.

1. *Administrative control* includes, but is not limited to, the plan of organization and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions.[1] Such authorization is a management function directly associated with the responsibility for achieving the objectives of the organization and is the starting point for establishing accounting control of transactions.
2. *Accounting control* comprises the plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that:
   a. Transactions are executed in accordance with management's general or specific authorization.
   b. Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and (2) to maintain accountability for assets.
   c. Access to assets is permitted only in accordance with management's authorization.
   d. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

The foregoing definitions are not necessarily mutually exclusive because some of the procedures and records comprehended in accounting control may also be involved in administrative control.

Microfiche is a technique which compacts information for dense storage and uses the latest in microfilm, magnetic encoding, and visual screen technology for referencing and display access.

Operating system is an organized collection of programmed routines and procedures for operating a computer. These routines and procedures normally perform some or all of the following functions: (1) scheduling, loading, intitiating, and supervising the execution of programs; (2) allocating storage, input/output units, and other facilities of the computer system; (3) initiating and controlling input/output operations; (4) handling errors and restarts; (5) coordinating communications between the human operator and the computer system; (6) maintaining a log of systems operations; and (7) controlling operations in a multiprogramming, multiprocessing, or time sharing mode. Among the facilities frequently included within an operating system are an executive routine, a scheduler, input/output routines, utility routines, and monitor routines.

System administrator is an employee responsible for ensuring that information processing services are consistent with the needs of the organization and that the integrity, security, and auditability of the system meets corporate standards.

System programmer is a programmer responsible for implementing upgrades to operating systems and other general systems software and maintaining revisions or modifications to such systems.

[1] This definition is intended only to provide a point of departure for distinguishing accounting control and, consequently, is not necessarily definitive for other purposes.