1-1-1972

Computer controls and audit, management summary edition

Touche Ross & Co.

COMPUTER CONTROLS AND AUDIT

MANAGEMENT SUMMARY EDITION

TOUCHE ROSS

COMPUTER CONTROLS AND AUDIT

Management Summary Edition

FIRST EDITION
SEPTEMBER 1973

TOUCHE ROSS

TOUCHE ROSS & CO., 1633 Broadway, New York, New York 10019

COMPUTER CONTROLS AND AUDIT

Management Summary Edition

PREFACE

The Computer Controls and Audit manual, originally issued in September 1972, has been extensively revised and is being reissued at this time. In conjunction with the reissuing of the manual, this non-technical, heavily abbreviated condensation of the full text has been prepared.

This "Management Summary Edition" is primarily intended for briefing purposes only. It is also to be used as introductory reading prior to Firm training programs on computer auditing. Performance of EDP audit activities should not be based on this summary alone.

A further word of *caution* – this summary does not attempt to inform the reader on how much test work should be performed in an audit of EDP. It also does not attempt to show where the audit of EDP fits into the framework of the complete financial statement audit. These are both judgmental areas. Normal audit judgment must be applied to the circumstances in each engagement to make these "how much" and "where" decisions.

This preface would not be complete without recognizing the extensive amount of work – much of it "trail blazing" areas that had not been covered to any degree before – that went into the full manual and summary, and the personnel who did that work, much of it in their "spare" time. Don Wood, Chicago Management Services Partner; Bill Mair, Detroit Audit Manager; and Keagle Davis, National Accounting and Auditing Staff Partner and Director of Computer Auditing were instrumental in preparing this work. They received significant assistance from various personnel, including Richard Webb, National Accounting and Auditing Staff Audit Manager and Carl Pabst, Los Angeles Audit Manager.

National Accounting and Auditing Staff
September, 1973

Note: Use of this summary outside the Firm is permitted.

Printed in USA

COMPUTER CONTROLS AND AUDIT
Management Summary Edition of Volume 1
TABLE OF CONTENTS

Introduction

Notes to Readers . . . This "Introduction" is identical to the introduction to the full text. It is included here to give the reader a flavor of the overall content and intent of the full text.

The reader will additionally note that Sections I–IV (the overview and "control" sections) are more heavily condensed, i.e. they are briefer, than Section V, the "audit" section. There are two reasons for this. First, extensive use of charts which compactly cover much of the narrative allows heavier condensation in Sections II, III and IV. These charts and figures must be reviewed carefully if the reader is to obtain a proper level of familiarity with controls. Secondly, much has been written in the past on computer controls (although not in the format of this work). Therefore, many readers will already have some familiarity with controls. The audit section, however, contains a significant amount of new material, particularly on the areas of audit endeavors, the approaches to be taken and the tools and techniques to be used. Hence, there is a lesser degree of condensation in Section V to assure reader understanding.

WHAT THIS BOOK IS ABOUT

This book is about the control principles associated with and the development and audit of computerized information systems.

Controls, as the term is used in this book, include all of the computer equipment, programs, procedures, personnel, and forms necessary to assure that reliable results are realized from an information system.

The term "audit" refers to the activities associated with the examination of the computer-produced elements of an information system to establish reliability of financial, operating and management data. In the EDP area, the auditor's concern for reliability extends to:

- The processing of applications on computers
- The operation of the EDP installation
- The development of systems.

Computers represent change – but they do not change the logic of information processing.

In this book, methods of control over the processing of data and the development of information are treated primarily at a logical level. *Computers represent changes in technique, environment, and capacity, but they do not change the logic of information processing.* Therefore,

the methods described are designed both for application to currently implemented computer systems and for future systems of increased magnitude and capacity.

A basic thesis of this work is that control over information systems utilizing computers can best be achieved from a starting point which breaks the elements of control down to their lowest common denominators. In doing this, it becomes apparent that the underlying objectives, concepts, and responsibilities associated with control have undergone surprisingly little change in the transition of systems to computers. Thus, in approaching controls at their lowest common denominator, it is possible to maintain a structure of information system reliability, even in the face of continual changes.

In considering control as a fundamental requirement for both management and auditing, it is increasingly possible, in fact essential, to discuss the *logical* aspects of controls proportionately more than the *technical* aspects. This approach recognizes that the major control considerations associated with computer lie in:

- Integration and processing of files across organizational and geographic boundaries

- Centralizing of files and records necessary to a company's existence.

In the area of technical aspects of EDP systems, hardware malfunctions and controls once absorbed a major share of the attention. But these have receded in importance due both to increased reliability and to improved capabilities of hardware and support software features to detect and cope with processing problems without human intervention.

This book is written for the non-EDP technician – but its content is useful to all involved with EDP. Because nontechnical considerations are increasingly paramount, most of this book has been written to be useful to the reader with only limited background in data processing. The initial edition of this book was used in training auditors whose technical knowledge was limited to 50 hours of training in basic computer concepts and the generalized audit software system – STRATA[1].

[1] System by Touche Ross for Audit Technical Assistance – STRATA/360 is a Registered Trademark of Touche Ross & Co.

Discussions of computer system controls are equally appropriate for the manager, the information user, the systems analyst, the data processing operations supervisor, and auditors with similar background. Content of this book is intended to provide both the conceptual and detailed information necessary for controls over a broad range of applications under varying degrees of processing integration and complexity.

No attempt has been made to anticipate every set of controls which might be required for an application in each possible situation. Such an undertaking is both impractical and practically impossible. Control requirements and methods are environmental and highly individual in nature. Therefore, sufficient latitude has been provided so that the systems analyst and the auditor are unconstrained by "cook book" directions for control methodology. The analyst and the auditor must have the responsibility and the judgment to apply the appropriate techniques applicable in individual situations.

The increasing role of systems standards and documentation is also covered in depth.[2] Documented standards are considered an essential for full utilization and control of EDP systems and are not an optional frill.

APPLICATIONS FIRST – THEY'RE MORE FAMILIAR

This approach taken to describe EDP control and audit considerations differs from previous works in this field. Earlier writings tended to begin with discussions of system development and technical computer considerations. They then went on to discuss operation of the computer facility and to treat control and audit of applications last.

Experience has shown, however, that the typical audit career path first encounters EDP control considerations in reverse of this order. The average auditor, on early assignments in his career, will deal primarily with the control and audit of applications. Later, as he gains experience, he will approach EDP control and audit from an overall installation standpoint. During that portion of the job, he will normally select the applications to be reviewed and will assign them to other, less experienced personnel.

Because this is the typical career path, this book stresses applications as a starting point for control and audit consideration. This is brought

[2] Much of the information in this area has been taken from two books in the Touche Ross & Co. Management Series: *Managing the EDP Function,* by Arnold E. Ditri, John C. Shaw, and William Atkins (McGraw-Hill, 1971), and *Managing Computer System Projects,* by John C. Shaw and William Atkins (McGraw-Hill, 1970).

out *in the first, introductory section written at a nontechnical, overview level for the benefit of managers or auditors with no previous EDP experience. Then, succeeding sections move from the specific to the general:*

- Section II deals with the control and audit of applications
- Section III assumes that a familiarity with applications serves as the basis for involvement in the control and audit of facilities (computer operations centers)
- Section IV deals with the system development process and accompanying management, control, and audit considerations
- Section V deals with the impact of EDP on and the planning of and structure of an independent audit engagement involving the computer.

ORGANIZATION AND CONTENT – PRACTICAL AND EDUCATIONAL

The content of this book is both practical and educational. Because it begins from a familiar application base and moves to the more technical and involved aspects of EDP control and auditing, any reader with an interest in information systems can follow the content as far as his interests and responsibilities require.

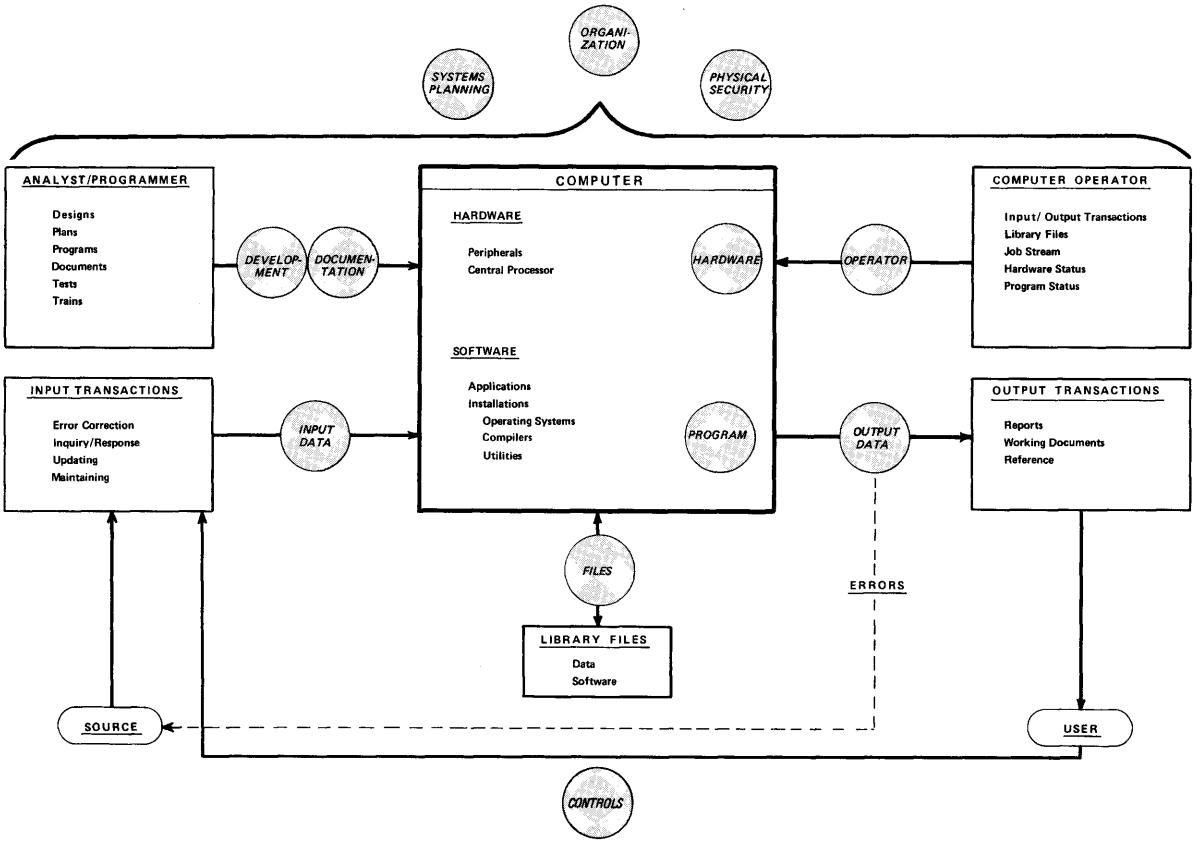
Organization and content have been designed for a wide range of readers, including:

- Independent auditors
- Internal auditors
- Financial management
- General corporate management
- EDP management and EDP systems analysts
- College students in auditing and business data processing.

STRUCTURE OF CONTROLS FOR EDP – A PREVIEW OF THE CONTENT OF THIS BOOK

To give the reader a preview of the content of this book, the structure of controls for an EDP installations and systems has been summarized in the figure across the page. The figure shows that in any EDP environment, there are:

A STRUCTURE OF CONTROLS FOR EDP SYSTEMS



- Areas, activities, and items to be controlled

- Specific responsibilities assigned to each area, activity, or item to be controlled

- A variety of individual types of controls which must exist and must be examined collectively as each area is affected by the others.

Broadly speaking, any entity utilizing EDP is usually organized into three general areas:

- *Installation/Operations* — The actual computer room including the CPU and all peripheral equipment (hardware), the programs that control the functioning of the hardware and application programs (installation software), the computer operating personnel, the EDP library, and security over it all

- *Applications* — The business system which EDP is "applied" to, e.g., billings, payables, payroll, etc.

- *Systems development* — The activities of the systems analysts, and programmers in planning and developing the systems which meet user requirements.

Within each area there are a variety of specific responsibilities, activities, items, etc., which are subject to control. The extent and nature of the control procedures will vary among EDP installations depending upon:

- The size of the installation

- The complexity of operations

- The relative cost of control vs. the risk or exposure to loss

- The level of control or checking exercised at the source of and by the users of data

- The extent to which compensating controls have been built into the system.

Proper control of an EDP system is the mutual responsibility of the data source and user areas and EDP personnel. Abrogating that responsibility in any way by any of those parties is the first step to an unwieldy, uncontrolled environment in which a company's information

resources can quickly deteriorate to an unusable state – or be lost entirely.

The auditor of an EDP system must first, as in any situation, get to know his client and his client's system in depth. Understanding and the ability to independently evaluate a system can come only from knowledge of the system. The auditor can and should be able to approach a review of EDP controls at a very logical, as opposed to a technical level – with a full bag of audit tools and techniques available to assist him in the review. When completed, a well thought-out and constructive computer control review will lead to a better understanding of and communication with the client – benefiting all parties – auditors, users, EDP personnel, and finally, company management.

THERE IS NO SUCH THING AS "AN AUDIT TRAIL" – THERE IS ONLY A "MANAGEMENT TRAIL"

To conclude this Introduction, and to further set the tone for the remainder of the book, we will attempt to destroy a phrase or philosophy that is often deeply imbedded in the minds of management and data processing personnel. The "audit trail" as it has been called for the past decade or more is a highly misunderstood phrase. It implies that the sole function of certain aspects, of computer systems and application design is only to service auditors needs. Not so! If anything, the requirements for adequate documentation of and controls in computer applications are *management requirements* – to permit verification of reliable processing by managers of user departments and to prevent erroneous processing – and allow correction of errors when errors do occur. The lack of hard copy output does not destroy an "audit trail" because today's generation of generalized audit software permits the auditor to extract information at will from machine readible media. The needs for controls in a system, and hardcopy at various stages of processing for the purposes cited above, are management needs – not audit needs.

SECTION I - OVERVIEW

PROBLEMS OF EDP CONTROL

The computer has been actively used for financial and operating applications in most medium-sized companies since the early sixties, and in many of the largest companies since the late fifties. Only in the last few years, however, have changes occurred which require an intensive review and reorganization of controls for computerized business systems.

Mechanization itself is not the major factor requiring this increased attention to controls; instead, the more extensive systems skills developed over two decades has made this necessary. Only recently have these skills started changing the basic logic of how data are acquired, purified, concentrated, and used in decision making in systems — systems which cross geographic and organizational barriers.

The primary effects of this "extending of systems" are twofold:

1. Redundancies have been eliminated in the entry and storage of data. This resulted in many users losing the "feel" for the quality of the data with which they were once intimately associated — and now seen only in remotely produced computer outputs. Conversely, persons who provide an efficient single source for data they do not use directly are less aware of control implications than they formerly were.

2. Concentration of data increasingly facilitates the interrelation of files, as well as the computerization of operational decision rules. This, in turn, results in the automatic initiation of chain-related actions and transactions Previous methods for manual approvals are replaced by pre-authorization through the logic implanted in computer application programs.

The increase in sophistication experienced in systems skills can be expected to continue. Consequently, what is called for is a corresponding sophistication in understanding control techniques and points at which controls are applied in order to maintain control over the processing logic, as well as to provide security for the increasing concentration of data and processing facilities. These information assets are becoming *essential* to the operation of the company. Safeguarding these assets, therefore, may be more important than that of negotiable assets around which the tradition of effective controls has grown.

Control Responsibilities

Responsibilities for control of information assets must be assumed jointly by system users, the EDP department, and the auditor.

The user should conduct himself as a prudent businessman who has subcontracted for the processing of his data and logic. He must specify the thought processes and controls to be applied, satisfy himself that they have been implemented within the system, and monitor results for quality.

EDP people have dual responsibilities. They must develop and apply custodial controls for the physical security of the information assets entrusted to them. And they must serve as prime contractor or coordinator for the development of manual and EDP controls over the processing of information.

The auditor's basic financial examination responsibilities have not changed. However, the auditor is responsible for modifying his methods to assure effective, efficient examinations in a changing environment.

In addition to responsibilities for financial examinations, the auditor – and particularly the internal auditor – is held responsible increasingly for providing assurance that operational information is controlled and used effectively. Operating in this new dimension, the auditor will use the power of the computer to meet his expanding obligations.

AUDITING EDP SYSTEMS - AN OVERVIEW

EDP presents both threats and opportunities to the auditor.

Threats stem largely from the rate of change in EDP systems. Changes of audit significance occur at an accelerating rate and are of greater magnitude than changes previously experienced. Corresponding computer-associated audit opportunities include:

- The increasing number of data concentration locations convenient to the auditor.

- The increase in audit understanding gained in the use of properly documented logic requisite to computerized systems.

- The speed and capacity of computers as promising audit tools.

Audit Planning

In all areas of an audit touched by a computer, the auditor should go through a thorough rethinking of audit scope and objectives. Areas of prospective change include:

- Audit Programs and Work Plans
  To best satisfy audit scope and objectives, audit planning calls for re-evaluation of audit techniques for selection of methods most

appropriate to computerized systems. Audit programs may be subject to anywhere from minor to total revision in sections related to systems which have been computerized.

- Around or Through the Computer
  The auditor may use the computer as a tool in his examination, or, if adequate documentation and control exists, he may audit around the computer. If there is a choice, he should evaluate alternatives in terms of cost and effectiveness and decide on the basis of comparison. If this comparison results in a tie, the auditor is well advised to decide in favor of the computer. The next time it may not be a tie, and each experience builds his EDP auditing capability.

- Timing
  Where a computer is used, the auditor may have to adjust the timing of his examination activities to conform to EDP schedules. The specific computer files to be used may exist only at a given point in time. In many cases, it may be necessary for the auditor to plan his examination to conform to these availabilities.

- Location
  With the concentration of processing and files in computer centers, a portion of examination activities may also shift to a centralized location. The auditor may find he can perform a more thorough examination of a greater number of files and procedures centrally through the computer. Remote examination procedures will continue to be necessary for verification of authorizations, data entry procedures, and physical assets.

Segmentation of the EDP Audit

In an EDP environment, the auditor should segment his work into manageable, do-able steps, including:

- Auditing individual applications processed on computers.

- Auditing activities and reliability of procedures in the computer installations center.

- Review of and participation in the system development activities of the company to assure the quality of controls built into new EDP systems.

These three segments of the EDP audit activity relate to each other logically in the training and experience pattern of the typical auditor. The audit of applications closely resembles the procedures familiar in conventional audit activities, and thus, is a preferable starting point for one who is new to EDP auditing.

The control of applications, however, must include in a single sweep the control of both the manual and computerized application activities. This is due to the increasing interdependence between the two areas of activities. As described in the full text, the manual entry of a single transaction may automatically impact in a chain-related fashion a series of computer activities, without manual intervention.

The EDP familiarity gained in studies of applications leads naturally to work on review and control of the more technical activities in computer centers.

Audit participation in system management then becomes the next, most-sophisticated level of activity. This involves review and assistance in the planning of new systems to assure inclusion of adequate controls.

Levels of Audit Activity

Within each of these segments of EDP audits, three different levels, or scopes, of audit concern exist:

- Controls,
- Procedures adherence, and
- Operational auditing

Controls and procedures adherence are conventional audit concerns. Operational auditing through EDP represents a particular opportunity for the professional auditor. Operational auditing opportunities should not be limited to EDP operations themselves. Rather – and perhaps more important – they extend to the data and logic processed by EDP on behalf of users.

Impact of EDP on Auditors

AICPA Statement on Auditing Standards #1 requires the auditor to test those controls he intends to rely on to produce accurate financial data. Very often, EDP installations and applications encompass internal controls of this nature.

As EDP techniques become increasingly important in the processing of financial and operating data, the auditor will have to develop bilingual skills – that is, conversational capability covering EDP, adding to his more thorough expertise in auditing.

The trend toward incorporating EDP techniques in audit procedures can be expected to accelerate. This will be due both to the threats and opportunities presented by changes in systems and to pressures exerted as more persons enter the profession with college training in business data processing. Young auditors familiar with computer capabilities will be reticent to adhere to older and perhaps more tedious ways.

CONCEPTS OF INFORMATION SYSTEM CONTROLS

Within EDP systems as elsewhere, controls are applied to assure the accuracy and reliability of results of processing. Control objectives include:

- Complete and accurate processing of all authorized data, including prevention, detection, and correction of errors
- Continuous operating capability
- Prevention and detection of misuse of equipment and data
- Development of effective, efficient, and maintainable systems.

Computers do not alter the basic concepts or objectives of systems controls for information users. However, techniques and points of control must be adapted to the changing conditions and responsibilities of an EDP environment. For the most part, these changes deal with relocation of operational and control points, and with the concentration of information assets.

The first requirement for the development of appropriate controls in an EDP system is a common understanding by all parties – user, systems analyst, management, and auditor – of the basic structure of both manual and computer processing activities, as well as of the concepts and needs for controls and of the applicable control techniques. This understanding must be reached first on a non-technical, user level.

Logical and Technical Controls

Two general levels of control can be recognized within a computerized system - logical and technical. The distinction between these two levels is chiefly in their respective degrees of complexity.

Logical controls are those applied for the specific application or function performed and fall within the normal comprehension level and responsibilities of the user or auditor. Logical controls can be applied either by people or computers.

Technical controls, on the other hand, are those applied by hardware or software independently of application logic. These controls require a technical background for comprehension, design, and implementation. In the early days of EDP, technical-type controls were of predominant concern. Today, however, many of the problems have been resolved or reduced. Technical controls *are* still important, but there is generally little need for the user or the average auditor to become heavily involved with computers on a highly technical level.

Preventive vs. Detective Controls

Since it is neither practical nor feasible to prevent the entry of all errors into an information system, techniques are necessary for recognizing and dealing with those which are created. Both preventive and detective controls are necessary within EDP systems.

Preventive controls are designed to prevent errors or unauthorized transactions from occurring.

Detective controls are designed to:

- Detect errors
- Locate the causes of errors
- Assist in correcting errors
- Identify points where future errors can be minimized thru system changes, personnel training or preventive controls.

Activities Subject to Control

Information processing activities, both manual and automated, which are subject to control considerations include:

- Initiation of transactions
- Coding of entries
- Recording of data
- Processing logic
- Data storage and movement
- Output distribution

(These activities are referred to in subsequent sections and illustrations.)

The Cost/Risk Equation

Each control applied to an EDP system has a cost. Obviously, no control should cost more than the consequences of the conditions it is designed to prevent or detect.

To the extent that controls are poorly designed or excessive, they become burdensome and are under threat of being ignored. Applying

controls as early in the processing cycle as feasible minimizes the number of control points required, the damage which can be done to files, and the need for corrective efforts.

Both the cost of controls and the feasibility with which they are accepted can be enhanced if they are designed for operational interests. Counts and values of transactions, files and in-process items, for example, can serve valuable operational as well as control functions.

Structure of Controls

If a system is to be controlled effectively and economically, the control process itself has to be brought under a manageable structure. Succeeding sections will deal with these structural elements of systems controls:

- *Application controls* are those unique to individual user systems.
- *Installation controls* apply to a computer installation and how most or all applications are processed through the data processing center.
- *Systems management controls* are intended to assure that the planning, development and operation of EDP systems, are themselves performed in a systematic manner.

ROLE OF SYSTEMS STANDARDS

A standard is a statement of "the way we do things around here." Information systems standards as used in this text are procedures, documents and benchmarks which together describe how the systems development activity is performed and how the resulting system is operated. Standards apply to both manual and machine activities.

Increased development and use of formal standards represents a favorable trend in EDP management and control — a necessity for keeping up with the increasing capacities, costs, and risks associated with EDP systems. For the auditor, standards represent both aids in examination activities and norms against which to compare operations and to report deviations.

In general, systems standards do three things: they provide direction, documentation, and measurement.

Direction. Standards are drawn at three levels; instructions, guidelines, and policies. Instructions provide specific direction for repetitive, high volume, clerically-oriented activities. Guidelines describe generally how a job should be done but leave a degree of

judgment to the discretion of the person doing the work. Policies provide room for still-higher levels of judgment.

Documentation. Standards serve two primary purposes: communication and the recording of accomplishments. Documentation of systems development provides a basis for establishing and communicating agreements between the user and the EDP systems analyst on what is to be done, who is to do it, and why. Documentation also records accomplishments and serves as a primary basis for quality control reviews and for effective maintenance and continuity of the system.

Measurement. Standards are applied to describe performance objectives and to measure results.

Application and Installation Standards

Comprehensive, detailed standards are important in two areas of an EDP operations environment – individual applications implemented on computers, and for the computer installation.

Application standards cover every activity involving clerical or computer processing of user data and logic through the entire cycle of an operational system. They are primarily in non-technical terms.

Installation standards should be expected to cover those functions which apply to most or all applications processed in an EDP installation. Installation standards include elements that are both technical and non-technical in nature. The user or auditor may require assistance from a specialist when it becomes necessary to evaluate and test technical installation standards.

Systems Management Standards

These standards apply to the planning and the development of EDP systems. They are primarily at the guideline and policy levels. The characteristics of planning and development work which lend themselves to guideline and policy standards are a moderate degree of repetition of the work performed, and the increasing importance of efficient, predictable results from these activities. The auditor is becoming increasingly involved in systems management, i.e. the application development process, due to the impact it has on controls and on providing appropriate documentation for efficient audits.

Standards as a Basis for Auditing

The availability of formal system standards improves the process of understanding, testing, and evaluating system reliability.

In any audit engagement involving computerized systems on which the auditor intends to rely, the auditor should begin with a review of available standards and documentation. Their absence or inadequacy is cause for comment by the auditor and revision of the planned scope of substantive audit procedures.

SECTION II - CONTROL AND AUDIT OF APPLICATIONS

APPLICATION CONTROL RESPONSIBILITIES

One of the obvious requisites for control lies in fixing responsibilities for all persons and departments initiating, processing, or using data. Four separate areas of control responsibility can be defined:

- User or source departments
- System designers
- The EDP control group
- EDP operations.

User and source departments should maintain support controls to satisfy themselves on the quality of the data on which they rely. This is a responsibility that cannot be transferred to an EDP organization for other than the most trivial information.

System designers and project teams should assure that:

- A range of control alternatives is considered.
- Controls agreed upon by the user and EDP personnel are the most effective and economic for each individual application.
- Instructional procedures and training are prepared and used.

Particular emphasis should be given to explicit corrective and recovery actions to be taken in case of error or failure.

The EDP control group is responsible for maintaining accountability for all data which enter or leave the computer center. Specific responsibilities for control of input transactions include:

- Maintaining schedules and communication between EDP department and sources and users regarding the flow and accountability of data.
- Logging the flow of data through the EDP department and balancing of input to output.
- Detecting missing and duplicate batches.
- Verifying authorization for input batches.

The EDP operations group is responsible for performing the control activities specified – and only the action specified – during development of the system. These activities consist primarily of handling of files, noting that appropriate balancing of files is being logged on the console by the software, preparing output for distribution, responding as prescribed to errors and failures, and recording all activities.

INPUT TRANSACTIONS

Input—the initiation, coding, and recording of data—has traditionally been the most significant area for application of controls to computer systems. If anything, this concentration on input controls can be expected to expand in the future. The more scattered and remote input points become from data processing facilities, both geographically and organizationally, the more structured input activities must be.

Although there are many variables of environment, procedures, and controls, input transactions can be divided, for the purposes of establishing or evaluating controls, into four general categories. Each category of transactions has associated characteristics and control concerns that influence the techniques and points of control that should be considered. These categories are summarized in Figure 2-1.

For convenience, selected techniques of input control, together with related processing activities subject to control have been highly condensed in Figure 2-2. See the full text for a more complete treatment of control techniques.

OUTPUT TRANSACTIONS

Output transactions are the results – the reasons for being – of data processing systems. Output controls are primarily detective in nature. Many relate directly to, and in some cases overlap, input controls. However, output controls have differences in points of occurrence and emphasis.

It is usually convenient to consider output transactions in four categories when establishing or evaluating controls over output. Each of these categories has its own associated characteristics and concerns. These are summarized in Figure 2-3.

Techniques for controlling output transactions are highly summarized in Figure 2-4, which indicates the processing activity each technique will assist in controlling. See the full text for a more complete treatment of control techniques.

TYPES OF TRANSACTIONS	CHARACTERISTICS	CONCERNS
UPDATE	Large volumes Chain related and processed from initial authorization Transaction value limited to one-time impact on files Routine and repetitive processing	Increasing concentration of processing Verifying initial authorization in transaction chains Completing the processing chain Authorization of adjustments and deviations Controls must be efficient
FILE MAINTENANCE	Limited volumes Restricted sources Permanent or semi-permanent impact on data files	Authorization is critical Timing of transactions affects content of processing cycle
INQUIRY	File reference only; no impact on file content May trigger subsequent decisions, transactions or inputs	Security of data in custody Accuracy of data displayed must be in keeping with the decisions to be made and actions to be taken
ERROR CORRECTION	Records have been entered and rejected previously Processing is more complex than for routine input transactions	Re-entry controls must be as stringent or more stringent than for original input Correction is more complex than original entry; error probability is higher with corrections Errors should be reviewed to determine causes for potential system improvement or user training

Figure 2-1 CHARACTERISTICS AND CONCERNS FOR INPUT TRANSACTIONS

INPUT CONTROL TECHNIQUES	ACTIVITIES SUBJECT TO CONTROL			
	INITIATE	CODE	RECORD	MOVE
APPROVALS				
SIGNATURES	X	X	X	X
STATION CODES	X			
FORMS DESIGN				
TURN AROUND DOCUMENT	X	X	X	
PREPRINT		X	X	
LAYOUT		X	X	
INSTRUCTIONS		X		
PRENUMBER	X			
VERIFICATION				
REDUNDANT INPUT			X	
MECHANICAL			X	
CHECK DIGIT		X	X	
VISUAL	X	X	X	
BATCHING				
BATCH CONTROL TOTALS		X	X	
BATCH SERIAL CONTROL	X			X
BATCH ANTICIPATION/SCHEDULING				X
BALANCING INPUT TO OUTPUT				
USER	X	X	X	
EDP CONTROL GROUP	X	X	X	
APPLICATIONS PROGRAM	X	X	X	
PROCEDURES MANUAL	X	X	X	X
DIVISION OF DUTIES	X			
ON-LINE INPUT WITH COMPUTER EDITING	X	X	X	

Figure 2-2 INPUT CONTROL TECHNIQUES AND THEIR RELATIONSHIP TO ACTIVITIES SUBJECT TO CONTROL

TYPES OF TRANSACTIONS	CHARACTERISTICS	CONCERNS
WORKING DOCUMENTS	Wide range of forms and uses; orders, invoices, shipping papers, checks, statements, etc. Large volumes Usually generated by or related to specific inputs Routine and repetitive in nature	Tradeoffs between effectiveness of control and efficiency of operations with large volumes
REPORTS	Limited volumes Primarily preplanned and repetitive Wide variation in uses of information and impact of company operations	Are content and timing of reports consistent with use of information and decisions to be made? Greater concern and control efforts should be applied to one-time or intermittent reports than to those issued regularly and frequently
REFERENCE DOCUMENTS	Periodically produced Voluminous, especially when whole files are "dumped" Increasingly being stored in micro-image format	Conscientiousness of production; reports should not be put off because they get little use Safe custody for reports in event they are needed for recovery Application of stipulated cutoff dates for report production
ERROR LISTING	Limited volumes Complex transactions requiring greater application of logic and judgment than other input transactions	Distributed to proper parties for corrective action Establish control to assure entry of corrections Experienced people should process because of complexities Learn reasons for errors and avoid recurrence where feasible through training or system modification

Figure 2-3 CHARACTERISTICS AND CONCERNS FOR OUTPUT TRANSACTIONS

OUTPUT CONTROL TECHNIQUES	INPUT - OUTPUT ACTIVITIES SUBJECT TO CONTROL					
	INITIATE	CODE	RECORD	PROCESS	MOVE	DISTRIBUTE
BALANCE TO INPUT CONTROLS	X	X	X	X	X	X
SCAN BEFORE DISTRIBUTION	X	X	X	X	X	X
VISUAL VERIFICATION AND APPROVAL OF SELECTED TYPE TRANSACTIONS	X	X	X	X	X	X
SUSPENSE FILE CONTROL OF ERRORS		X	X		X	
DISCREPANCY REPORTS	X	X	X	X	X	X

Figure 2-4 RELATIONSHIP OF OUTPUT CONTROL TECHNIQUES TO INPUT-OUTPUT ACTIVITIES

APPLICATION PROGRAMS

Controls exercised by computer application programs can be evaluated in four different categories – transaction edits, processing logic, files, and machine checks. Figure 2-5 defines these categories along with objectives for each.

Figures 2-6, 2-7, 2-8 and 2-9 outline the control technique for these categories. Again, the full text should be referred to for a more complete treatment of these techniques.

Controls over the programming effort itself are discussed in Section Four on Systems Management.

CONTROL	TYPES	OBJECTIVES
TRANSACTIONS	Applied to records or batches in a transitory state; prior to impacting files Sources: transaction batches entered through peripherals, on-line transactions, and transactions originated within computer	Isolate errors as soon as possible within processing cycle Identify points where errors or oversights occur as guide to corrective activities
PROCESSING LOGIC	Applied to logical functions performed by application on computer	Detect logical errors or oversights within programs Detect operator errors
FILES	Insure integrity of files in processing by monitoring absence or incompleteness of records, preventing processing of improper data, and identifying duplicate records presented for processing	Detect operator, librarian or programming errors
MACHINE CHECKS	Controls of same three type above, but applied by system software and hardware	Eliminate or identify malfunctions in hardware and installation software

Figure 2-5 TYPES OF APPLICATION PROGRAM CONTROLS AND THEIR OBJECTIVES

TRANSACTION CONTROLS	
TECHNIQUE	**FUNCTION**
EDIT ROUTINES	Transaction validation Balancing Reasonableness and limit checks Security checks
BATCH CONTROLS	Balancing Serial number checks
ERROR OUTPUT DOCUMENTS	Error reports Suspense file status reports Aging error suspense files Correction responsibility Suspense file size limitations Operations data reports

Figure 2-6 TECHNIQUES AND FUNCTIONS OF TRANSACTION CONTROLS WITHIN APPLICATION PROGRAMS

PROCESSING LOGIC CONTROLS	
TECHNIQUE	**FUNCTION**
LIMIT CHECKS	Checks for high or low balances
REDUNDANCY CHECKS	Checks summary level totals against controls for batches or source files

Figure 2-7 TECHNIQUES AND FUNCTIONS FOR PROCESSING LOGIC CONTROLS WITHIN APPLICATION PROGRAMS

FILE CONTROLS	
TECHNIQUE	**FUNCTION**
INSTALLATION SOFTWARE FILE CONTROLS	File identification File trailer totals Run-to-run balancing
APPLICATION PROGRAM FILE CONTROLS	File trailer totals Sequence checking File utilization measurement

Figure 2-8 TECHNIQUES AND FUNCTIONS FOR FILE CONTROLS WITHIN APPLICATION PROGRAMS

MACHINE CHECKS	
TECHNIQUE	**FUNCTION**
OVERFLOW CHECKS	Set flag on noting overflow condition Interrogate all overflow flags Apply control action specified in program
READ-AFTER-WRITE CHECKS	Apply to disc files at application program level Tradeoff is between control implementation time and possible cost of file reproduction

Figure 2-9 TECHNIQUES AND FUNCTIONS FOR MACHINE CHECKS WITHIN APPLICATION PROGRAMS

SECTION III - CONTROL AND AUDIT OF EDP INSTALLATIONS

EDP ORGANIZATIONAL CONTROLS

An EDP department is unique in its variety of functions, responsibilities, skills, and characteristics. It is useful to understand the wide range of EDP functional activities as a basis for discussions on how these activities can best be grouped organizationally for maximum operating effectiveness and internal accounting control. Major functions include:

- Operation and production (includes computer operations, data conversion, input-output controls, and report distribution)
- Project-type functions (includes feasibility studies, systems analysis, system design, programming, testing and conversions)
- Technical services functions (includes continuing analysis of hardware, software, systems technology, and quality control).

The characteristics and responsibilities of these three major functional areas are shown in Figure 3-1.

In addition to the line-type functions indicated above, and in Figure 3-1, the EDP department will also have conventional staff-type functions. The size and scope of these staff functions will be commensurate with the size and mission of the department itself.

EDP Organizational Structure

The organizational structure of a large EDP department is shown in Figure 3-2. A chart for the organization of a smaller EDP department is shown in Figure 3-3.

In both cases, the organizational arrangement results in operational effectiveness and satisfactory controls through the segregation of responsibilities for:

- Processing of data
- Accounting for and custody of transactions and library files
- Programming.

Within the larger organization, separate managers are assigned to these different functions. Within the smaller organization, some functions have been combined. Separation, however, is still maintained between programming, computer operations, library files and data control.

FUNCTIONAL GROUPINGS	FUNCTIONS INCLUDED	GROUP CHARACTERISTICS	RESPONSIBILITIES
EDP OPERATIONS	Operation of computer and related equipment Data conversion Library Control group	Highly repetitive workloads predictable and subject to scheduling Operations routine, require supervision Instructions necessary Operations subject to performance measurement Visible results for users Quality of controls quickly determinable	Achieve efficiency for group as a whole Maintain committed schedules High level of accuracy for data processed Maintain quality consciousness for group as a whole
PROJECT FUNCTIONS	Systems development Procedures and forms Quantitative analysis	Only nominally repetitive Long duration Projects with structured activities for visible interim results High level of interpersonal skills Numeric orientation (quantitative analysis) Systems analysis skills necessary	Understand objectives, responsibilities and functioning of user organization Improve effectiveness of user through application of EDP processing
TECHNICAL SERVICES FUNCTIONS	Equipment selection Software and operating system selection Program maintenance Quality assurance Programming	Highly technical Results may have low user visibility	Technical support to operating and project functions Improve efficiency and effectiveness of operating and project functions Development and maintenance of standards for computer operations Monitor compliance with standards

Figure 3-1 CHARACTERISTICS AND RESPONSIBILITIES OF EDP FUNCTIONS

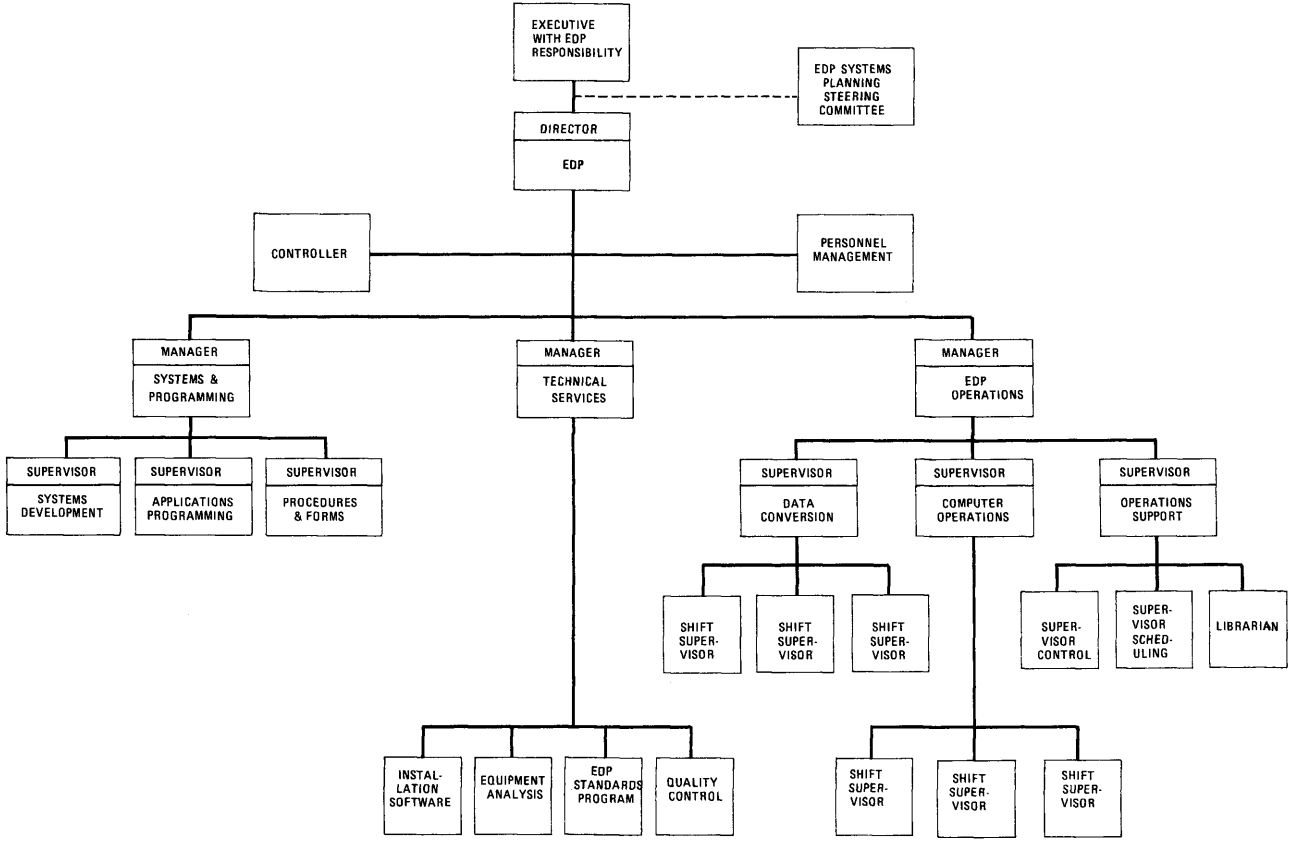


Figure 3-2 STRUCTURE OF A LARGE EDP ORGANIZATION

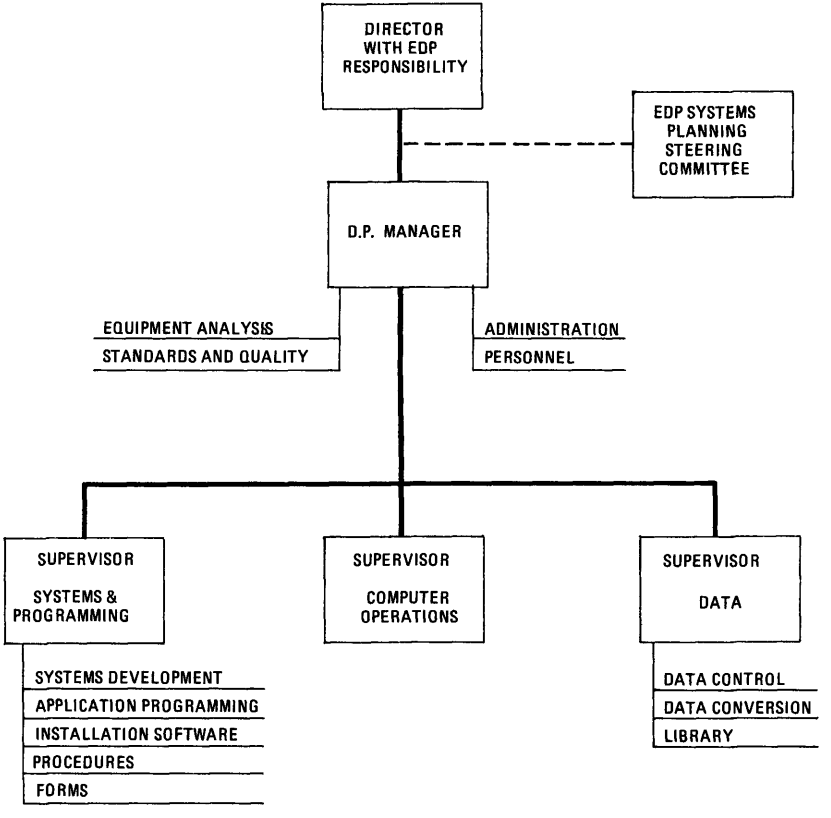


Figure 3-3 STRUCTURE OF A SMALL EDP ORGANIZATION

Operations Center Organization

The first control consideration normally associated with organization of a computer operations center is segregation of duties. Computer operators should be separated from:

- Accountability for and custody of computer files.
- Control of and accountability for transaction data.
- Programming and program documentation.

EDP Library Functions

Procedures and facilities within the library itself should include two types of preventive controls:

- There should be protection against improper use of files. Since files can only be used on a computer, this control is applied by retaining files in a secure library and restricting access to only authorized persons and only for scheduled, controlled utilization.
- The library is responsible for ensuring that control records are maintained for the files themselves. First, there should be records covering file content assuring that adequate backup files are maintained and available for emergencies. Second, there should be records covering recording media themselves – tape reels and disk packs. These records should monitor use of media for possible malfunction patterns as well as for maintenance and certification for use on a regular basis.

Control Group Functions

The control group has responsibility for control and balancing of transactions being processed by other groups within the computer operations center. The control also provides representation and accountability to users on behalf of the computer operations center. Controls applied by this group keep improper or unauthorized transactions from entering or leaving the operations center, and to identify and deal with errors initated within the computer center organization.

Programming

Programmers access to the computer should be restricted in order to limit or eliminate the opportunity for a knowledgeable person to make unauthorized changes to conputer records. The programmers responsibilities, however, include the development and maintenance of program logic, program coding, file record layouts and program testing. Programmers should also prepare detailed operating instructions including identification of all error situations, messages, and actions to be taken.

Control and Organizational Formality

Controls within an EDP department are as effective as the formal organization structure under which it operates, including documented:

- Policies
- Procedures
- Position descriptions
- Personnel evaluation

HARDWARE/SOFTWARE CONTROLS

Important controls within any EDP application fall within the capabilities available from equipment and installation software. Technical controls applied by hardware and installation software should be understood by the system designer and auditor and should be considered separate elements from those applied by applications controls in procedures and standards.

In large measure, the application of these technical controls results from an interaction of hardware and software. The detailed tasks and methods for applying these controls vary among vendors, computer models, and versions of software. It is more appropriate, therefore, to discuss the basic controls rather than how they are applied under all the various arrangements.

Computer Equipment

The terms equipment, hardware, and computer are frequently used interchangeably in describing EDP facilities. These terms, however, do have different shades of meaning:

Equipment and *hardware* are inclusive terms. They generally take in all working equipment within a computer facility, including items which are not part of the computer itself.

Computer, when the term is used specifically, applies to an interconnected group of equipment modules which function together for the processing of data. A computer includes a central processing unit (CPU) and a group of connected devices known generically as peripherals.

The CPU performs arithmetic, logic, and most control functions. Peripherals serve two general purposes: input/output (I/O) and data storage.

Installation Software

Installation software consists of the programmed routines designed to control and support the processing function of the computer for the execution of application programs. Installation software includes a number of elements:

- Operating systems which control the functioning of all elements of a computer configuration and application programs. Operating systems include facilities to perform much of the handling and control of application files, execute multiple applications or jobs concurrently in inter-leaved fashion, and provide protection capabilities to limit access to specified data or programs on the basis of appropriate "keys."

- Data management systems are specialized file management software for complex information structures or data bases.

- Software utilities are programs or sets of programs which provide commonly encountered data handling functions, such as sorting data, merging files, reading data from cards, reading data from tape, output to cards, output to tape, and others.

- Language translators, compilers, assemblers accept coding written by programmers and convert it to matching language for processing by the computer.

Control Objectives

There are four specific objectives of installation hardware and software controls:

- Detection of errors

- Prevention of unauthorized access to and use of data, programs, and equipment

- Recording of activities performed by the computer installation

- Supporting effective utilization of the computer.

Control Techniques

Both preventive and detective controls are applied within computer hardware and software.

Preventive controls are applied primarily by the manufacturer. They include:

- Design of equipment

- Thorough testing of computer modules
- Testing of configurations of equipment before they are put into use
- Extensive preventive maintenance programs
- Field replacement of potentially troublesome parts or components.

These preventive control techniques have resulted in high levels of hardware reliability.

In the preparation and distribution of software, preventive controls have tended to lag somewhat behind preventive efforts in hardware. The most significant control associated with software is recognizing that utilities can be used to modify files, and therefore, limiting exposure of files only for authorized uses.

Detective controls in both hardware and software have been refined to points where undetected processing errors are considered highly unlikely. An abbreviated list of detective control techniques includes:

- Redundant check bits to disclose errors in recording, reading, and transferring data
- Validity checks to insure that only valid characters are represented
- File data controls to provide positive identification of files and assurance that all records were made available to application programs for processing
- Access security controls based on classification of file data or devices and "keys" in accessing, software, hardware, and transactions
- Overflow checks to signal when data are lost through arithmetic operations that exceed the planned capacity of receiving fields or registers
- Diagnostics applied by maintenance organizations
- Console logs and utilization reports detailing and summarizing all operations performed by the computer.

COMPUTER CENTER OPERATIONS

Unsatisfactory control conditions encountered in computer operations centers frequently represent a carrying forward of the practices prevalent in the use of early generations of computers and predecessor punched card installations. During this time the computer operator provided the linkage for all elements of processing. In addition to running the computer, the operator usually handled most of the library functions and whatever balancing controls were performed, and often resolved and corrected errors in data and programs.

Facility for sharp improvements in operating controls generally came about following installation of third-generation computers and associated operating system capabilities when many of the repetitive, time-consuming tasks were built into software. Systems design changes have been made which combine to make for a more controllable environment in today's computer operations centers. These new conditions include:

- Programs are designed to run continuously. Errors no longer interrupt processing.
- The operator is no longer required, and should not be allowed, to make decisions on dispositions of errors or discrepancies.
- Error handling has undergone major changes. On most computers today, error reports are prepared for users, who make dispositions and enter corrections.
- Control techniques and disciplines have evolved which should replace prior practices in all installations.

Control Techniques

In addition to controls applied through EDP organization and by hardware and software, a number of other control techniques can be identified, including:

- Comparison of actual computer utilization with scheduled utilization and authorization of computer use
- Computer center supervision
- Security exercised over files by the library
- Rotation of jobs.

Utilization, Scheduling and Reporting.

Tight, effective scheduling and review of computer processing is a major technique for preventing unauthorized use of the computer. Scheduling procedures are built around the fact that computer utilization should be prescheduled and authorized. Even short-range schedule changes or additions of an emergency nature should be authorized by someone other than the operator.

Operations should be compared with schedules and variances understood. These comparisons would utilize console logs and computer utilization reports based on hardware or software recording devices or manually maintained records.

The level of detail in computer utilization reporting should include at least five categories:

- Test
- Rerun
- Assembly or compilation
- Maintenance
- Production.

Each category should be analyzed through breakdowns and comparisons of run times for similar jobs and with volume statistics. Special analysis should be made of rerun and maintenance times to understand causes and exposures.

Computer Center Supervision.

For control purposes, a supervisor is any individual to whom computer operators report. Supervisory responsibilities should include:

- Approving the computer operations schedule prior to each working shift.
- Monitoring actual operations for adherence to standard procedures.
- Approving the console log at the close of each shift.
- Reviewing computer utilization reports and describing variances daily while the facts are still fresh in his mind.

Library.

These controls were described earlier in the section on organization.

Job Rotation.

Job rotation is a standard control technique. At a minimum, job rotation should be practiced for vacations.

PHYSICAL SECURITY

Special security measures are necessary for any EDP facility where vital financial and operational data are processed and stored. Specifically, the areas of concern are:

- *Prevention of loss* – i.e., fireproof facilities, limited access, etc.
- *Protection to minimize loss when accidents occur* – i.e., duplicate files, duplicate processing center, etc.
- *Recovery from loss* – formal plan and contract to reconstruct data files, for use of alternative facilities, etc.
- *Insurance on loss and cost of recovery* – as with *any asset!*

Generally, the nature and extent of the particular security measures will depend on the nature of the facility – complex facilities would obviously require deeper security measures than simple facilities.

In order to secure against accidental and malicious causes of damage, preventive controls are needed. They can be divided into three major areas:

- *Responsibilities* – restriction of access, job descriptions, procedures manuals, etc.
- *Facilities*
  - Low profile should be sought for computer room, i.e., no large neon signs pointing to computer room
  - Few avenues of access
  - Keys to authorized personnel only
  - TV monitoring, etc.
- *Individuals*
  - Both employees and outside service personnel
  - Bonding, security checks

While no facility is *absolutely* secure from natural damage (fire, earthquake, etc.), care in planning is needed to minimize the risks of such damage occuring. Consequently, the facility should be located in as safe a location and facility as possible. In addition protective measures against disaster are needed. They can be classified into three categories:

- *Disaster detection* – i.e., early recognition of unauthorized entry or dangerous levels of heat, smoke, etc.

- *Secure storage* – selection of secure storage devices, i.e., fireproof safe or vault, keeping backup at remote locations, etc.

- *Extinguishing techniques* – automatic, gas or water. They are installed to protect and minimize damage to resources.

The key to the capability of an EDP installation to recover from damage or disaster is a proven, operational plan which provides for a range of losses from casual operator accidents to major disaster. This contingency plan should be:

- *Formal*
  - Fully documented
  - Activities and responsibilities of *all* personnel defined
- *Modular*
  - Should cover several levels of disruption
  - For each level (module), the plan should provide for recovery to predetermined operating levels
  - Set priorities
- *Tested*
  - Each element of the plans should be tested through some type of simulated emergency

In establishing priorities for protection and recovery plans data should be classified in terms of their critical nature. This would range from those which are *necessary* for continued operation, to those which are simply *useful* for operation. Media should be classified according to its susceptibility to damage. For example magnetic tapes and disks have narrower tolerances than paper or cards.

If damage or disaster does occur, of course, to such an extent that continued operation is no longer possible, the facility would be lacking in a proper backup facility. A backup facility is necessary so that it can take over during the recovery stage to whatever degree necessary.

An insurance program should exist to offset costs of recovery from disaster. Insurance costs should be evaluated in terms of the risks involved and the consequences of those risks.

In summary, an understanding of security requirements relates closely to an understanding of the flow of data. Given such an understanding, a person with normal business judgment can in many circumstances, evaluate an EDP security program. Such evaluations can be made at a logical level, without getting into the highly technical areas of security.

SECTION IV - SYSTEMS MANAGEMENT

SYSTEMS DEVELOPMENT

When computers first entered the business scene, system efforts carried a heavy technical emphasis. Management was minimal, and cost overruns abounded. Concentration was chiefly on the technical bottlenecks in system development - design, programming, and debugging.

Management of systems evolved gradually. System development was brought under a set of standards and a structure akin to project management techniques which had been applied successfully in management of engineering and other similar functions in industry.

Under these new techniques, management commitments are planned in advance but actually made only incrementally, with performance in each activity serving as a basis for continuing support of the succeeding efforts. The project concept applied to EDP systems has been referred to as one of "creeping commitment" by management. This process is illustrated in the table in Figure 4-1.

Systems Development Standards

Systems development standards apply to the structuring and documenting of the process of developing new computerized applications. Systems development standards have two major management implications:

- A standardized process has evolved for the development of new applications. This calls for a project structure with uniform activities performed in a consistent and measurable way. This structure can be used to understand and guide system development efforts, to assure application of controls, and to know where they fit in the process.

- Documentation standards provide a basis for both financial and operational control.

The System Development Structure

As indicated in Figure 4-1, a typical project structure involves a sequence of activities. Each activity within a project structure has specific scope, levels of detail, skill requirements, control considerations and documented results. These project elements and activities are displayed in table form in Figures 4-2a and 4-2b and 4-3a and 4-3b.

PROJECT ACTIVITY	Degree of Risk of Proceeding to Project Completion Without Further Checkpoints	Degree of Organizational Commitment to Project	Cumulative Expenditures
Initial Investigation	100%	0%	0%
Preliminary System Study	90	10	5
System Planning Study	75	25	15
System Requirements	50	50	25
System Specifications	40	60	30
Technical Requirements	30	70	35
Implementation Planning	20	80	40
Programming	15	85	70
User Training	15	85	75
System Test	10	90	80
Conversion	5	90	99
Post-Implementation Review	0	95	100
Ongoing Maintenance			

Figure 4-1 "THE CREEPING COMMITMENT"

SYSTEM PLANNING	SYSTEM REQUIREMENTS	SYSTEMS SPECIFICATIONS AND TECHNICAL REQUIREMENTS	IMPLEMENTATION PLANNING	PROGRAMMING
Scope and Purpose: Establish project scope, objectives, economics and feasibility – to level necessary for management decision on resources allocation and priority	Establish detailed specification of new system for the user viewpoint Confirm economics	Develop technical - level decisions and documentation Transition from business to technical solutions or problems	Review development progress Plan for balance of implementation of new system Re-assemble project team as working unit following technical planning	Prepare detailed logic, write coding, and test programs
Level of Detail: Depends on: Significance of costs and benefits Impact on other EDP operations Degree of technical stretch required Place in overall system development activity of company	Prepare full documentation of present and new system from user viewpoint	Final, detailed design and documentation for computer portions of new application Programs specified to module level for coding and control. Programming schedules developed.	Develop specific plans and schedules for: • Conversion • System test • User training Review and validate programming plan, revising as necessary	Deliver operating programs which have been tested and documented
Skills Required: Business and technical management participation – at senior level	Systems analysts User/business orientation	Almost entirely technical at supervisory level	Full range of project skills Management review and approval	Activity is entirely technical. Programming management and supervision sets up work modules for programmers
Control Consideration: Review control concept Carry System Planning Report forward for later review Limited audit effort	Requirements documentation serves as primary source for review of controls specified for new system	Controls imbedded in technical specifications Processing logic specifications include controls Control review frequently postponed to next activity	Major control review-point, since all controls have been specified for conversion and ongoing operation Review here guides audit participation and examination after implementation Audit test can be specific	

Figure 4-2a SYSTEMS DEVELOPMENT ACTIVITIES

USER TRAINING	SYSTEM TEST	CONVERSION	POST-IMPLEMENTATION REVIEW	ONGOING MAINTENANCE
Scope and Purpose: Performed concurrently with programming Users are trained to operate new system User manuals are prepared	Tests complete, integrated system Certifies readiness for use	Implement new system for ongoing use Achieve targeted benefits	Determine how well system met objectives Measure and evaluate benefits realized	Change system as necessary to meet external requirements or to enhance value
Level of Detail: Full user staff must be trained	Test: • Programs • Computer operations • User activities • Control group	Users take possession of system EDP operations and control personnel begin regular duties	Auditor and supervisory or management personnel participate	Generally carried out by EDP technical personnel
Skills Required: Users primarily Systems analysts support and monitor	Users perform final functions EDP personnel operate computer functions Systems analysts and programmers note and deal with exceptions	All user, systems analysis, and EDP operations personnel active	Management and supervision of user, EDP and audit	User supervision and EDP technical personnel
Control Consideration: Control reviews of: Procedures manuals Functional job descriptions	Control interests: Test results Documentation and handling of exceptions Approvals	File conversion control documents Initial operating reports on new system Operating approval or "buyoffs"	Operational audit?	Assure continuing control and documentation

Figure 4-2b SYSTEMS DEVELOPMENT ACTIVITIES

SYSTEMS PLANNING	SYSTEMS REQUIREMENTS	SYSTEMS SPECIFICATIONS	TECHNICAL REQUIREMENTS	IMPLEMENTATION PLANNING
A System Planning Study Report, covering: · Executive Summary · Introduction (background, terms) · Objectives and scope · Functional Descriptions · Performance Specifications · Design Specifications · Feasibility Analysis (technical, economic) · Acceptability Analysis (user, legal) · Supporting Documentation · For Present System: Functions, documents, manning chart, file elements, flow chart, constraints, controls, costs · For Proposed System: Functions, files, documentation, flow chart, constraints, controls, manning chart, file elements, inputs, outputs, flow charts and costs for non-computer and computer parts, development project plan, Gantt or PERT chart, cost comparisons, tangible and intangible benefits	A Systems Requirements Report, containing: · Job Descriptions · Input/Output Documents · File Description and Inquiry · Flow Chart of Computer System · Summary of Functions Performed (volume, times) · Data Element Description · Data Description · Glossary For Proposed System: · Management Summary (General description, benefits, processing cycle, system outputs) · Output Format · Output Description · Input Data Description · Data Element Catalog · Design Constraints · Controls · Flow Chart of Non-Computer Systems · New Manual Functions · Benefits Analysis · Economic Evaluation (updated) · Tangible Benefits Evaluation (updated)	A Systems Specification Report, covering: · Output Layout · Input Layout · Data Flow Diagram (of processing steps) · Master File Definition · Processing Flow Chart and Volumes · Run/Module Definitions and Volumes · Constraints (refined or updated) · Controls (refined or updated) · Back-Up Procedures and Security · Tangible Benefits Evaluation (updated)	A Technical Requirements Report, including: · Job/Run/Module Flow Charts · File Definitions & Labels · Input Definition · Standard Program Requirements (form headings, tables, run controls) · Run/Module Requirements (Functions, decision tables, logic charts, matrix tables, printer specification and support, merge or sort macro specifications, file controls) · Operating System Requirements (Job stream assembly, JCL) · Programming Schedule and Costs	An Implementation Plan, consisting of: · Project Plan (updated) · User Training Checklist · User Training Plan · System Test Increments · System Test Checklist · Computer Test Plan · Conversion Plan (Parallel processing, sequence) · File Data Acquisition Plan · Manpower and Equipment Plan · Tangible Benefits Evaluation (updated)

Figure 4-3a SYSTEMS DOCUMENTATION

PROGRAMMING	USER TRAINING	SYSTEMS TEST	CONVERSION	POST IMPLEMENTATION REVIEW
· Source Listings · Object Listings · Supervisory Parameters (JCL, etc.) · Utility Parameters · Program Test Plan · Test Data · Test Results · Console Messages and Operator Responses · Computer Center Instructions : ·· Console ·· Library · Restart Procedures · Logic Documentation ·· Logic Diagrams ·· Decision Tables	· Modified User Training Plan · Policies · Procedures · Job Outlines · Forms · Notifications · Training Plans · Training Schedules · Training Manuals · Training Aids · Equipment and Facilities Requirements	· Revised Systems Test Checklist · Revised Computer Test Plan · Test Data · Systems Test Results (approved by user or IPC) · Systems Test Discrepancy Notices (acted upon) · Systems Acceptance · Updated Systems Project Plan	· Modified Conversion Plan · Implementation Results Log · Implementation Discrepancy Notices (acted upon) · Implementation Results Approval · Project Termination Notice	A Post-Implementation Review Report, including: · Management Summary · Interview Schedule · Related Systems Service Requests or Initial Investigation Summaries · Implementation Discrepancy Notices · Interview Summary · Actual Staffing Requirements · Actual Non-Computer Cost Summary · Actual Computer Cost Summary · Systems Development Cost and Schedule Performance Summary · Actual Benefits Analysis (Narrative) · Actual Tangible Benefits Evaluation · Planned versus Actual Economic Evaluation Summary

Figure 4-3b SYSTEMS DOCUMENTATION

Management Participation

To render such a project structure manageable, the chief ingredient required is management itself. Where structured system development processes have been installed successfully, management committees have frequently assumed responsibility for commitments of resources and monitoring of progress. Management's role is very much akin to that within any effective capital budgeting process. In fact, where adequate capital budgeting mechanisms have existed, it may be preferable to apply these mechanisms to the planning and control of EDP resources.

Management committees with EDP responsibility may be formed at one or two levels. The function discussed below in two levels may be consolidated into a single level where size and scope permit.

EDP steering committees, typically, are formed at the vice-president level. Because of its stature, such a committee functions at a policy and direction level, establishing priorities, allocating resources, and monitoring progress. The committee may occasionally become involved in individual projects, and with establishing management for the EDP function.

Task force committees tend to be larger than steering committees. Their membership tends to be at a departmental management level, supplemented by full-time participation of supervisors assigned to specific projects. The EDP director and key project leaders also participate. This committee meets more frequently than the steering committee. It is a working group charged with day-to-day performance and monitoring of a specific project or related projects.

PROJECT MANAGEMENT

Project management is the planning and controlling of the system development process. This discussion of project management techniques assumes a structure for system development which is comparable, but not necessarily identical, to that described above.

The objectives of project management are to:

- Deliver a quality product, on schedule and within budget.
- Communicate an understanding of status throughout the duration of a project
- Identify inevitable problems as early as possible, providing the ability to react with optimum results.

Prerequisites for project management include establishing understandable measurable work units. These make possible the assignment of work, identification of completed tasks, forecasting of progress, and measurement of results. Included in these work units must be predetermined quality control review points interspersed throughout the project structure. Quality control can not be effective if it takes place only at the completion of a project, forcing expensive revision if problems are detected.

Project management is implemented in two phases, project planning and project control. A project plan is a formalized statement structuring the activities of a project for orderly implementation. Project control covers the execution of project activities.

Project Planning

Project planning is usually performed just before the start of system requirements activities. Planning relies heavily on system planning documentation (See Figures 4-2a and 4-3a). Wherever feasible, planning is done by persons who will lead the project itself. Planning elements include:

- Finalized project guidelines, including statements of objectives and scope and descriptions of end products.

- Work breakdowns prepared for each activity, task, and subtask. These breakdowns are carried to a work unit level where performance requires a single skill and work conclusions can be evidenced with tangible output. Each unit can be accomplished in a predetermined, maximum time, such as two weeks.

- Budgets and schedules built up from the lowest work units through successively higher-level summaries. For each work unit, start and completion dates are set. Budgets are based on types and levels of skills involved rather than on assignments of individual persons.

- Plans and schedules reviewed and approved. Formal commitments are obtained for their fulfillment. At this point, project planning documentation becomes a yardstick against which all subsequent activities within a systems project are monitored and measured - and variances are reported.

Project Control

Project control is a process for assigning, measuring, evaluating, and redirecting the performance of a project. Three basic elements are involved:

- Short-term scheduling performed just prior to initiation of individual work units. This involves assurance that prior work is complete and that personnel are available. Changes to the formal plan are made only if they are significant – and if they are necessary to meaningful communication. Explanations and approvals are, of course, required to support such changes.

- Work assignment is an extension of short-term scheduling. Individuals are assigned to specific tasks with explicit directions for the work to be performed and results to be realized.

- Evaluating and reporting of status concentrates on reporting progress against plan. All variances are identified and reported according to cause – planning, individual performance, or resource availabilities. Status is reported according to two main categories - by activity and by people.

One essential for the development of project control is reporting on the basis of earned hours. Work units are not considered complete and hours are not considered earned until there is a review and approval of the tangible output from the work – no matter how long it actually takes to complete the work. Large variances between hours earned and hours worked indicate potential problems not just in performance, but in possible restrictions in completing or reviewing work units.

SECTION V - THE EDP AUDIT ENGAGEMENT

EDP IMPACT ON THE AUDIT ENGAGEMENT

The preceding sections provided a background in the computer control concepts and techniques. This section discusses the audit philosophy and practice in an EDP environment.

AICPA Statement on Auditing Standards No. 1 (Section 320.03 and .04) sets forth definitions and basic concepts for "The Auditor's Study and Evaluation of Internal Control" and for correlation with other auditing procedures. This statement establishes:

> "The increasing use of computers for processing accounting and other business information has introduced additional problems in reviewing and evaluating internal control for audit purposes . . .
>
> "Closely related to the increasing use of computers is the trend toward integrating accounting information required for financial and other operating purposes into coordinated management information systems. This development increases the need to clearly identify the elements of the total system that are comprehended in the auditing standard concerning internal control."

The auditor normally divides the client's accounting system into individual or groups of applications to facilitate review, e.g., purchasing, cash disbursements, payroll, etc. Each application containing internal controls on which the auditor plans to rely in arriving at his opinion on the financial statements, as shown in Figure 5-1, should be:

- Reviewed – primarily a process of obtaining information about the organization and the procedures prescribed.
- Tested – to assure that the necessary procedures were performed correctly and by the proper personnel.
- Evaluated – by applying the following steps to each significant transaction, asset or application:
  - Consider the type of errors and irregularities that could occur.
  - Determine the accounting control procedures that should prevent or detect such errors and irregularities and insure they are corrected if they occur.
  - Determine whether the necessary procedures are prescribed and are being followed satisfactorily.

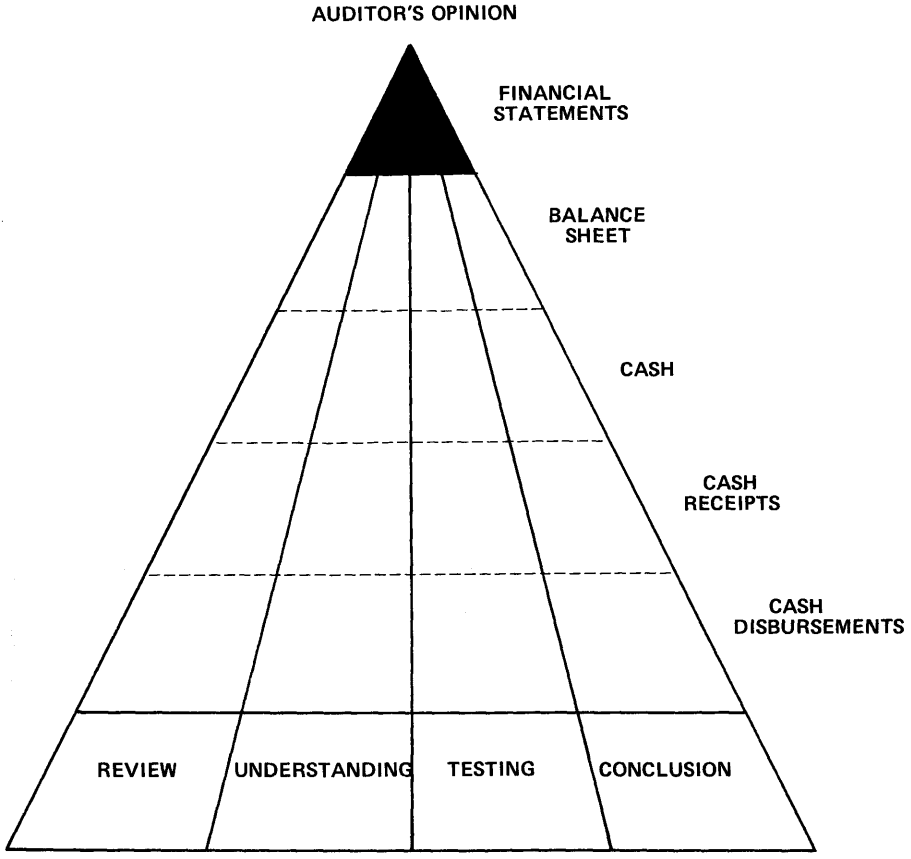


Figure 5-1 GETTING TO THE "ULTIMATE CONCLUSION" THAT THE FINANCIAL STATEMENTS ARE FAIRLY PRESENTED

- Evaluate any weaknesses – i.e., types of potential errors and irregularities not covered by existing control procedures to determine their effect on the reasonableness of the financial statements, on the auditing procedures to be applied, and on suggestions to be made to the client.

If any application which has been selected is processed by computer, the auditor must evaluate what method he will use to review, test and evaluate the "EDP application." The steps that the auditor follows in an EDP application review are discussed later in this section.

HOW EDP AFFECTS THE AUDIT

Areas within the structure of the audit engagement where changes are likely to be required to accommodate EDP considerations include:

- Scope
- Timing
- Staffing
- Preliminary review
- General computer installation review
- Application reviews
- Examination of application/system development controls
- Budgeting and scheduling
- Supervision and review
- Reporting

Scope

Just as the extent of audit procedures is affected by evaluating the client's system of internal control, so too is the extent of the EDP review. Accordingly, the applications with material financial statement impact should receive the greatest attention.

In the manual phases of an engagement, i.e. "auditing around the computer," the auditor could examine only that part of a computerized data file that was printed out in the normal course of the client's

business. Since such files often contain much information which is not normally printed out, the auditor should determine what this "additional" information is as it could cause a change in his audit scope.

Timing

The principal reason for differences in audit timing between "manual" and "EDP" audits is because of the difficulty in obtaining client data files, debugging programs and arranging access to the computer. Additionally, the staff may have a lack of experience with the computer, resulting in extra time required to set-up and/or complete the job.

Another factor that tends to extend timing is the need for careful planning. In a manual audit, the auditor can alleviate poor planning by making changes on the spot, but when using a computer, such changes may not be as easy to make.

Staffing

The staff on any EDP audit should have actual experience with computers, the ability to communicate with EDP personnel, and a willing attitude to try new techniques. The areas of the EDP examination to be performed by this staff should be divided as follows:

- Audits of systems development requires the most EDP expertise. Technical assistance may be necessary,

- Installation (operation) audits require a moderate degree of EDP expertise with a good background knowledge of computerized financial and other applications,

- Application audits require the least EDP expertise because it is the most familiar area to the auditor.

In addition to competent and experienced staff, the number of staff assigned to different sections (tests of manual procedures, confirmations, etc.) must be determined.

Preliminary Review

The purpose of the preliminary review is to obtain a familiarization with the client's overall organization, accounting information system, and general controls permitting the development of an audit plan. The preliminary review should be sufficient to permit the auditor to identify material applications which will require further review, evaluation and audit testing. The preliminary review should result in an audit plan that includes the following:

- Extent of further examination to be performed
- Organization
- Applications to be examined
- The timing of these examinations
- The handling of special problems which may be encountered in performing the examinations, such as the loss of visible audit trail or preliminary indications of serious control weaknesses.

In establishing the audit plan, the auditor should keep in mind that each review area has its own typical areas of exposure. Some of these are:

- *Installation/operations* – general errors and omissions, operating capacity and capabilities, file integrity, accountability of processing, business interruption, etc.
- *Applications* – unauthorized transactions, incomplete or duplicate inputs, fallacious processing logic, unresolved exceptions, omitted or duplicate transactions, undetected erroneous transactions, nonconformity with generally accepted accounting principles or lack of consistency of application of accounting principles, etc.
- *Applications and system development* – unsatisfactory application processing logic, internal controls, auditability or application of generally accepted accounting principles; and unanticipated audit problems including extra audit time.

General Computer Installation Review

If an application identified during the preliminary review is processed with a computer, the auditor should make a study and preliminary evaluation of the computer installation controls to identify major weaknesses to be considered in the study and evaluation of accounting controls.

Installation controls are directed to most or all of the applications processed by an EDP system. Effective installation controls provide an environment conducive to good accounting control. Further, the effectiveness of many applications controls can be significantly impaired without the support of effective installation controls.

When installation controls within the EDP organization are found to be weak or absent, the auditor must consider whether those application

control procedures performed external to the EDP organization reasonably compensate for the deficient installation controls.

Applications Review

The application analysis enables the auditor to expand his knowledge of the client's accounting information system and permits him to determine the degree of reliance that may be placed on the client's system of internal controls and the resultant nature, timing and extent of the audit procedures to be performed. This analysis is performed in four phases:

- *Preliminary Understanding* – the auditor obtains a preliminary understanding of the application through review of existing client documentation. As required in the circumstances, he adds to this understanding by interviewing client personnel and preparing supplemental audit documentation, which may include analytic flowcharts of the application processes.

- *In-Depth Understanding* – to verify his preliminary understanding, the auditor may perform a limited amount of compliance testing, interviewing of personnel, observing of processing or he may inquire into exceptions to prescribed controls and procedures. Further, a limited sample of transactions may be "walked through" the computer.

- *Testing Controls* – the auditor will then test both the manual and computer phases of the application, using one or more of several available EDP audit tools and techniques to verify that the controls are in fact working.

- *Evaluation of Results* – finally, he will determine the degree of reliance that may be placed on the client's internal controls. This evaluation is based upon the auditor's knowledge of the client's procedures and controls obtained during the previous phases.

During these phases, an internal control evaluation guide or checklist may be consulted to provide points for consideration in identifying the existence or absence of specific internal control procedures.

Documentation of the auditor's evaluation should include working papers and memoranda which cover:

- A factual description of the client's system

- Identification of weaknesses in the client's system of internal controls, and compensating strengths (if any),

- Evaluation of the internal control over the application based on all controls present, and

- Substantive audit procedures selected as a result of the evaluation process.

Each application control must be considered in light of others within the application, i.e., the auditor must ask himself "what would happen if this control did not exist," and for essential but inadequate controls "does a compensating control exist which eliminates the problem?" If compensating controls exist, the exposure (e.g., estimated error rate multiplied by the maximum value that the error could attain) may negate the problem. In all cases, the cost/risk equation must be applied, i.e., no control should cost more to install or maintain than the maximum error that could arise if it were not installed or maintained.

Examination of Application/System Development Controls

The controls exercised over the development of a computer application or system, and the controls implemented in the developed application should be examined in detail on a first examination or when extensive changes have taken place. They should be reviewed and tested during each audit, to the extent they relate to an area in which the auditor plans to rely on internal control, to determine that they are still working satisfactorily.

Budgeting and Scheduling

Once the auditor has established the scope of the review and has selected the approach, he should establish a budget for each task and a schedule for when the tasks are to be performed. Computer utilization and staff time (as previously discussed) will make the budgeting task difficult but it *must* still be performed.

Supervision and Review

Because of the unfamiliar and often complex nature of the environment, the EDP auditor must be more intensively supervised than in the traditional manual environment. The review of the EDP audit *can be* performed at the functional level *by regular audit supervisory personnel.* However, review at a technical level *may also be* required if the engagement covers complex areas.

Reporting

The purpose of the auditor's study and evaluation of internal control is primarily to establish a basis for reliance thereon in determining the nature, extent and timing of audit tests to be applied in his examination

of the financial statements. His first "report" then, is on audit scope. The auditor also should report to management in a "letter of recommendations" regarding possible operating efficiencies and improvements in internal control.

Summary of EDP Impact on the Audit Engagement

The "EDP review" is really a function or extension of the auditor's professional responsibilities when a particular application contains internal controls on which the auditor plans to rely. The "normal" audit is affected in various ways by EDP, e.g., if EDP is present, the need for more careful planning and supervision is increased.

EDP AUDIT TOOLS AND TECHNIQUES

Once the auditor has selected the applications to be tested, he must select the verification method he will utilize to perform tests of the key functions and controls in the application. These are covered now so the reader will have a proper frame of reference when they are discussed in conjunction with particular application and other audit procedures later in this section.

The auditor can use a variety of EDP audit tools and techniques in verifying controls. Figure 5-2 summarizes these, relating the various techniques to the applicable tool. The purpose of each is also indicated. There are two purposes for utilizing the various tools and techniques described: (1). to verify the manual and/or computer phases of processing, i.e., *processing operations* or (2) to verify the *results of processing.*

Auditing Around the Computer

In auditing around the computer (the traditional manual approach), the results of computer processing are verified manually against source data processed by the computer. Verification takes place without direct involvement of the auditor in processing within the computer itself. This type of verification can be done either on a sampling basis or through a comparison of balances.

Auditing around the computer has the following *advantages:*

- Little technical training is necessary – the auditor has used this approach many times and very little new training is necessary.
- It is results oriented – the end products are readily identifiable and may be used as a measure of processing reliability.
- It is understood by everyone – there is little technical terminology and audit objectives are clear and easy to understand.

TECHNIQUE	TOOL	PURPOSE
Auditing around the computer	Manual approaches	To verify the manual *and/or* the computer *phases* of processing
Program listing verification		
Program logic flowchart verification	Manual approaches *and / or* Program flowchart software	
Test data approach	Manual approaches *and/or* Test data generator software	
Integrated test facility or "mini-company" approach, an extension of the test data approach		
Parallel simulation of all or parts of a client computer system to produce a system that parallels the client program and independently reprocesses client data	Custom designed computer programs	
	Generalized audit software	
Confirmation of items on a file with another person	Manual approaches *and/or* Custom designed computer programs *and/or* Generalized audit software	To verify the *results* of processing
Comparison of items on a file with another independent file or to their physical existance		
Edit and reasonableness tests on items in a file		

Figure 5-2 EDP AUDIT TOOLS AND TECHNIQUES

Note on Terminology: This text is a blend of EDP and audit terminology, and thus throughout this text the term "verify" is used in two ways — to determine accuracy or correctness, and to substantiate, as by audit tests, accuracy or correctness. The particular meaning is dependent on the context.

- Cost is generally low – because of the little technical training necessary and the other aspects above, the costs of this method are very low.

The following *disadvantages* can, however, cause the auditor to select another method:

- Detailed output for testing purposes is required at all stages in the application to see what has happened to the records. It may not be available.
- Voluminous systems may exceed the capacity of manual testing even with use of statistical sampling techniques.
- It may be difficult to obtain representative data.
- The staff is not exposed to EDP and they may not be prepared for more complex audits in the future.

Program Listing Verification

This method, also known as "code checking" or "desk checking," verifies the reliability of computer processing through detailed analysis of program code listings. It is the *least used method* because:

- It is necessary to understand the programming language and, therefore, requires a high level of expertise
- If the program is changed, the listing becomes obsolete
- It is time consuming and cumbersome for large applications
- It does not verify processing, i.e., it does not get into the operating environment, e.g., processing by utilities, operating systems, etc.

Code checking has its place when it is used for examining specific problems or debugging programs.

Program Logic Flowchart Verification and Flowchart Software

Program flowchart verification is an examination of logic processing flowcharts which provides a graphic view of the processing that takes place. Most computers now accept software routines which will generate computer process flowcharts mechanically.

As to *advantages,* program flowchart verification is very useful for debugging program logic or examining specific logic because the visual representation of the logic processing is easier to follow and understand than are program code listings.

As to *disadvantages,* the software which generates these flowcharts is, however, often expensive and technical assistance or training may be necessary to understand more complicated applications. If the auditor is not thoroughly familiar with the application logic or flowcharting, this method can become very time consuming.

Test Data Approach

Test data ("test decks") are sets of input data which present a repertoire of transactions to the computer for verification through actual processing as a means of identifying invalid results. The most effective circumstance in which test data techniques are applied is in the verification of on-line, realtime applications.

Test data have the following *advantages:*

- Little technical training is necessary for staff
- It is excellent if the variety of possible transactions is limited
- It is excellent for debugging programs or testing one part of an application where variety is limited.

The auditor should be *cautious in the use* of test data for the following reasons:

- In complex systems or in systems where voluminous varieties of transactions are present, it is very difficult to anticipate all conditions and variables.
- It is impractical to expect the auditor to be highly familiar with the application logic. As a result some unanticipated bugs or test conditions which were created may show up as exceptions and debugging of the auditor's test data may become necessary.
- The auditor must have highly detailed documentation of the application.
- Master file creation may require technical assistance due to complex file arrangements, etc.

- Test data can be very time-consuming when attempting to test *all* conditions for a given part of or an entire application.

- The approach lacks objectivity in that the tests are oriented to documented controls and what will go wrong is what is not expected.

Test Data Generators

One of the more recent attempts to improve the applicability of test data in complex systems and situations is test data generator software. This type of software package employs various techniques to generate variable test data such as random values, constant values or values within specified ranges to be placed into fields within records and may also be used to create data that is in error.

This method helps to eliminate some of the disadvantages cited above such as the time consuming nature of preparing test data and the difficulty in identifying *all* exception situations. A possible disadvantage of this method is the potential cost of comprehensive versions of these software systems.

Integrated Test Facility (ITF) Method (The "Mini-Company" Approach)

The integrated test facility (ITF) method (also often referred to as the "mini-company" approach) is an extension of the test data approach. It permits the introduction of selected test input against a master file that also contains live data and the tracing of these test transactions through the various functions in the system with comparison to predetermined results.

ITF involves the establishment of a "dummy" entity against which the data can be processed, i.e., a division, employee, etc. After the entity is established, transactions can be processed through the regular programs against this entity using the normal company documentation. The auditor determines what checks he wishes to make, such as overdue items, merchandise returns, etc., and compares the results to predetermined results. The programs are designed to exclude the test transactions and records from the totals that are recorded in the accounting records.

The *advantages* of using ITF are as follows:

- Little technical training is necessary because the auditor can utilize existing company documentation, which should be understandable by the users of the system, instead of being technically proficient enough to prepare it himself from technical system documentation.

- Low cost of test data as it is processed with regular input.

- It gives an ability to test the actual system as it is currently operating.

The *disadvantages* of ITF are:

- The "test data" transactions must be removed from the company's control records (e.g., general ledger, etc.) by use of either journal entries or program modifications.

- Cost can be high if the client's program requires modification to exclude "test data" transactions.

- There is a possibility of destroying client files since transactions can affect "live" records.

- It is difficult to identify all variations of exceptions to test the program.

- The program logic being tested may not be identical to that processing "live" data.

Parallel Simulation

Parallel simulation consists of the preparation of separate computer audit programs that perform the same functions as those used for daily application processing. The simulation programs accept the same input data as the application programs, use the same files, and attempt to produce the same results. This is illustrated in Figure 5-3.

The important characteristic of parallel simulation is that independent processing of relevant data takes place. The *advantages* of this technique are:

- It is more thorough than sampling – full days, weeks, etc. transactions can be processed rather than 1% or a block

- Little technical training is necessary for the staff and they also get involved in EDP

- It is excellent for complex or voluminous systems – which are not susceptible of manual testing

Parallel simulation, however, has the *disadvantage* that special care must be exercised in selecting representative data as the "live data" of the client may not include unusual or significant items.

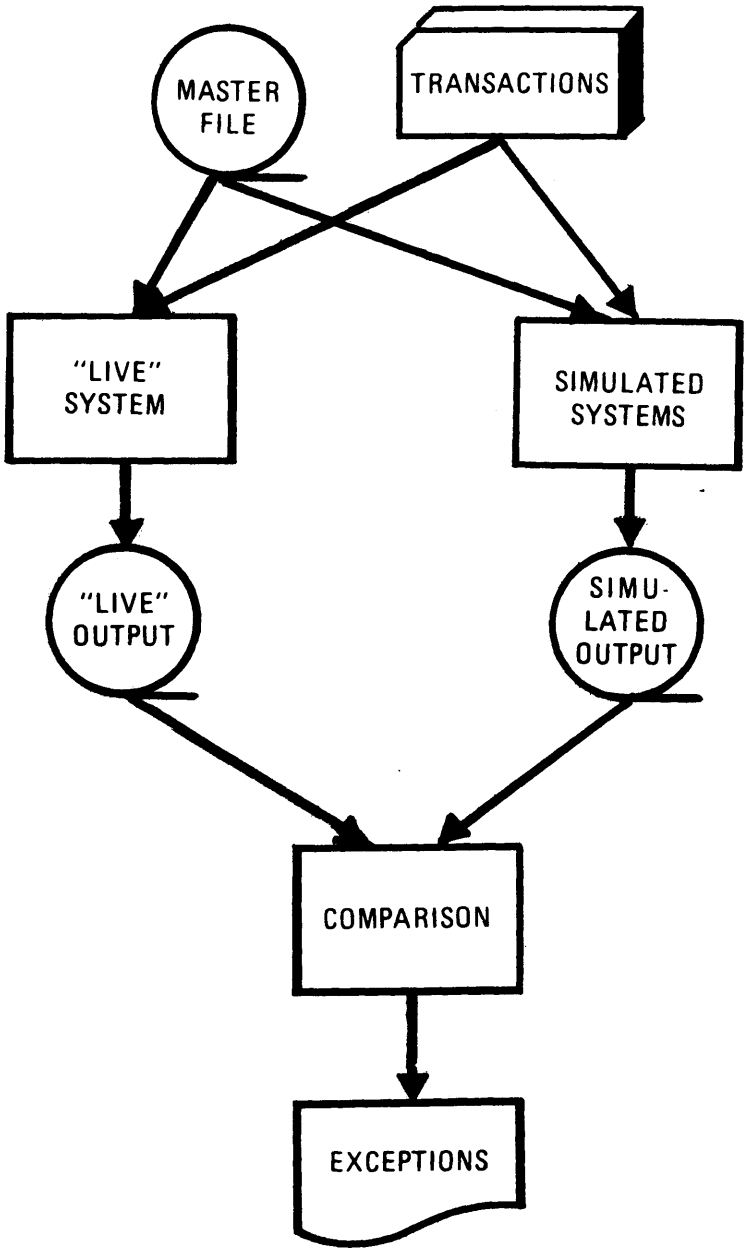


Figure 5-3 PARALLEL SIMULATION TECHNIQUE

Custom Designed Computer Programs

In the past auditors often had client programming personnel or other EDP technicians write special, custom designed programs for specific audit purposes. These programs were usually written in COBOL or some other language with which the auditor was not expert. With the advent of audit software such as STRATA, custom programs have become partially obsolete. However, they do have the following *advantages:*

- The auditor is still involved with EDP because he works with the programmer and sets the required parameters.
- They often are used in place of audit software or when "non-standard" files exist.

Some of the other reasons why custom programs have *decreased in usage* are:

- High cost – due to required technical assistance from a programmer.
- Programmers usually need long lead-time.
- If system or application changes are made, the entire program may become obsolete.
- The auditor must still insure that the programmer wrote a valid program, i.e., he still must test it and control it year to year.

Generalized Audit Software

Basically, general purpose audit software, e.g. STRATA, presents a method of converting instructions, written in terminology functionally related to audit activities, into computer programs. It is *applied in four broad areas:*

- Detective examination of files, i.e., confirmations, comparisons, etc.
- Verification of application processing, i.e., parallel simulation,
- File correction, i.e., translation of audit adjustments to adjustments of computer files, and
- Management inquiry, i.e., special reports.

Originally developed in the late 1960's and improved upon significantly in the early 1970's, generalized audit software has become in

many cases a "high level auditor's computer language." Generally developed by auditors for auditors, audit software has the following *advantages:*

- It requires a minimum of special training and a minimum of EDP expertise for use.

- It allows the user, i.e., the auditor, to write his own programs without the assistance (except in the most complex of cases) of an EDP technician.

- The auditor is in control of the programs at all times.

- In developing, writing, and running his own programs, the auditor gains a significant amount of familiarity with EDP in general and particularly with application design and control "on the job."

- The auditor can also utilize it, because of its power and flexibility, to perform a variety of tasks including parallel simulation of client programs, tests of results or processing, e.g., confirmations, and can often use it in place of the test data approach, i.e., simulating edits in a client program against live data.

- In addition, it provides the auditor, and many other users, with the capability to produce quickly and inexpensively special one-time reports, to produce programs to fill the gap in existing systems, to meet unusual or new requirements, to initially design and debug new systems, etc.

The *only disadvantage* of audit software is that, as with any other computer audit tool, changes made to applications *may* require that the audit software program be partially rewritten each year. The changes, however, are generally much faster and easier to make than with other tools, e.g. custom designed computer programs.

Confirmation, Comparison, and Reasonableness and Edit Tests

All three of these techniques have been used extensively for many years in non-computer audits of applications. They are used primarily to verify results. As they are familiar to the auditor, they will be commented upon here only briefly:

- Confirmation — of contents of a file with another person, e.g. the customer. This provides strong assurance that the file is being maintained accurately.

- Comparison — of the contents of a file with the contents of other records maintained independently, e.g. checking payroll records to

personnel files. Comparison can also be the comparison of the records on a file to the physical item, e.g. comparing inventory records to the actual inventory.

- Reasonableness and edit tests – of items within a file, e.g. checking for credit balances, zero balances, excessive balances, etc.

Verifying results with these techniques may be done either manually or with the computer using custom designed audit programs or generalized audit software.

Summary of EDP Audit Tools and Techniques

The range of audit tools and techniques which the auditor has at his disposal to use either to verify results or to verify processing is wide. Each of the tools and techniques, used separately or in combination, may have its place in any given audit situation. Each, however, has its own particular advantages and disadvantages – and the auditor must be cautious to pick the one with the most advantages for his engagement.

Any one or a combination of these techniques may be utilized by the auditor. It is usually easy to negate disadvantages of certain techniques by combining two or more techniques.

AUDIT OF EDP APPLICATIONS

The audit of applications is covered in this text before the audit of installations and systems because:

- It is a more familiar area for the auditor
- A knowledge of documentation and applications is necessary in order to understand how the installation operates.
- Knowledge of existing applications is a key factor in the review of developments of new systems and applications.

Overview of Steps in Application Audits

The steps that the auditor should follow in an application audit, as illustrated in flowchart fashion in Figure 5-4, are:

- Obtain a *preliminary understanding* of the application:
  - Review existing documentation and interview personnel
  - Prepare supplemental audit documentation, including analytic flowcharts, as required

- Evaluate existing controls in relation to audit objectives.

- Obtain an *in-depth understanding* of the application:

  - Verify the preliminary understanding. The auditor may interview personnel, observe processing, inquire into exceptions to prescribed controls and procedures, or track a limited sample of transactions through the system, i.e., "walk them through."

  - Identify and evaluate critical controls and processes and known exposures. (At this point, it may be necessary to retrack the preliminary understanding steps if enough information is not available.)

- *Test* the system:

  - Select the verification methods, i.e., verify results or processing (both manual and computerized)

  - Select the verification techniques, e.g., comparisons, confirmations, parallel simulation, test data, etc.

  - Determine whether use will be made of the computer for testing and, if so, which tool (or tools) are to be used

  - Perform the tests.

- *Evaluate and report* on the results of the reviews and tests.

These steps are discussed in more detail in the remainder of this section.

Obtaining a Preliminary Understanding of the Application

In order for the auditor to obtain a preliminary understanding of the application, he must obtain all necessary and relevant application documentation. This information should be obtained in advance of any test procedures. (In addition, of course, he should obtain any relevant information resulting from other phases of the overall review, i.e., the installation/operations review and/or any systems/application development reviews.)

There are three steps in the preliminary understanding phase:

- Reviewing existing documentation

- Preparing supplemental audit documentation as required

- Evaluating the existing controls in relation to the audit objectives.

Review Existing Documentation

Traditionally, system documentation available to the auditor has varied widely by company. Where a company has installed and followed adequate standards, existing documentation should go beyond the requirements of the audit examination. At a minimum, existing documentation should include:

- System and application logic flowcharts
- Information on the programs and files in the application
- Summary of the application input
- Schedule of exception reports
- Schedule of output

An initial examination of the above documentation, and particularly the flowcharts, should be performed to obtain an understanding of the application and to determine if the necessary controls exist for the application. In performing this review, the auditor will be particularly interested in two types of documentation:

- Documentation of manual processing, i.e., paperwork flows, examples of forms used, clerical instructions, and policies and procedures manuals
- Documentation of computer processing, i.e., file definitions, transaction definitions, non-technical specifications describing processing for the users.

In addition, the auditor will obtain or prepare, and review, for each material application, documentation on the backup of the application files, program documentation, etc., and recovery plans in the event primary application files are lost or destroyed.

In the process, activities in the following areas should be covered for both transaction and master files:

- Input controls
- Processing controls
- Control over error handling

APPLICATION REVIEWS

Page 1 of 2

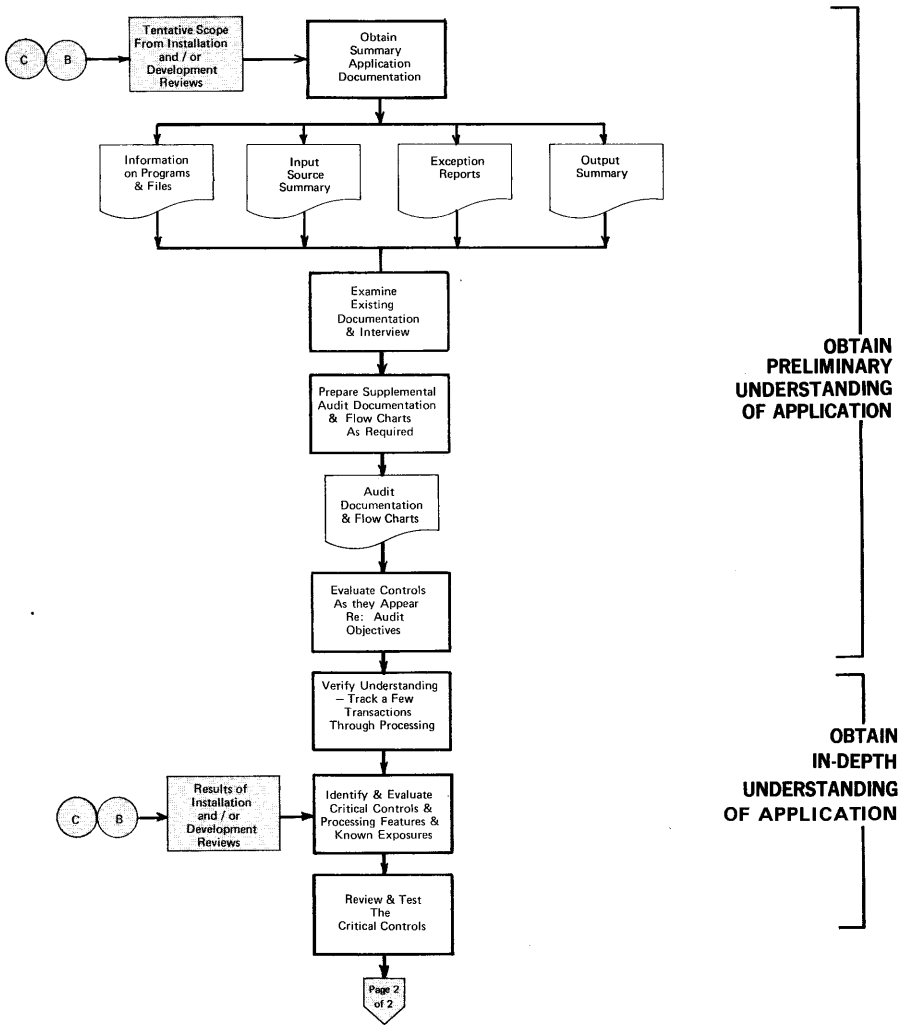


Figure 5-4 FLOWCHART OF APPLICATION AUDIT PRACTICES, Page 1 of 2

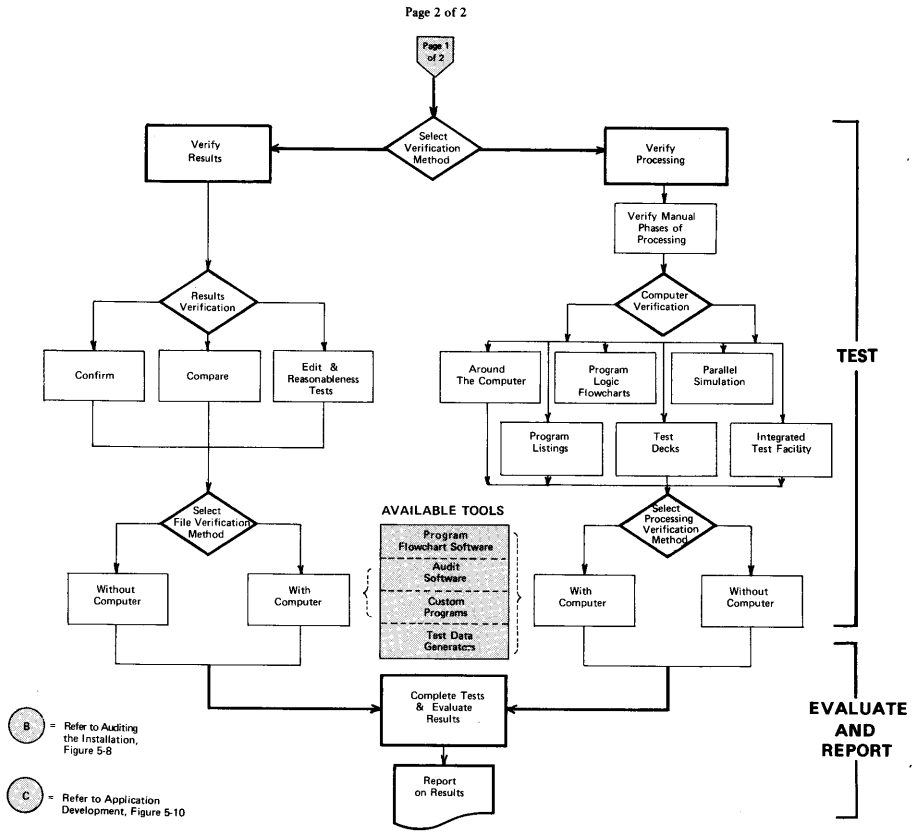


Figure 5-4 FLOWCHART OF APPLICATION AUDIT ACTIVITIES, Page 2 of 2

- Input/output control group
- Output controls

Where detail documentation is not available, interviews should be conducted with responsible personnel to define operating procedures.

Prepare Supplemental Audit Documentation As Required

If the company's documentation is not adequate for the auditor's purposes (this itself is a control weakness), the auditor will have to prepare, or have prepared, supplemental documentation in order to adequately evaluate controls.

A useful audit analysis tool not often found in many installations is an analytic flowchart, which identifies all manual and computer processing in an application. It shows all files and transactions subject to processing, who does the processing, and what is done.

A completed flowchart presents a comprehensive picture of:

- What is happening during the normal processing of transactions, files, and outputs
- Many of the controls incorporated in the processing sequence of the application
- The nature of the various files which are used within the application.

Figure 5-5 is an example of a standard analytic flowchart for the input/output control and keypunch portions of a system. Preparation of an analytic flowchart may be advisable in many cases.

Evaluating Existing Controls in Relation to Audit Objectives

After reviewing existing documentation and preparing such additional documentation as is required, the auditor should evaluate the controls as they appear in the documentation in respect to the audit objectives. This preliminary evaluation of the apparent level of control will assist him in determining the details of his compliance tests and approach to later substantive audit tests.

Obtaining an In-Depth Understanding of the Application

Once the auditor has obtained, reviewed and preliminarily evaluated the application documentation, he must verify that the documentation

is current and valid for the present system. Often, the auditor must retrace his steps and get additional information or interview additional personnel to obtain an "in-depth" understanding.

There are two steps in the "in-depth" phase:

- Verifying the preliminary understanding
- Identifying and evaluating the critical control and process features.

Verify Preliminary Understanding

The most common method that the auditor uses to verify his understanding of the application is to "walk through" the manual portions of the system, tracking a few transactions and observing a limited number of examples of:

- Transaction working documents which have been filled out
- Control logs or registers
- Other available documentation to verify the accuracy of the flowchart and the auditor's understanding of the system.

Identify and Evaluate Critical Control and Process Features

The next step after verifying understanding is the verification and evaluation of the control and processing steps and features which are critical to the application. In identifying those controls which must be tested, the auditor must distinguish between *characteristics that constitute controls* and *activities subject to control.*

To accomplish this identification, the auditor may use a control matrix, similar to the one shown in Figure 5-6a. Characteristics that constitute controls are shown down the left side, with activities subject to control across the top. The characteristics that constitute controls, i.e., potential controls, are categorized under the two general headings of preventive and detective controls. Detective controls are then further subdivided as indicated in Figure 5-6a. These controls have been discussed throughout previous sections. However, for convenience in reviewing what the controls mean, they have been explained in Figure 5-6b.

A few examples of the broad categories of activities subject to control are shown on the top of the matrix in Figure 5-6a. The general terms describing these categories have also been discussed previously, but are summarized for convenience in Figure 5-6c. Depending upon the application, transaction, process, etc., being reviewed, each category

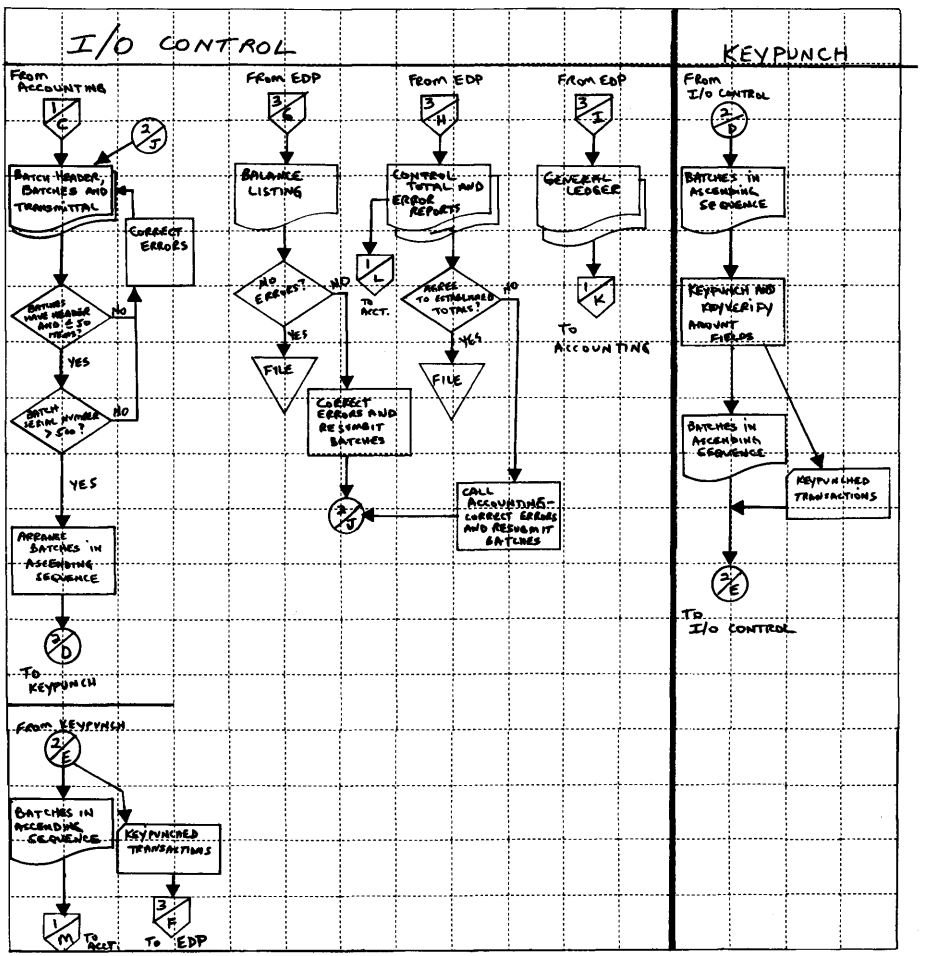


Figure 5-5 EXAMPLE OF A PORTION OF AN ANALYTIC FLOWCHART

may be composed of many individual parts. "Editing" for example could be composed of all the individual edits on each field in a particular transaction.

The matrix will be completed by referring to the application documentation previously reviewed and to the analytic flowchart of the application. In the process, each activity on the analytic flowchart should be categorized either as a control or activity over which control is exercised. The analytic flowchart may not indicate controls which do not involve a decision or activity. These passive controls are usually preventive in nature, but their identification is still important.

The types of controls usually found to be essential include those which assure:

- That all valid and no improper or extraneous transactions that are significant to audit objectives were processed
- That processing logic is proper and correct
- That all transactions processed through one step reach the next step
- That unreasonable or erroneous processing or results is detected.

If controls which should exist are not found, the auditor must look for compensating controls. He must then evaluate the adequacy of the controls, including compensating controls, and estimate the exposure caused by missing controls.

In addition to the above, the auditor must also be concerned with the activities of the EDP control group and the functions it typically performs (particularly if those functions are in fact performed by users and not the control group). Proper control of processing from start through each step of processing, handling of out-of-balance conditions and rejected transactions, error resolution, and the impact of unresolved errors are of particular concern to him. The adequacy of the control group's testing of output must also be reviewed.

In the event the application involves file maintenance transactions and master files, they must be reviewed as are other application areas. Control over sensitive master files and file maintenance transactions, periodic user review of important master files and frequency of file verification are several of the major areas that must be reviewed by the auditor.

CONTROLS MATRIX

ACTIVITIES SUBJECT TO CONTROL

CHARACTERISTICS WHICH CONSTITUTE CONTROLS

CONTROL FEATURE \ TRANSACTION/PROCESS	Initiating	Recording	Formating	Coding	Etc.													
PREVENTIVE CONTROLS																		
Segregation of duties																		
Definition of responsibilities																		
Rotation of duties																		
Competence of personnel																		
Secure custody																		
Dual access / dual controls																		
Standardization																		
Mechanization																		
Prenumbered forms																		
Precoded forms																		
Authorization																		
Cancellation																		
Endorsement																		
Simulation preparation																		
Documentation manual																		
DETECTIVE CONTROLS																		
Accountability of Input																		
Anticipation																		
Transmittal																		
Batch serial numbers																		
Completeness of Input																		
Amount control total																		
Document control total																		
Line control count																		
Hash total																		
Batch totals																		
Completeness check																		
Visual verification																		
Turnaround document																		
Approval codes																		
Correctness of Input																		
Format																		
Mandatory data present																		
Legitimate codes																		
Check digits																		
Reasonableness																		
Limit check																		
Validity check																		
Read-back																		
Expiration																		
Dating																		
Keystroke verification																		
Approval																		
Security checks																		
Completeness of Processing																		
Run-to-run totals																		
Reconciliation																		
Balancing																		
Aging																		
Suspense file																		
Matching																		
Suspense account																		
Clearing account																		
Tickler file																		
Periodic audit																		
Correctness of Processing																		
Redundant processing																		
Summary processing																		
Sequence checking																		
Overflow checks																		
Scan before distribution																		
Discrepancy reports																		

Figure 5-6a WORKING PAPER MATRIX FOR DESIGNATION OF CONTROL AND PROCESSING TO BE TESTED

CHARACTERISTICS WHICH CONSTITUTE CONTROLS - 1

CHARACTERISTICS WHICH CONSTITUTE CONTROLS	EXPLANATION OF CONTROL
PREVENTIVE CONTROLS:	
Segregation of Duties	The responsibility for custody of data and accountability for its handling and processing are separated.
Definition of Responsibilities	Specific descriptions are provided for the performance of all tasks within an information processing system. These indicate clear beginning and termination points. They also cover the relationship of responsibilities to each other.
Rotation of Duties	Under this control technique, jobs are rotated periodically, at irregularly scheduled times if possible. This applies to persons with responsibility for key processing functions within a financial information system.
Competence of Personnel	Persons assigned to processing or supervisory roles within information systems should have the training and experience to perform them reliably.
Secure Custody	Information resources of a company are subjected to special measures for safekeeping. These measures are similar in nature to those accorded to cash, negotiable securities, signature plates for checks, or other assets.
Dual Controls/ Dual Access	These are controls for which two simultaneous actions or conditions are required before processing is permitted.
Standardization	Uniform, structured procedures are developed for all processing which takes place.
Mechanization	Mechanization of a processing function applies control to the extent of the greater consistency of the equipment involved.
Prenumbered Forms	Allows later detection of loss or misplacement of transaction documents. Sequential numbering makes accountablility controls feasible.
Precoded Forms	A control to prevent errors in entry of repetitive data. Fixed elements of data are entered on processing forms in advance, sometimes in a format which permits direct machine processing.
Authorization	Limits the initiation of a transaction to selected individuals.
Cancellation	A control which identifies transaction documents to prevent their further or repeated use after they have performed their function.
Endorsement	Control technique marks a form or document so as to direct or restrict its further use of processing.
Simultaneous Preparation	Primarily manual control technique is the one time recording of a transaction for all further processing using multiple copies as appropriate to prevent transcription errors.
Documentation Manual	Control technique consists of written sets of standards to provide consistent communication.

Figure 5-6b, Page 1 of 4, CHARACTERISTICS WHICH CONSTITUTE CONTROLS

CHARACTERISTICS WHICH CONSTITUTE CONTROLS - 2

CHARACTERISTICS WHICH CONSTITUTE CONTROLS	EXPLANATION OF CONTROL
DETECTIVE CONTROLS	
Accountability of Input	
Anticipation	Controls are set up to expect a given event at a specific time.
Transmittal	Controls provide the medium for other controls over the movement of data, particularly from source to processing point or between processing points.
Batch Serial Numbers	Controls cover the completeness of data during and following the transmittal function. Batches of data are numbered and accounted for consecutively.
Completeness of Input	
Amount Control Totals	Totals of homogeneous, significant amounts in corresponding fields of records within a processing stream or file. An example would be totals of dollar amounts for invoices.
Document Control Total	A control covering the number of documents.
Line Control Counts	Counts applied to line-items within all documents of a transmittal. This control is typically applied to documents where line-items represent an important measure of volume, such as invoices or orders.
Hash Totals	Totals for processing controls only. They are applied to meaningless nonmonetary amounts, such as account numbers.
Batch Totals	In handling and error resolution, input transactions may be packaged in small groups. Any type of control amount, document, line or hash - may be applied to the transmittal of batches.
Completeness Check	A comparison of items actually processed with a control total. It is designed to assure completeness of processing.
Visual Verification	Control involves the visual scanning of documents for general reasonableness.
Turnaround Documents	Control involves using a computer produced document as an invoice, billing statement, etc., which is then re-input into the system after handling by the recipient. Use eliminates transcription errors and facilitates handling.
Approval Codes	"Stage of completion" or "review" technique involves the coding or mechanized signature or initialing by personnel as authorization for proceding to the next stage of processing or handling.
Correctness of Input	
Format	Format controls determine that data are entered in the proper mode - numeric or alphanumeric - within designated fields of information records.
Mandatory Data Present	Control is applied to assure that data entries are made in fields which cannot be processed in a blank state.

Figure 5-6b, Page 2 of 4, CHARACTERISTICS WHICH CONSTITUTE CONTROLS

CHARACTERISTICS WHICH CONSTITUTE CONTROLS - 3

CHARACTERISTICS WHICH CONSTITUTE CONTROLS	EXPLANATION OF CONTROL
Correctness of Input - Continued	
Legitimate Codes	A table or matrix of codes acceptable for processing is established. Coded fields within input transactions are compared with codes in the table. Only transactions with matching codes are accepted.
Check Digits	Characters within identification fields which are used to validate the appropriateness of the other characters within the same field. Check digits have no meaning of their own. They represent the result of calculations which determine that fields such as account numbers are valid.
Reasonableness	Controls apply tests to specific fields of data. This is done through comparison with other information available within the application.
Limit Checks	Controls test specified amount fields against stipulated high or low limits of acceptability.
Validity Checks	A control similiar to checking for legitimate codes, applied without use of tables or matrices. The characters comprising an indicative field are examined for a defined pattern of format, legitimate subcodes, or character values.
Read-Back	Control calls for immediate return of the information to the sender for comparison and approval.
Expiration	A limit check based on a comparison of current date with a date recorded on a file. The current date must be equal to or past the expiration date to permit processing.
Dating	Control involves a direct comparison between a current date set up in a computer program with dates recorded in transactions. Limit tests are applied according to reasonableness or expiration.
Keystroke Verification	The redundant entry of data into keyboards. The second entry verifies accuracy of the first. Differences between two entry procedures are identified and resolved.
Approval	A control which accepts a transaction for processing after the fact. Transactions are tested for specific conditions as a basis for approval.
Security Checks	Control technique involves the requirement for the entry of valid codes before processing (generally on-line) can take place.
Completeness of Processing	
Run-to-Run Totals	Control utilizes output control totals resulting from one process to establish input control totals or summary processing controls over subsequent processing. Full processing results of each step are validated. Run-to-run controls are likened to the forming of solid links in a chain.
Reconciliation	Control calls for identification of differences between the value content of two substantially identical files or between a detail file and a control total. The control total is frequently an accounting ledger balance.

Figure 5-6b, Page 3 of 4, CHARACTERISTICS WHICH CONSTITUTE CONTROLS

CHARACTERISTICS WHICH CONSTITUTE CONTROLS - 4

CHARACTERISTICS WHICH CONSTITUTE CONTROLS	EXPLANATION OF CONTROL
Completeness of Processing-Continued	
Balancing	A test for equality between the values of two equivalent sets of items or of one set of items and a control total.
Aging	An identification of unprocessed or retained items in files according to date — usually transaction date. Aging is by time frame, usually days or months.
Suspense File	A controlled location for retention of unprocessed items.
Matching	Matching of items from the normal processing stream of an application with others developed independently identifies items unprocessed through either of the parallel procedures.
Suspense Account	Technique establishes a control value for items awaiting further processing.
Clearing Account	An amount which results from the processing of independent items of equivalent values. Net control value should equal zero.
Tickler File	A control file consisting of items sequenced by age for followup purposes. Tickler files are usually maintained manually.
Periodic Audit	A periodic, internal verification of a file or of a phase of processing. It is intended to detect problems and encourage future compliance with control procedures.
Correctness of Processing	
Redundant Processing	A repetition of processing and an accompanying comparison of results. This control is applied to each item.
Summary Processing	A redundancy of processing using a summarized amount for comparison with a control total from detailed processing as a validation of results.
Sequence Checking	An identification check on items for continuity of processing. Sequencing verification can be ascending or descending. Control is over the order in which records are presented for processing.
Overflow Checks	A limit check based upon the capacity of a mechanical memory or file area to accept data.
Scanning Before Distribution	The scanning of output before distribution is a control to prevent obviously erroneous information from being distributed and used.
Discrepancy Reports	Periodic listing of exceptions for management review is a control which allows for correction or change as required of other procedures which are allowing the discrepancies to occur.

Figure 5-6b, Page 4 of 4, CHARACTERISTICS WHICH CONSTITUTE CONTROLS

ACTIVITIES SUBJECT TO CONTROL

ACTIVITY SUBJECT TO CONTROL	EXPLANATION OF ACTIVITY
Initiating	Creating transactions which will be processed on a system
Recording or Transcribing	Entering of data on any media — paper, cards, magnetic or paper tape, terminals, etc — i.e., coping it from one medium to another.
Formatting	Recording transactions in a standardized manner, usually on pre-printed documents.
Coding	Applying codes to indicate various status, processing options, etc., in an abbreviated manner to show which records, files and/or data elements will be changed or affected.
Transmitting	Moving of data from one location to another, e.g. control group to the accounting department.
Editing	Testing transactions for validity and reasonableness before they impact records and files.
Comparing or Selecting	Examining data for certain characteristics based on logical or conditional tests to determine or identify similarities or differences
Processing or Calculating	Performing various arithmetic or mathematical operations to change input to output, i.e., the series of steps that leads to the end result.
Correcting	Reprocessing data which was rejected because of some error condition, which actually begins again at the initiating activity
Terminating	Stopping processing or actions upon an item
Updating or File Maintenance	Changing information on a file, which usually contains cumulative transactions, with current activity transactions. The changes normally have a continuing impact on future transactions.
Summarizing	To combine detail items into a single, summarized total
Sorting	To resequence information
Reporting	To produce machine readable information in a format which may be read by a person

Figure 5-6c, ACTIVITIES SUBJECT TO CONTROL

Testing the Controls

The auditor, having obtained an "in-depth" understanding of the application, must now test the application controls.

There are three steps in the testing phase:

- Select the verification method and technique
- Determine whether use will be made of the computer
- Perform the tests.

Select the Verification Method and Technique

In general two approaches can be applied in verifying processing in an application:

- *Verifying Results of Processing* — selecting one or more key files which are produced by the application and verifying the accuracy of the results of the processing

  Verification of results is usually performed by one of three methods as discussed earlier:

  - Confirmation
  - Comparison
  - Reasonableness and edit tests

  Verification of results of processing may be done *either manually or with the computer* using custom designed audit programs or generalized audit software.

- *Verifying Phases of Processing* — performing specific tests of critical processes and controls using one of the audit tools and techniques discussed earlier, i.e., by employing:

  - Auditing around the computer, the traditional manual approach
  - Program listing verification, i.e., manually reviewing program code listing
  - Program logic flowchart verification, using program flowchart software
  - Test data approach, using manually prepared or test data generator software generated test data

- The integrated test facility approach, an extension of the test data approach

- Parallel simulation, using custom designed computer programs or generalized audit software

Verification of phase of processing is divided into verification of:

- *Manual processing* – verify manually, or with the computer if complex or voluminous

- *Program, i.e., computer processing* – through use of one or more of the audit tools and techniques previously discussed.

Determine Whether Use Will Be Made of the Computer

For either of the above approaches, i.e., verifying results or processing, the auditor must determine if he will utilize the computer in performing his tests. The tools available if the computer is used are program flowchart software, test data generators, custom designed computer programs and audit software.

Perform the Tests

Using the tools and techniques selected from those above, the auditor next performs such compliance tests as are required in the circumstances to verify that the controls previously disclosed for the application are in fact working properly. The supervising auditor must carefully review subordinates' work at this point in the internal control evaluation.

Evaluate Results of Review and Tests

As previously stated, a final, thoroughly documented determination must be made by the auditor on the adequacy of existing controls. Any exposure resulting from weak or non-existent controls must be evaluated by the auditor as he defines the scope of his substantive test procedures.

Report on Results of Review and Tests

This is the summary, the end result, of all of the computer audit efforts of the auditor. The auditor should prepare a constructive letter of comments to be given to management which discusses the results of the review and recommendations for improvement.

Because the auditor may be somewhat unfamiliar with all the ramifications of control of a computer system, it is possible that he may recommend something that is impractical, impossible, erronous, etc. All detailed recommendations should *always* be reviewed with

appropriate data processing personnel before the formal recommendation letter is issued.

The report should be issued in the following format recommending revisions in the computer system:

- The objective and scope of the review
- The nature and extent of tests performed
- A general description of the control strengths and weaknesses or efficiency factors found
- One or more examples that support the finding
- An explanation of the control improvement or efficiency changes desirable
- A recommended action to be taken.

AUDIT OF THE INSTALLATION

In practice, the installation review is performed before application and/or system development reviews. The objective of the installation or computer operations center review is the verification of effective implementation of the controls discussed in Section III.

Initially, the auditor reviews summary information about installation activities in order to obtain a preliminary understanding of the size and complexity of the overall data processing function. Only then can he determine the tentative scope of audit work necessary in the installation, applications, and application/system development areas.

Overview of Steps in Starting the EDP Review and Completing the Installation Review

Figure 5-7 presents the primary steps in starting the overall EDP review and performing the review and evaluation of installation controls, while in the process setting the tentative scope of application reviews and development process reviews. In summary, these steps are:

- Obtain an initial understanding of the size and complexity of the EDP function by obtaining and reviewing summary information about the installation, its people, organization, hardware and software, applications, and physical layout.
- Review this information and evaluate its impact on overall audit scope and set tentative scope of installation, application, and development process reviews.

- Determine the policies and practices in each segment of the installation through examination of informational documentation, interview various personnel to supplement this understanding of policies and practices, and prepare supplemental audit documentation as required.

- Determine which installation controls are critical to overall audit objectives and the tentative scope of application and development reviews.

- Determine the technical proficiency necessary to perform the various areas of test work, select the verification technique, and perform compliance testing.

- Evaluate the results of the compliance testing in relation to the scope of substantive testing, finalize the scope of application and application/system development reviews, and report on results of the installation review.

The above steps are expanded upon below. In addition, specific segments of the review are covered in later parts of this section.

Obtain Initial Level Information About Data Processing

To set tentative review scope, the auditor must obtain and familiarize himself with the following types of information about the installation and its activities:

- Its organization in respect to the total company organization and the number and classifications of personnel

- The type and size of the computer and related peripheral devices. This is similar to obtaining basic financial information about a company, e.g., profit and loss reports, amount of sales, etc.

- The type of operating system, primary programming languages and software and/or data base management packages used. This is similar to obtaining information on the company's methods of accounting

- A listing of applications with some indication of their size (and copies of control reports for key applications) both presently being processed and under development. This is similar to determining what accounting activities take place in a company, e.g., cash receipts, disbursements, order entry processing, etc.

- Operating and budget information broken down to show expenditures for equipment, people, etc., and by the expenditure of

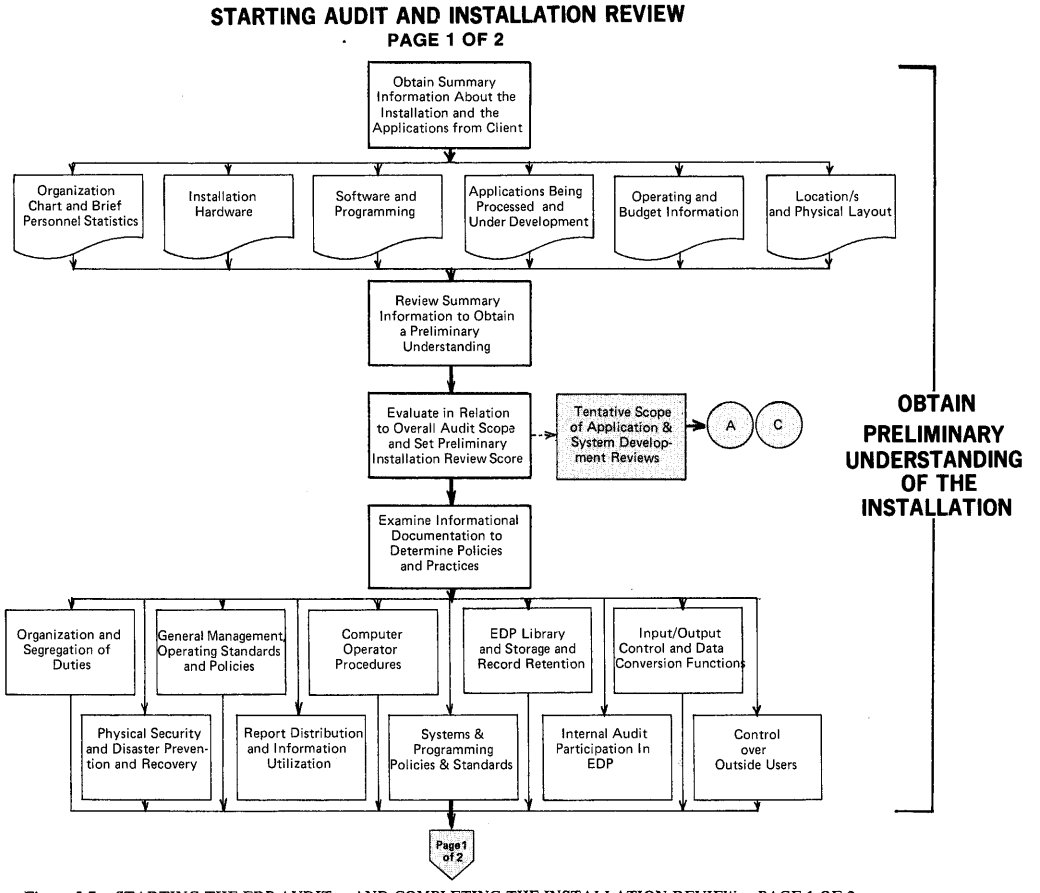


Figure 5-7 STARTING THE EDP AUDIT – AND COMPLETING THE INSTALLATION REVIEW – PAGE 1 OF 2

STARTING AUDIT AND INSTALLATION REVIEW
PAGE 2 OF 2

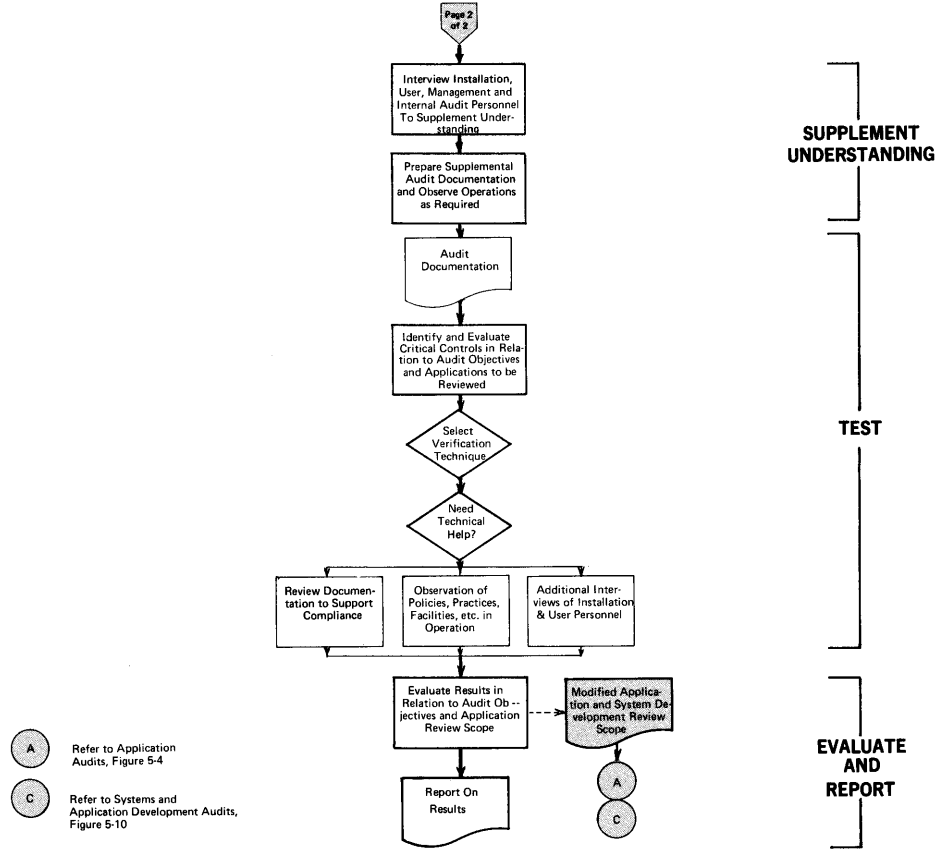


Figure 5-7 STARTING THE EDP AUDIT – AND COMPLETING THE INSTALLATION REVIEW –Page 2 of 2

computer time such as regular applications, testing, etc., and copies of installation reports on equipment scheduling and utilization.

- A sketch or description of the physical layout of the department and computer room(s). This is similar to reviewing a floorplan of a warehouse or plant prior to an inventory observation.

This information should be readily available from the client.

Obtain Preliminary Understanding of Overall EDP Function, Evaluate, and Set Scope of Reviews

The summary information must be reviewed and evaluated to determine the tentative scope of the installation, application, and application/system development reviews. The tentative decision on scope must, of course, be made based on an evaluation of the tentative size and complexity of the installation and the controls in the installation in respect to the overall audit objectives.

From a practical standpoint, if more than one person is involved in the overall installation review, the application audit work will normally start in parallel with the remaining installation review work, but should not be finalized until the installation results have been obtained.

Examine Informational Documentation to Obtain Preliminary Understanding of Computer Center Policies

The auditor next obtains informational documentation on the policies and practices of the various segments of the computer operations center and related activities, e.g., organization and segregation of duties, general management, etc., as shown in Figure 5-7.

The documentation to be examined and the audit work to be performed in each of these segments are discussed in more depth later in this section.

Interview to Supplement Understanding and Prepare Supplemental Audit Documentation

The primary method of determining policies and practices in the installation review is examining documentation of an informational nature. However, all policies and practices may not be documented. Therefore, interviewing of personnel (installation, users, management, and internal audit) may be required to complete the understanding of the policies and practices in the installation. Upon completing interviews and observations, the auditor should prepare such supple-

mental audit documentation as is required to document his understanding of the installation.

Identify and Evaluate Critical Controls in Relation to Audit Objectives and Applications to be Reviewed

Having obtained a complete understanding of the installation's policies and practices, the controls critical to the overall audit objectives and the tentative scope of application audits and application/system development work must be identified, i.e., selected, and evaluated. Inadequacies in policies and procedures and/or defects in controls must be measured to determine the degree of exposure they create and the impact they will have on further substantive audit tests. Any such exposures relate directly to the quality of implementation of virtually all controls within the installation.

Determine Technical Proficiency Required and Test to Verify Understanding

The auditor assigned to the review must evaluate his own technical proficiency in respect to the size, sophistication and complexity of the installation, its more complex and technical areas, and the scope of the test work to be performed. Assistance on the more technical areas may be required from a qualified EDP technician on the audit firm's consulting staff.

Unlike the application audit, where a variety of tools and techniques may be utilized, there are three basic verification techniques applicable in the installation area:

- Review of documentation supporting compliance, i.e., items which verify adherence to policies, practices, and controls
- Interviewing additional personnel
- Observation of activities and operations

Review Documentation Supporting Compliance

The primary verification technique for many areas of the operation center is a review of documentation supporting compliance of prescribed policies, procedures, and controls. This includes supervisory signatures or initials on console logs evidencing supervisory review, daily work schedules, examination of library logs on files in and out, and so forth.

Interview Additional Personnel

Most computer operation center controls should be verifiable through documentation examinations or through observation of activities. Interviewing as a verification technique is primarily applicable in the administrative efficiency/control areas where there should be "user and installation" or "internal audit and installation" liaison – or to determine practices where documentation is inadequate.

Observation of Activities and Operations

Certain controls can be verified only by observing that they do take place or do exist. Several short periods of time, e.g., 1-2 hours at a time on an unannounced basis, should be scheduled and utilized to observe activities and operations such as; that machine readable media do contain external labels, that the library is not open to unrestricted access, that file protect rings are removed from tapes, that supervisors are periodically in the computer room, etc.

Evaluate Test Results in Relation to Audit Objectives and Application and Development Process Review Scope

The results of compliance tests, the existence and adequacy of controls, must be evaluated in relationship to their impact on overall audit objectives, and the tentative audit objectives previously established for application and application/system development reviews. Inadequate controls must mean an appropriate adjustment to subsequent substantive audit tests.

In evaluating the results of tests, the auditor must clearly separate administrative vs. accounting controls. If accounting controls are inadequate he must further see that compensating controls exist and work or do not exist. Finally, of course, the auditor should report on the results of his findings in a letter of recommendations, similar to the format discussed previously for applications.

Segments of the Installation Review and Audit Work to be Performed

Each of the segments of computer center operations and certain related activities shown in Figure 5-7 are discussed below. The auditor's concerns and procedures in respect to documentation, interviews and observations for each of these segments are also summarized in Figure 5-8.

Organization and Segregation of Duties

To understand the organization, the auditor should review:

- Corporate and departmental organization charts
- Manpower and overtime reports
- Job descriptions.

A primary concern in this area is the segregation of duties as it affects both working efficiency and potential conflicts of responsibility. The auditor should determine that there is proper segregation of duties, as previously discussed in Section III.

Observation is the primary verification technique in the organization area because there will be no audit trail to support adherence to documented standards.

General Management and Operating Standards

The auditor should become familiar with the quality of management standards as documented in internally created reports. The auditor should review the following types of management reporting on EDP operations to determine that there is adequate planning and supervision of operation:

- Processing logs
- Daily, weekly, etc., operations schedules preauthorizing computer use
- Reports on completed jobs processed
- Reports on nonproductive machine time
- Summary performance statistics based on detailed reports listed above
- Payroll and overtime reports
- Operator rotation and vacation schedules
- Budgetary results, i.e., forecast to actual.

During documentation reviews or interviews the auditor should particularly note whether supervisory personnel do plan, or review planned computer use in advance – and that they subsequently review plan to actual and follow up on any exceptions. This is a prime preventive control. In the observation phase the auditor should note the typical availability level of management personnel in the computer center and the degree to which activities in the computer area may be

AREA OF CONCERN	DOCUMENTATION	INTERVIEWS	OBSERVATIONS
Organization and Segregation of Duties	Corporate and department organization charts. Manpower and overtime reports. Job descriptions.	Interview senior management personnel and prepare own organization charts and other documentation.	Verify lines of reporting, job descriptions, and separation of responsibilities.
General Management, Operating Standards and Policies	Processing logs. Daily operations schedules. Reports on completed jobs. Summaries of above.	If documentation inadequate, interview EDP operations management to identify any compensating controls. Develop awareness of capacities and costs as a basis for evaluation of utilization of resources.	Note availability of managers in computer center. Note degree to which management can observe operations.
Computer Operator Procedure	Operator logs. Error reports.	Not appropriate.	Series of brief, unannounced visits spread over all shifts. Observe neatness and orderliness of installation and such procedures as file handling, cleaning tape heads, accepting inputs, etc.
EDP Library and Storage and Record Retention	Library log of file, program, etc. in use Records of data files Records of disks and tapes Record retention policy statement	Interview management about IRS Ruling 71-20 agreements	Observe how files and programs are handled Observe accessibility of library, during all shifts.
Input/Output Control and Data Conversion	Analytic flow chart depicting control group activities. Console and operator logs. Conversion instructions Error reports	Interview users to determine if controls are being applied. Interview users to determine satisfaction level with equipment reliability and error resolution	Observe control group functions. Verify correction of errors in course of other duties.
Report Distribution and Information Utilization	Report schedules.	Interview users on adequacy of distribution.	Not appropriate.
Equipment and Software Reliability and Utilization	Records for utilization, cleaning, and recertification to tapes and discs. Preventative maintenance controls and logs.	Interview users to determine satisfaction level with equipment reliability.	Observe presence and use of temperature and humidity control devices.
Physical Security Disaster Prevention and Recovery	Plans of action. Certificates for devices. Contingency plans. Arrangements for backup facilities. Documented test procedures which have been performed on backup facilities. Fidelity insurance. Insurance for equipment damage. Insurance for reconstruction costs. Business interruption insurance. Duplicate application documentation.	Interview fire prevention personnel. Appraise quality of preventive measures and exposure. Interview management to identify and describe undocumented recovery facilities, plans, or arrangements.	Observe segregation of computer facility, access controls, protective equipment, and library controls over files. Visit night shift. Examine file labels. Observe off-premises backup files and facilities. verify usability.
Systems and Programming Policies and Standards	---------- Refer to discussion in Chapter 17 ----------		
Internal Audit Participation in EDP	Reports of work performed. Internal audit working papers.	Interview internal audit on level of particpation and findings in work performed.	Not applicable except to see internal audit does not participate in day-to-day control activities.
Control over Outside Users	Copies of Agreements. Billing procedures. Operating reports.	Interview EDP manager to determine if there are other outside users.	During routine observations, note third party job handling procedures, if appropriate.

Figure 5-8 AREAS OF CONCERN AND TECHNIQUES IN AUDITS OF EDP OPERATIONS

observed by supervisory personnel from within their offices.

Computer Operator Procedures

Operator activities should be conducted in an efficient, orderly manner. Verification of operator procedures is primarily through observation as the major documentation available for operating practices is usually limited to operator schedules and logs, and error reports. The auditor should address his verification techniques to the following areas:

- Adequacy of supervision of operators
- Operator access to program documentation or general purpose utility programs that allow changing files
- Magnetic tape and disk file labeling procedures (both internal and external)
- Use of file protect rings on magnetic tapes
- Control over error corrections, output distribution, and utilization
- Quality of operator personnel
- Housekeeping – i.e., a neat and orderly computer room
- Adherence to manufacturer's preventive maintenance programs

The EDP Library, Storage and Record Retention

The library records discussed in Section III should be reviewed to determine accountability of files and programs, for indications of problems or inappropriate use of media, programs, etc. The auditor should also observe library procedures during all shifts to determine that proper standards are maintained.

The auditor should also determine the client's file retention policy for both printed and machine readable media. In addition, he should determine whether or not the Internal Revenue Service has performed a review under Revenue Ruling 71-20 of the client's file retention program and should obtain a copy and review it if such an agreement has been completed.

Input/Output Control Group and Data Conversion Functions

These areas are covered together as they are directly related and are often reviewed by the auditor at the same time. The functions of the

I/O control and the data conversion groups are reviewed at two levels by the auditor. During the installation review, he establishes what the general policies and practices are in respect to this function, i.e., the accountability of data from receipt through data conversion, processing, error correction, and re-entry and final distribution of output. During application reviews, he goes into further detail on the I/O control function, and how it, or its equivalent, performs in respect to specific applications.

Existence of an I/O control group is itself a major preventive control. Its function of applying detective controls to insure accountability of all data at all times and to insure proper resolution of errors is of paramount importance. Documentation the auditor should review at the installation level includes:

- Balancing logs and control sheets
- Edit reports
- Written instructions for error conditions
- Operator and console logs for handling of errors
- Written instructions for data conversion and policies on major data field verification, e.g., key verification.

Report Distribution and Information Utilization

The auditor's prime concern in this area is to see that there is control over the distribution of information and that information is distributed on a timely basis. He should examine output distribution, control schedules and, in the process, determine that procedures for review of output before distribution for gross errors are functioning. Sensitive documents and confidential information should also be under adequate control to assure that only the proper persons receive them.

Operating Hardware and Software Reliability and Utilization

To a substantial degree, the auditor can rely on controls built into the equipment and software by manufacturers. Further, this is primarily a technical area requiring specialized, technical review expertise. However, the auditor should ascertain that controls over files require that complete records be maintained covering utilization, cleaning and recertification of tapes and disks. He should further see that humidity and temperature standards are adhered to at all times, and can examine logs and controls over preventive maintenance.

Physical Security and Disaster Prevention and Recovery

Management's – and the auditor's – concern in the area of preventing disasters, accidents, theft and other malicious acts, is to satisfy himself on the safeguarding of information assets and the continuity of EDP operations in such event. The auditor will normally review this area at both the installation and application levels. Documentation in this area is usually scarce, consisting chiefly of plans of action in the case of disaster and evidence of offsite storage of programs and key files. The documentation which should be examined (a copy of which should also be offsite) should include:

- Plans of action in the event of disaster, including a set of priorities on what must be done in which order

- Evidence covering protective devices and offsite storage of current key data and master files, programs, operating systems and all related documentation

- Arrangements for backup, for alternative facilities, including documented test procedures which have been performed on backup facilities and plans for rapid replacement of the installations facility and hardware

- Insurance in respect to damage and other types of loss including employee fidelity; errors and omissions; equipment and facility damage; reconstruction costs on facilities, programs, data etc.; and business interruption.

The auditor should also observe the general security and access aspects of the installation and the vaults and other storage facilities for on-premises retention of files, etc., to determine if they are secure and appear to have proper protective capacity.

Systems and Programming Policies and Standards

The size, sophistication, and functions performed by this activity vary widely between installations. Due to the nature and potential complexity of this activity, it is covered separately in the next section. In that section the auditor will see that a clear distinction must be made between:

- The minimum audit review level at the installation level of general policies, practices, and controls exercised over the systems and programming function, and

- The full audit of the application development process, the prime topic of the next section

Internal Audit Participation in EDP

Active internal audit participation, particularly in the financial controls segment of EDP, is itself an internal control strength. The auditor should interview internal audit personnel, and determine the level of their participation in EDP activities and review documentation of internal audit staff work in respect to EDP. He should then consider the impact of their work on his overall evaluation of internal control. The areas of participation to consider are:

- The planning and development phase of applications
- Review of applications under development for inclusion of proper controls and audit trails
- Participation in the testing and conversion phases of application implementation
- Implementation of new controls in existing applications resulting from reviews of applications currently in process
- Periodic review of controls such as organization and segregation of duties, functions of the I/O control group, error and exception handling, etc.

Control Over Outside Users

Many organizations have some excess computer capacity which they attempt to sell to help cover equipment costs. If the installation does this, the auditor should examine the controls over billing procedures; installation security, program security and file security; and should review operating procedures in respect to outside users' use of the installation.

Administrative Control Concerns Within EDP Organizations

The auditor's attention in the examination of the computer operations center deals mainly with accounting controls for applications with financial materiality. However, a review of the operations center also offers opportunities for the auditor to make recommendations in the areas of improving overall operational efficiency and administrative control. The following primarily administrative control areas normally fall within the scope of the examination of EDP operations:

- Organization and segregation of duties
- Supervision and management reporting

- Operator procedures
- Data and information utilization
- Equipment reliability and equipment and software utilization
- Use of facilities by outsiders.

The auditor's exposure to a variety of computer installations, the experience gained through the use of generalized audit software and his experience in management practices will often allow him to note areas for improvement in administrative control. Underused or unused equipment or reports, unused data fields, organizational conflicts, and the potential for combining separate but related files, e.g., payroll and personnel, are examples. The auditor must, however, be constantly alert to the requirements for technical proficiency and technical help in many of the administrative control areas of a computer operations center.

SYSTEMS MANAGEMENT AND THE AUDITOR

The principal effect of a company's systems and application development mechanisms on audit activities lies in preventing omission of adequate controls during the application maintenance process and during the development of new applications. In total, the systems development and maintenance process, i.e., the function of the systems and programming staff, constitutes a preventive control.

The "Systems Audit" is Several Things

The size of and functions performed by the "systems and programming" group varies widely between installations. Because of this, the auditor must clearly understand that the audit of the systems process can be more than one thing. Further, he must understand the level of audit expertise required and the relationship of the roles of the internal and external auditor in audit activities in this area.

As pointed out previously, several levels of audit work may be required in this area:

- A minimum audit review level at the installation level of general policies, practices, and controls in the systems and programming function with verification of controls being performed through an application audit – because of the impact that this function *can have* or *could have had* on applications in process of development or recently developed, i.e., a *detective control* review.
- An audit of the complete *development process – the primary*

subject of this part of Section V – either:

- Retrospectively – looking at applications developed in the past to determine changes needed in the future in the development process to assure the inclusion of adequate controls, i.e., a *detective review,* or

- Prospectively (or currently) – examining the application development process by looking at applications in the process of development to assure that adequate controls are included as the development and implementation process progresses, i.e., a *preventive control* review.

As the steps in the retrospective and prospective reviews are essentially the same except for timing, they will be treated as one and the same in the remainder of this section.

Overview of Steps In the Review of Systems and Programming and the Application Development Process

Figure 5-9 presents the primary steps in the review of the systems and programming function in the application development process (if it is undertaken). Summarized, these steps are:

- Obtain an initial understanding of the system and programming function's activities during the installation review and evaluate it in relation to overall audit scope to set the preliminary "systems" audit scope

- Examine informational documentation to determine policies and practices of the function, supplementing these findings with interviews of various personnel where necessary

- Identify, i.e., select, and evaluate the controls critical in the circumstances in this activity in relation to overall audit scope and the initial scope of application reviews (set during the initial overall installation review) and establish the scope of required compliance testing

- If overall audit objectives and earlier findings call for a detective control review, verify the adequacy of controls through an application audit as explained previously in Section V

- If overall objectives in earlier findings call for a preventive control review (with or without internal audit staff assistance), select applications to review and test, select development process steps to be tested, and determine the technical proficiency required to perform the tests

- Evaluate the results in respect to applications developed and in the process of development and prepare a report on findings.

The External Vs. Internal Auditors' Roles in the Systems Audit Process

Before expanding upon the above steps, it is important to understand who normally does this work. The external auditor must at least participate in the minimum audit review of policies and practices of the systems and programming staff. This review will determine whether a detective or preventive control review is necessary, i.e., application vs. development process audit.

Direct participation in the audit of the application development process may be, in some cases, beyond the scope of the external auditor. However, where an application under development will have a major impact on the client's financial statements, the external auditor should be available for consultation at key accounting control points within the project. In contrast, the internal auditor should be closely and continuously involved in his company's systems development process. As indicated before in the installation section, the internal audit staff should participate in the development of each major application.

Steps in the Review of Systems and Programming and the Application Development Process

The items below expand on the overview of the steps above.

Obtain Initial Understanding of the Demands on the Systems and Programming Function

Information about the size of the installation and its systems and programming function, its organization and personnel, and applications implemented and in process of development obtained during the initial installation review will give the auditor a good overview of the demands on the systems and programming function. A review of this information in conjunction with overall audit objectives should enable the auditor to set the tentative scope of the "systems audit," or determine whether one is required at all.

Examine Informational Documentation and Interview to Determine Systems and Programming Policies and Practices

As systems and programming activities should be governed by well documented, current statements of policy, standards, procedures, etc., the auditor should first obtain and review informational documentation to determine such policies, etc., in each of the four major segments of activity:

APPLICATION DEVELOPMENT

Page 1 of 2

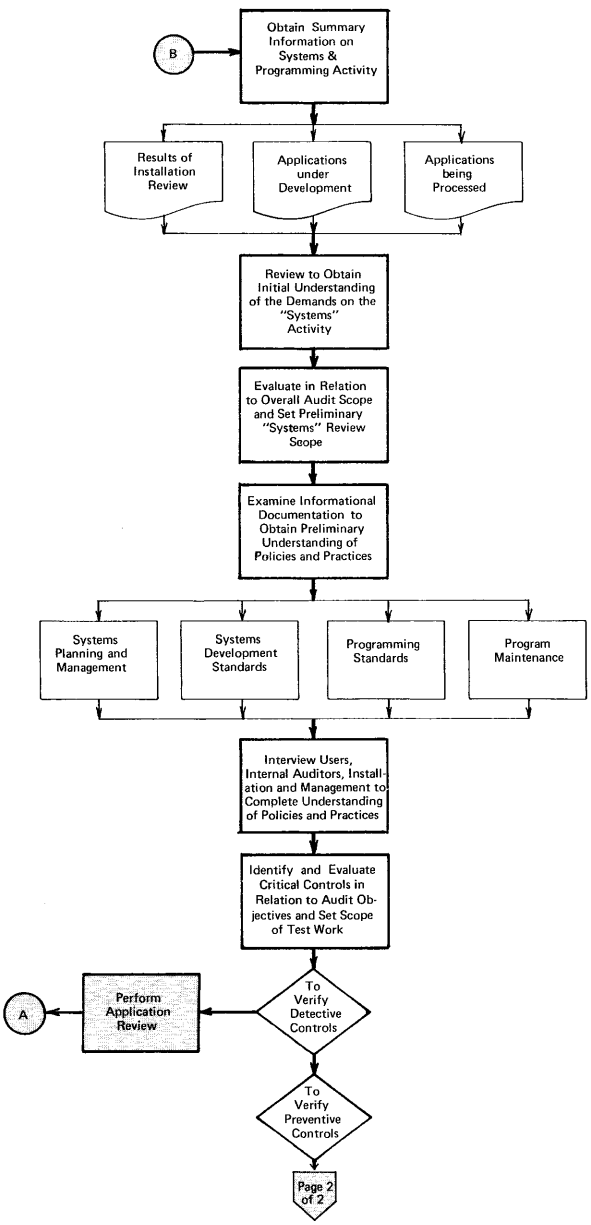


Figure 5-9 DETERMINING APPLICATION DEVELOPMENT AND MAINTENANCE STANDARDS AND PRACTICES
Page 1 of 2

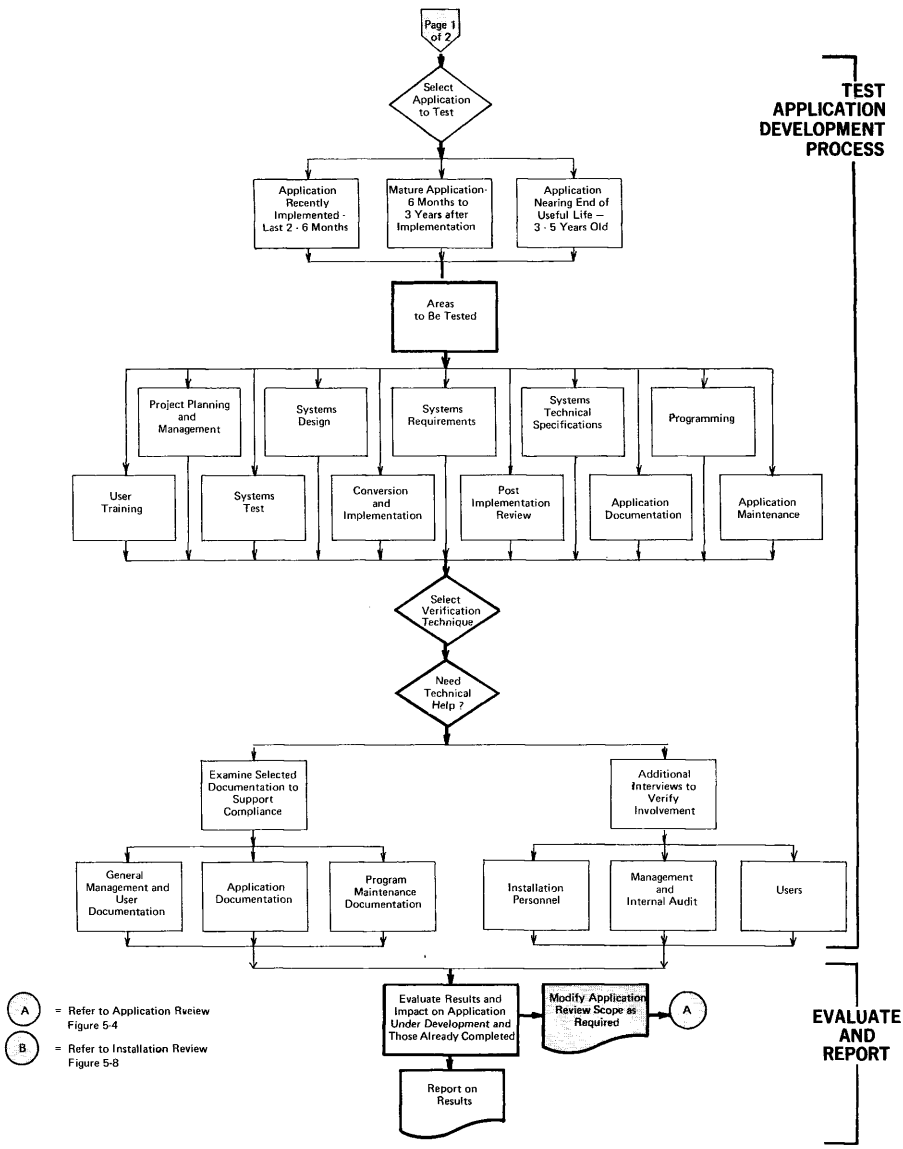


Figure 5-9 DETERMINING APPLICATION DEVELOPMENT AND MAINTENANCE STANDARDS AND PRACTICES, Page 2 of 2

- Systems planning and management
- Systems development standards (i.e., methodology and control)
- Programming standards
- Program, systems and application maintenance – which in the typical EDP audit engagement is the most important of these four areas to the auditor.

The primary documentation to be examined will normally be a systems and procedures manual or similar written statements of policy. Interviews of installation, user, management, and internal audit staff personnel may then be required to complete the understanding of policies and practices, depending upon the detail included in the systems manual.

Identify and Evaluate Controls Which Are Critical in Relation to Overall Audit Objectives and Set Scope of Compliance Testing

With an understanding of the systems and programming function, the auditor must select those controls which have an impact on the scope of his substantive tests and determine necessary compliance testing. In addition to well defined, documented policies and standards, a most important control in a systems and programming project is thorough review and approval at well-defined project checkpoints. Each project phase should have a specified end-product which is subjected to review and approval by all concerned parties before the next phase continues. If the client has defined checkpoints and end-products, compliance can be readily verified through examination of the approvals on such documents as work assignments, status reports, comparison of progress schedules with original objectives and schedules, feasibility studies, costs vs. benefit studies, user approval and signoff, etc. If no such definitions exist, other controls are not likely to compensate.

The external auditor's first concern should be the quality and control features of the general systems and programming methodology and application maintenance procedures within the company. Second, he should be concerned that project controls provide for satisfaction and specifications within tolerable costs, at least to an extent that assures completion and implementation of complete and adequate controls.

Determine if a Detective or Preventive Control Review is Needed Based Upon Earlier Findings and Overall Audit Objectives

If the overall audit objectives are limited to examining material financial applications currently being processed (as is normally the case) and

if systems and programming controls do not appear to be weak or inadequate, a detective, i.e., an application review, should be performed. To verify that systems and programming controls are working properly, the auditor should perform application verification procedures as previously covered in the "Audit of Applications" section. He would incorporate the results of the systems and programming "critical controls" review into the establishment of the scope of application verification procedures as required in the circumstances.

The *prospective, i.e, preventive review (the primary subject of the remainder of this section)* will not provide a basis for the evaluation of accounting controls applied over a historical period under review. Therefore, initiating a preventive control review of the development process will be requested by the client or will result from an expansion of review scope because systems and programming controls do appear to be weak or inadequate. The objective of the review would be to provide suggestions for improving the client's systems and application development process.

There are several alternative approaches to a preventive review including:

- The external auditor does it independently of other review areas as a special service at the client's request
- The external auditor does it all – the internal auditor does it all – or it is done by a team composed of both.
- Applications selected for review (mainly retrospective reviews) could be combined with the application audit work previously discussed and a combined, modified review scope encompassing both the application audit verification procedures and development process review could be performed.
- Applications can be selected and reviewed in respect to the development process in addition to those reviewed during the application audit to supplement the findings of the application audit review.

Irrespective of the type of review, or who does it, the steps in the examination of application and systems process are:

- Obtain all applicable documentation prior to beginning the review to facilitate it moving smoothly

- Select a cross section of applications to be tested if a retrospective review is being performed

- Determine the areas within each application, either part or all to be tested

- Select the verification technique to be used, evaluate the auditor's own familiarity with the development process, determine the technical proficiency required to perform these verification techniques and perform the procedures.

- Evaluate the results, the impact on applications audit scope, and report on the results

These areas are expanded upon later in this section.

The two primary techniques are much the same as previously discussed:

- Examine selected documentation to support compliance with policies

- Interview additional personnel to verify compliance and involvement on the part of users, management, internal auditors, and so forth with the various development phases

Having covered the steps in the review, the areas to be reviewed will be covered in the following sections. As this work is intended as only a summary and not a detailed study, the areas to be reviewed will be commented upon very briefly. The reader is referred back to Section IV to Figures 4-2 (a) and (b) and 4-3(a) and (b) for the control aspects and documentation involved in each of the areas below. For a further description, refer to the full text.

Project Planning

This area of the systems and application development process deals with primarily administrative controls rather than accounting controls, but the auditor should perform his review to at least ascertain the installation's future plans, evidence of sound management planning and judgment, and management review and control. Documentation which should be available for audit review to support project planning efforts should include:

- Formal descriptions of functions and duties of corporate level committees responsible for planning

- Plans for future EDP facilities and applications
- Samples of feasibility studies and related cost/benefit studies used to justify current facilities and applications.

The auditor's main concern is that adequate business perspective – with adequate management contact and review – is exercised in the planning phase.

General Systems Development Methodology

Systems development methodology should be based on a series of discrete steps that can be described, planned, and evidenced by appropriate documentation. The auditor's review of the general systems development methodology and standards within an organization should determine levels of management and controls prescribed in developing and implementing applications.

System development project documentation which the auditor should review should consist primarily of formal standards, such as:

- Systems design procedures
- Programming conventions, procedures, or documentation
- Flowcharting conventions
- Standard operating procedures
- Organization control procedures
- Project planning and management.

The remaining steps on the flowchart in Figure 5-9 to be examined are really parts of the overall systems development methodology. They are explained briefly below. (The reader should note that the names of each of the phases of the system development process may vary widely from installation to installation. The phases described below are parts of the Touche Ross & Co. Systems Management Process. Regardless of what the phases are called, the auditor is interested in certain items in each).

Systems Requirements Phase

Systems requirements is a statement in non-technical but detailed terms of:

- What does the system have to accomplish, i.e.:
  - What is the problem to be solved?
  - What is the solution, in business terms, understandable particularly to users of the planned system?

Systems/Technical Specification Phase

This phase is a translation of the problem and solution statement from a business to a technical language to a level necessary to communicate with programmers.

Implementation Planning

Following the preparation of detailed specifications in both user and technical languages, the balance of implementation of an application can be planned with a significant degree of reliability.

This phase is not shown on Figure 5-9 as it is not often used or is considered an adjunct to overall project planning and management. However, its purpose is obvious – detail plan the rest of the project. It is included here so that the auditor will understand the term if he hears it and will realize the planning phase is a continuous one. This is also a major control review point since all controls have been specified for conversion and ongoing operation. A review at this point can serve well as a guide to audit participation and examination after implementation.

Programming Phase

This step converts the technical specifications to an operational, tested computer (i.e., "machine") language complete with operational instructions. Programming should begin only after the above steps are performed.

User Training Phase

This includes the preparation of procedures for the conversion and operation of the new system. It is performed by the users themselves to insure that they fully understand the new system.

Systems Test Phase

This is the "make it fail" stage of extensive testing. Care should be exercised to insure that an appropriate range of valid and invalid transactions are tested and results are properly evaluated.

Conversion and Implementation Phases

This is the conversion of data, equipment, procedures and personnel for the new system. It must be performed within a carefully planned and controlled environment to prevent a breakdown and to insure the implemented new system yields satisfactory operating results. The new and old systems are often run "in parallel" until the new system is proven and accepted by users.

Post Implementation Review Phase

A review should be made by users and the installation after a new system has been operating for a period of time to insure that all functions of the system are operating as specified and that the systems development methodology itself was operating satisfactorily.

Application Documentation

Even though there has been a separate discussion of application documentation in the "Audits of Applications" section preceding, some consideration of documentation is also advisable as part of the review of the development process. In reviewing applications under development, the auditor should review documentation such as the following, which the auditor should determine is available for each application:

- A narrative description of the application
- A current system flowchart
- Instructions for computer operators
- File specifications and record layouts for all records in all files shown on the system flowchart
- Listings of all transactions used, together with explanations of edit rules and their impact on files and fields
- Descriptions of all input documents and machine readable interpretations, as indicated on the system flowchart
- Logic-level flowcharts and/or decision tables for all logic steps indicated on the flowchart – or the availability of software which will generate logic-level flowcharts as needed
- Formal documentation of system testing indicating acceptance by all parties associated with the application.

In addition to the above, the auditor should see that two more

technical types of documentation are available for each application. The auditor may also need to review these two types of more technical application documentation. The need for this depends upon the complexity of the application under review, the level of detail to be examined, and the tool or technique to be used in the testing phase. They are:

- Program specifications for all job steps on the application flowchart

- A current set of source code listings for the application programs – or program decks which can be converted readily to provide such listings.

The real purpose of thorough documentation, with regard to control, is to provide a medium for supervisory review and approval. In addition, it facilitates accurate logic, simplifies programming, and assists future maintenance. Without effective supervision, the quality of the application system is substantially dependent on the care and ability exercised by the individuals engaged in the development project. Such reliance may not be justified.

Application Maintenance

Application maintenance is the common term applied to any continuing work on the application after implementation is complete. The auditor should be mainly concerned with the reasons for and documentation of application change – and particularly with user and management approval of change. Application maintenance documentation is usually more scarce than initial application documentation, because changes to systems are usually made under pressure circumstances, and little concern is given to documentation. Also, correcting programming errors is usually a more error-prone activity than initial application programming.

Application maintenance that the auditor should normally find available (and should review) for each ongoing application will include:

- Narrative descriptions of application changes

- Statement of reasons for and the intended effects of changes

- The date changes were implemented

- Signed authorization for changes

- Numerical controls covering changes

- Documentation of tests performed before implementation of changes

- Appropriate revisions to all previous documentation affected by application changes.

In examining application maintenance documentation, the auditor should also note if users have indicated, where appropriate, their approval of changes. This may also be done through interviewing users. Poor program maintenance and/or development practices can usually be identified by many user complaints and reruns of programs.

A program maintenance verification technique for controlling programs and being able to quickly determine if there have been changes is also available to the auditor. On key applications, the auditor may obtain and maintain independently a control copy of the program. Periodically, he will compare the control copy to the actual running program in the installation. This comparison may be done manually (through examining program listings produced from the two program decks) or mechanically. Software is now available which allows the auditor to quickly compare the two program decks, the installation's and his control copy, and produce a list of changes, if any.

Finally, the auditor should interview the data processing manager and discuss all changes effected during the period of examination, with particular emphasis on those which may have impacted material applications.

* * * * *

Figure 5-10 graphically shows a summary of the phases of the entire systems development process.

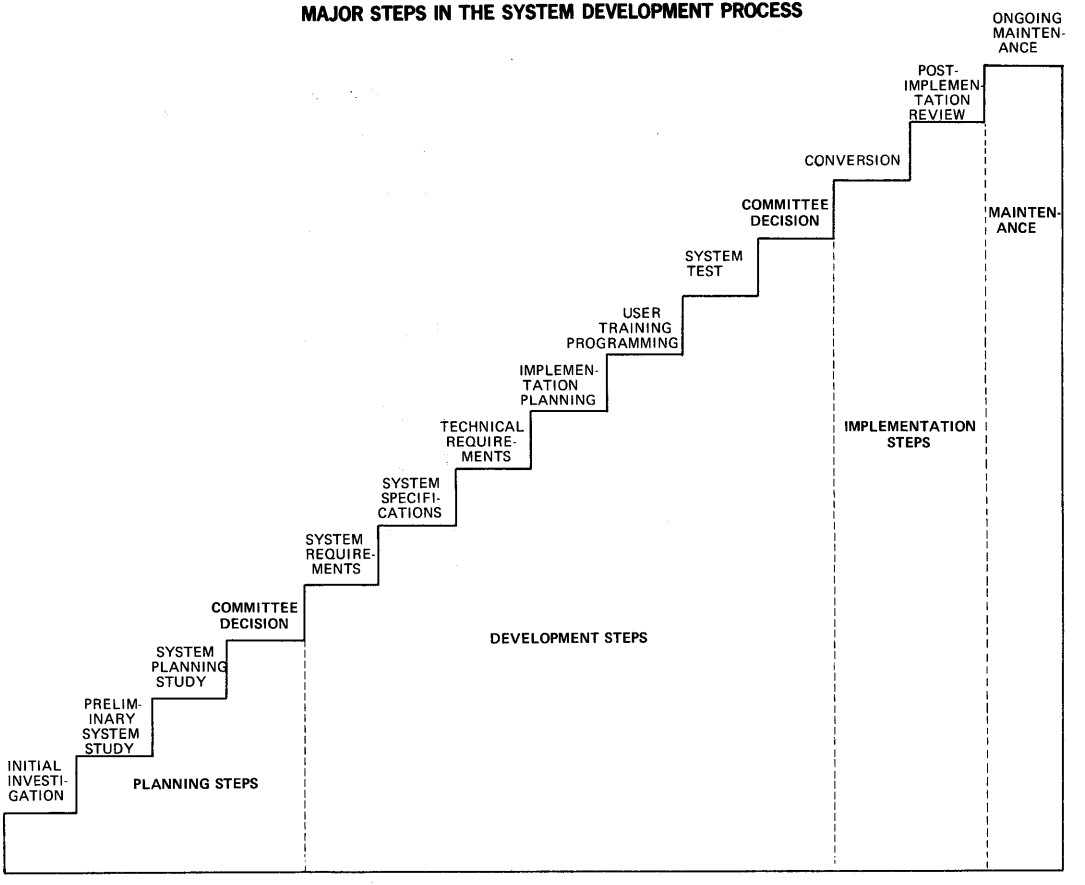


Figure 5-10 PROJECT STRUCTURE FOR THE DEVELOPMENT OF EDP SYSTEMS

CONCLUSION – THE AUDIT TRAIL IS A MANAGEMENT TRAIL

To conclude this synopsis of computer controls and auditing let's reiterate what was stated in the Introduction to this Summary – let's take the "audit" out of the "audit trail" and put the "trail" in proper perspective. A trail of documentation through anything exists with the benefit of management much more than for the auditor. Its first purpose is to permit verification of reliable processing by managers of user departments. In addition, the lack of this trail will have severe consequences normally on the confidence of users and resolution of errors. There are many ways for the auditor to get around the lack of hard copy output in today's audit environment. The existence of the trail then is primarily for the benefit of management and not the auditor. It facilitates the auditor's work but management cannot do without it. *Therefore, the audit trail isn't an audit trail – it's a management trail.*