Evaluating Internal Controls In Computer-Based Systems

Audit Guide

GAO
U.S. General Accounting Office
June, 1981

FOREWORD

This guide is intended to help auditors make a detailed review and evaluation of internal controls in computer-based systems. It is designed specifically for auditors who already have technical training in auditing automatic data processing systems. With this in mind, some terms are included without detailed explanations.

This guide includes the kinds of controls an auditor should expect to find in computer-based systems. However, the guide does not try to establish standards for specific combinations of controls that should be used. Auditors should not expect, therefore, any one system to include all the kinds of controls in the guide. Instead, each system should include controls which, under the circumstances, provide an adequate level of control to assure reliable and timely processing. Assessing whether an adequate level of control has been achieved is, of course, a matter of judgment.

The guide is intended to be used to help satisfy audit objectives that require the auditor to understand whether a computer-based system is adequately controlled and consistently produces reliable results in a timely manner. It is not intended to be used on every audit that involves a computer system. A decision to make a detailed review with the guide could result from

--a specific request for a review of the accuracy, reliability, and effectiveness of a particular computer-based system;

--a general survey or reliability assessment indicating there is an unacceptably high risk that computer data is erroneous and a separate detailed review is necessary to verify the extent of errors;

--a need to assess internal controls in financial audits to provide a basis for reliance on them and for restricting the extent of substantive tests; and

--a need to review general controls or application controls in data processing systems as required by generally accepted Government auditing standards.

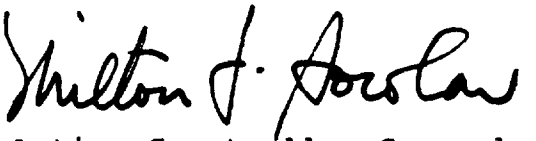
If auditors are to maintain professionalism in doing this audit work, a sound audit approach is needed.

This guide presents such an approach for evaluating internal controls in computer-based systems. It is a comprehensive document that incorporates techniques learned over the past several

years. Detailed audit procedures are included in sections. One or more sections can be applied to an audit as needed; it is not intended that all sections be applied to every audit.

Detailed procedures lead the auditor through initial collection of data, identification and evaluation of internal controls, and detailed analysis and testing of controls and records. Newly developed questionnaires, checklists, internal control profiles, and internal control matrixes are also included.

Since data processing is a continuously developing area, we anticipate that this guide will be revised. Comments and suggestions are welcome and should be addressed to the Director and Chief Accountant of GAO, Accounting and Financial Management Division, U.S. General Accounting Office, 441 G St. N.W., Washington, D.C. 20548.



Acting Comptroller General
of the United States

CONTENTS

		Page
INTRODUCTION		1
	DATA COLLECTION PHASE	
SECTION		
I	Background information on agency being evaluated	7
II	Background information on ADP department	10
III	Background information on computer application	17
	INTERNAL CONTROLS PHASE	
IV	Top management controls	20
V	General controls over the data processing function	36
VI	Controls over the computer application	139
	DETAILED ANALYSIS AND TESTING PHASE	
VII	Data flow analysis	233
VIII	Observation analysis	237
IX	User satisfaction analysis	239
X	Test data analysis	247
XI	Computer program analysis	255
XII	Data retrieval and analysis	261
XIII	Job accounting data analysis	267
	REPORTING PHASE	
XIV	Reporting and recommendations for additional audit work	273
APPENDIX		
I	Bibliography	275
II	Assessing risk	278

ABBREVIATIONS

ADP	automatic data processing
CPU	central processing unit
DBMS	data base management system
FIPS	Federal Information Processing Standards
GAO	General Accounting Office
ITF	integrated test facility
RJE	remote job entry
SDLC	system development life cycle

INTRODUCTION

Auditors frequently use computer-generated information when performing financial and compliance, economy and efficiency, and program results reviews. This information, and the systems that produce it, must be evaluated to make sure the data is accurate, reliable, and timely. These evaluations are necessary for the auditor to maintain professionalism in performing audits and to comply with GAO audit policy.

GAO AUDIT POLICY

GAO policy concerning computer-based systems is very specific and places the responsibility for evaluating computer-based systems directly on the auditor:

--"When ADP is an important integral part of agency operations which we are auditing, our work should include an appropriate examination of the functioning of the ADP system."

* * * * *

--"When examining the functioning of an ADP system, the auditor must make an evaluation of the system of internal control to assess the extent it can be relied upon to insure accurate information."

* * * * *

--"Review of the system of internal control and subsequent compliance and validation tests should enable the auditor to assess the reliability of the ADP system and its outputs. The primary purpose of internal control is to minimize the risks of errors and irregularities. Although the auditor's reliance on the system of internal control helps determine the extent of detailed examination and testing required, it should not, however, be considered a substitute for detailed testing."

In auditing ADP systems and their outputs, the auditor applies the same policies and objectives used in examining any other agency program or activity. Auditing objectives remain the same whether ADP is employed or not. Procedures required to accomplish these objectives, however, may be changed by the method of data processing used and may require the auditor to employ specialized ADP expertise.

PURPOSE OF GUIDE

This guide, which replaces the March 1977 exposure draft "Guide for Evaluating Automated Systems," provides the auditor with a structured approach for evaluating a computer-based system, i.e., a system designed to perform a particular task such as payroll, inventory, management analysis, etc. This "systems approach" helps evaluate the total system from origination of source documents through final disposition of output products. Primary emphasis is placed on assessing the system's or application's reliability in processing data in a timely, accurate, and complete manner. This is accomplished by evaluating both manual and automated internal controls and by performing tests to substantiate the existence and effectiveness of internal controls.

Audit procedures in this guide should also help the auditor comply with generally accepted Government auditing standards on auditing computer-based systems.

"The auditor shall:

1. Review general controls in data processing systems to determine whether (a) the controls

have been designed according to management direction and known legal requirements and (b) the controls are operating effectively to provide reliability of, and security over, the data being processed.

2. Review application controls of installed data processing applications upon which the auditor is relying to assess their reliability in processing data in a timely, accurate, and complete manner."

HOW TO USE THIS GUIDE

This guide is arranged in phases:

--Data collection.

--Internal controls.

--Detailed analysis and testing.

--Reporting.

Each phase is broken down further into sections. Each section briefly explains the reasons for completing detailed audit procedures that follow. This arrangement permits the audit staff to complete audit procedures in one section before moving to the next or to do work in several sections simultaneously. One or more sections can be applied to an audit as needed; it is not intended that all sections be applied to every audit. Several audit aids are also included.

Checklists

Checklists suggest documentation that should be gathered to conduct a review.

Questionnaires

Questionnaires were developed to help the auditor gather and analyze information about the system's internal controls. The questions should be self-explanatory. Responses to the questionnaires will frequently be a simple "yes" or "no"--the latter indicating a potential control deficiency. All responses should be indexed to supporting documents or records of interviews. Where different agency officials are asked similar questions, the responses should be checked for consistency. Reasons for conflicting responses should be fully examined and documented. The questionnaires should not be considered all inclusive, but rather should be regarded as detailed probing questions which should help the auditor determine the existence and effectiveness of internal controls. The auditor may wish to remove and copy the questionnaires for use in the audit.

Profiles

Profiles are included to help the auditor measure risk (low, medium, or high) when the presence or absence of controls is determined. Although the auditor exercises judgment in deciding which risk category applies, the profiles provide standard criteria which should lead to more uniform decisions. Appendix II includes instructions for using profiles and assessing risk.

Matrixes

Matrixes are included to help the auditor determine what additional tests and/or reporting options are available.

WORKING PAPERS

GAO policy for documenting evaluations of computer-based systems is as follows:

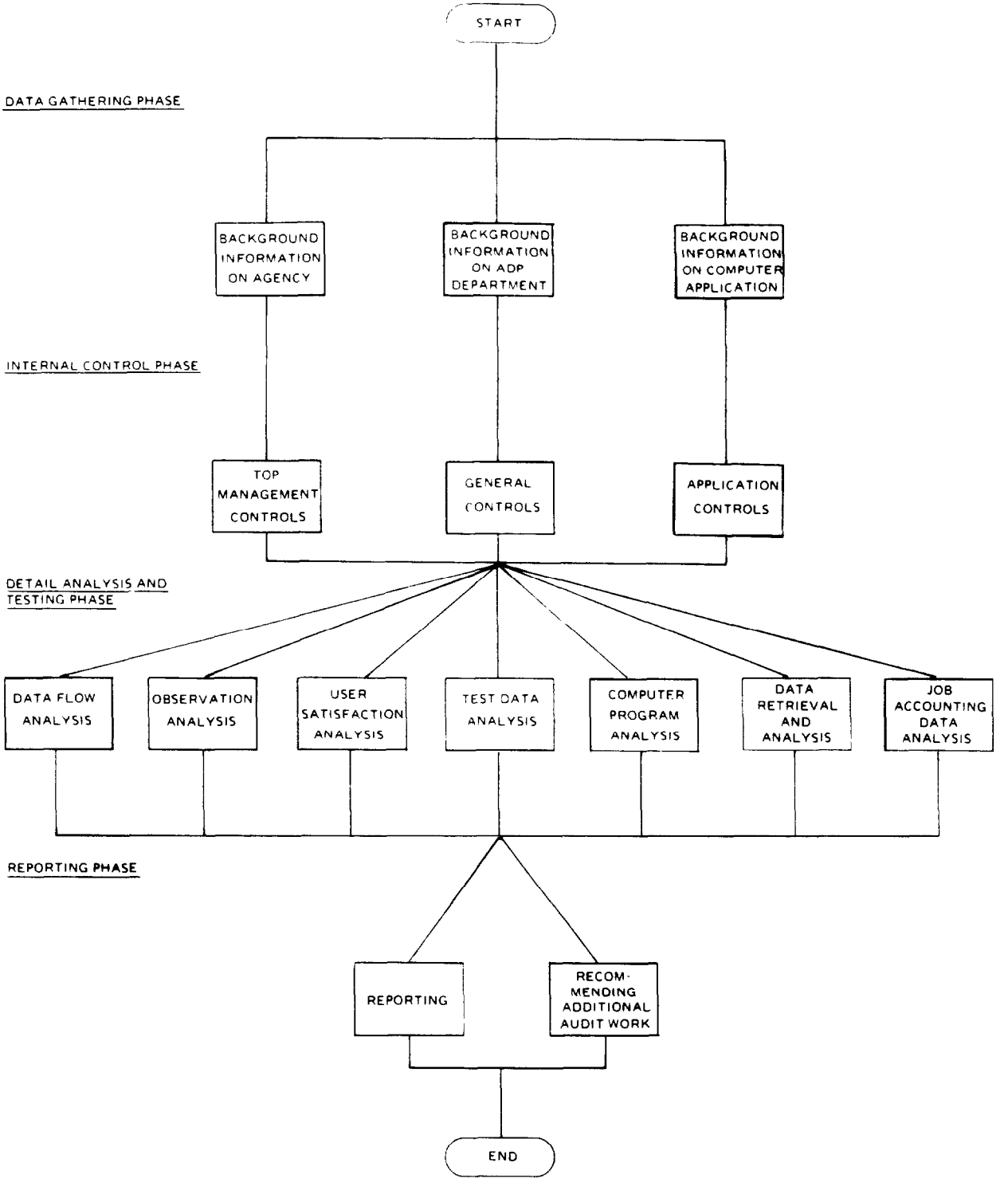
> "Work performed and auditor's conclusions about the functioning of the ADP system and the reliability of computer processed data included in a GAO report or used in support of findings, conclusions, and recommendations should be recorded in the working papers in accordance with [our] standards **** When work is performed by use of computerized techniques including data processing and statistical programs, the step-by-step process should be sufficiently documented to permit the process to be repeated."

The working papers should be self contained and prepared, indexed and reviewed the same way as regular audit working papers.

AUDIT APPROACH

This guide is presented in the order that an auditor would normally follow in reviewing a system. A brief overview of this "systems approach" follows.

OVERVIEW - EVALUATING INTERNAL CONTROLS IN COMPUTER-BASED SYSTEMS



Data Collection Phase

To begin an audit of a computer-based system, the auditor should collect background information about the agency or organization, ADP department, and computer application being audited. This information will be needed in subsequent audit phases.

SECTION I

BACKGROUND INFORMATION ON AGENCY BEING EVALUATED

The auditor should obtain certain information about the agency or organization whose computer-based system is being reviewed. Generally, it should include

--agency mission statement and organization charts;

--legislative history information, including laws or regulations which may have been incorporated in the computer-based system;

--public relations literature which describes the nature and characteristics of the agency and/or program;

--agency planning documents which illustrate the need for and use of ADP; and

--internal or external audit reports or studies concerning the agency's ADP operations or the application.

This information will provide a basic understanding of agency operations and the degree to which the agency relies on ADP to perform its mission.

AUDIT PROCEDURE

1. Use the following checklist 1 as an aid in obtaining background on the agency. Pay particular attention to the computer-based system being evaluated.

BACKGROUND INFORMATION ON AGENCY

ITEMS TO BE OBTAINED	Workpaper index
1. Agency mission statement.	
2. Agency organization charts.	
3. Functional descriptions of agency organization.	
4. Bills, acts, titles or laws that affect the agency and the computer application.	
5. Regulations, both agency and Government-wide, that affect the application.	
6. Pamphlets, brochures, newsletters, booklets, etc., that describe agency operations and the application.	
7. Copies of agency long- and short-range planning documents.	
8. A description of the executive ADP management committee duties, functions, and representation.	
9. Minutes of executive ADP management committee meetings.	
10. Previous GAO reports on Government-wide ADP issues that affect the application.	
11. Previous GAO reports on the agency's ADP procurement activities that affect the application.	
12. Previous GAO reports on the agency's ADP planning process that affect the application.	
13. GAO systems approval documentation on the application.	
14. Copies of external review reports prepared by private contractors.	
15. Copies of reports on financial statements and/or management reports prepared by private accounting firms.	

CHECKLIST 1

	Workpaper index
16. Documentation on the agency's ADP-related internal audit function.	
17. Copies of relevant internal audit reports.	

SECTION II

BACKGROUND INFORMATION ON ADP DEPARTMENT

The auditor should obtain information about the agency's ADP Department. It should include

--ADP department organization and staffing arrangements;

--general ADP procedures concerning systems development, data center management, and data center security and protection; and

--a description and inventory of system software and hardware in use.

This information will be needed to evaluate general controls over the data processing function.

AUDIT PROCEDURE

1. Use the following checklist 2 as an aid in obtaining background on the ADP department.

CHECKLIST 2

BACKGROUND INFORMATION ON ADP DEPARTMENT

Workpaper index

ITEMS TO BE OBTAINED

Organization and staffing

1. ADP department organization chart. _____

2. Functional descriptions of ADP department organization. _____

3. List of key officials in the ADP department. _____

Section and supervisor	Location and telephone number	Major responsibilities

Workpaper index

4. Staffing level of the ADP department by division or office. _____

	Number		Names of supervisors
	Authorized	Assigned	
ADP general management			
Security personnel			
System programmers			
Systems analysts			
Application programmers			
Other technical support			
Computer operators			
Peripheral equipment handlers			
Data entry operators			
Control clerks			
Schedulers			
Librarian(s)			
Data base administrator(s)			
Secretaries and clerks			
Other			
Total			

Anticipated staffing additions and deletions during the next 2 years:

5. Major position descriptions. _____

	Workpaper index
System design, development, and modification	
6. System documentation standards.	_____
7. System documentation procedures.	_____
8. System development procedures.	_____
9. Computer program change procedures.	_____
Data center management	
10. Data center operations procedures manual.	_____
11. File library procedures manual.	_____
12. User billing procedures, including the billing algorithm.	_____
13. Statistics on system utilization.	_____

	Total system processing	Specific computer-based system being evaluated
Number of scheduled 8-hour shifts per day	_____	_____
Number of scheduled days per week	_____	_____
Average number of jobs per day	_____	_____
Total hours scheduled for past 3 months	_____	_____
Actual hours used for past 3 months:		
Production	_____	_____
Testing	_____	_____
Rerun	_____	_____
Maintenance	_____	_____
Idle	_____	_____
Other	_____	_____

Explain how the numbers of actual hours used were derived.

_____

_____

Multiprogramming factor (average number of programs running concurrently) _____

14. Budgeted, actual, and projected costs for current and next fiscal year.

	Budgeted costs	Actual costs	Projected costs	Workpaper index
Costs of rented equipment:				
Central processing units				
Data communications				
All other				
Costs of purchased equipment:				
Central processing units				
Data communications				
All other				
Hardware maintenance costs				
Personnel costs:				
ADP general management				
Security personnel				
System programmers				
Systems analysts				
Application programmers				
Other technical support				
Computer operators				
Peripheral equipment handlers				
Data entry operators				
Control clerks				
Schedulers				
Librarian(s)				
Data base administrator(s)				
Secretaries and clerks				
Other				
Supplies (cards, paper, etc.)				
Contracts:				
Data conversion				
Other services				
Facility costs:				
Space				
Utilities				
Other costs (specify)				
Total costs				

CHECKLIST 2

	Workpaper index
Data center protection	
15. Data center security procedures.	_____
16. Emergency plan.	_____
17. Backup and recovery procedures.	_____
System software	
18. Operating system description.	_____
19. System utilities description.	_____
20. Program library system description.	_____
21. File maintenance system description.	_____
22. Security software description.	_____
23. Data communications system description.	_____
24. Data base management system description.	_____
25. System software change procedures.	_____

Workpaper index

Hardware

26. Complete inventory and description of the computer system. _____

CPU manufacturer	_____
CPU model number	_____
Date CPU installed	_____
CPU physical location	_____
Internal storage capacity	_____
Direct access storage capacity	_____
Console model number	_____

Peripheral devices	Number of devices
Magnetic tape drives:	
___track, ____density	_____
___track, ____density	_____
___track, ____density	_____
Magnetic disk drives:	
___series or model number	_____
___series or model number	_____
___series or model number	_____
Magnetic drum units	_____
Other mass storage units (specify type)	_____
Card readers	_____
Card punches	_____
Card reader/punches	_____
Line printers:	
___lines per minute	_____
___lines per minute	_____
On-line terminals	_____
Remote batch terminals	_____
Communications controllers	_____
Optical scanners	_____
MICR readers	_____
Mark sense readers	_____
Key-to-tape units	_____
Key-to-disk units	_____
Keypunch/verification units	_____
Card sorters	_____
Card collators	_____
Card accounting machines	_____
Other (specify)	_____

27. Schematic of telecommunications network. _____

SECTION III

BACKGROUND INFORMATION ON COMPUTER APPLICATION

The auditor should obtain information on the computer application(s) being audited. It should include

--narrative system descriptions,

--system flowcharts,

--computer program descriptions,

--file layouts, and

--procedures manuals.

AUDIT PROCEDURE

1. Use the following checklist 3 as an aid in obtaining background on the application.

BACKGROUND INFORMATION ON COMPUTER APPLICATION

ITEMS TO BE OBTAINED	Workpaper index
1. Project request document.	_____
2. Feasibility study document.	_____
3. Cost/benefit analysis document.	_____
4. Functional requirements document.	_____
5. Data requirements document.	_____
6. System/subsystem specifications.	_____
7. Program specifications.	_____
8. Data base specifications.	_____
9. Users manuals.	_____
10. Operations manuals.	_____
11. Program maintenance manuals.	_____
12. Test plan.	_____
13. Test analysis report.	_____
14. Overview of computerized application system.	_____
System name and agency identification number	_____
Date of initial implementation	_____
Date of latest modification	_____
Number of modifications in the last 2 years	_____
Type of system (administrative, scientific, other (specify))	_____
Type of processing (batch or on-line)	_____
Overview system flowchart and narrative description	_____
Number of computer programs	_____

Size of largest computer program (bytes of storage) _____

Programming language(s) used _____

Processing frequency _____

Total monthly processing hours _____

Design of system (vendor supplied or agency programmed) _____

Testing methodology (test data, live data, or not at all)

a. Initial system _____
b. Latest modification _____

Availability of test results

a. Initial system _____
b. Latest modification _____

Date of last audit or evaluation (obtain copy) _____

Output product distribution list _____

Internal Controls Phase

With information obtained in the data collection phase, the auditor should evaluate top management controls, general controls over the data processing function, and application controls over installed computer applications. This review should identify control weaknesses and help the auditor determine the scope of further testing and analysis.

SECTION IV

TOP MANAGEMENT CONTROLS

ADP, like any other resource, needs to be properly managed to take full advantage of its capabilities. Agency top management should exercise sufficient control over the ADP function to determine how well it operates, where improvements are needed, and what capabilities will be needed in the future. This control is normally provided through

--an executive ADP management committee,

--internal audits, and

--external audits and studies.

Collectively, these make up a network of management controls.

EXECUTIVE ADP MANAGEMENT COMMITTEE

Such a committee has proven to be effective in helping make sure that computers are used appropriately in carrying out the agency's overall mission. Membership of the committee, normally chaired by a representative of top management, usually includes

--a senior financial representative,

--a senior data processing representative,

--a senior legal representative,

--a senior personnel department representative,

--heads of user departments, and

--an auditor with experience in evaluating automatic data processing systems.

It is extremely important that user departments be fully represented so their needs are adequately considered. Active participation by management, user departments, and internal audit helps make sure that controls, procedures, and management policies will be incorporated in computer-based systems.

Generally, functions of the committee are to

--establish agencywide policies for data processing systems,

--approve short- and long-range plans to develop and implement new systems,

--evaluate the need for new computer equipment, and

--insure that new equipment is acquired in the most economical and expeditious manner.

The committee should also be responsible for making sure that recommendations made by both internal and external audit groups or other organizations are fully implemented.

AUDIT PROCEDURES

Use background information collected in section I and:

1. Complete the following questionnaire 1 on the executive ADP management committee.
2. Complete the appropriate section of top management controls profile 1, which is included at the end of this section.
3. On the basis of the level of potential risk determined on the top management controls profile, consult the top management controls matrix at the end of this section for guidance on additional audit steps.

EXECUTIVE ADP MANAGEMENT COMMITTEE

An executive ADP management committee, normally chaired by a top management representative, is usually responsible for

--establishing agencywide policies for data processing systems,

--approving short- and long-range plans to develop and implement new systems,

--evaluating the need for new computer equipment, and

--insuring that new equipment is acquired in the most economical and expeditious manner.

User departments and internal audit should be represented on this committee.

The auditor should determine whether the agency has an executive ADP management committee, its makeup, and the extent of its responsibilities.

	YES	NO
REPRESENTATION		
1. Does the agency have an executive ADP management committee? (Attach a copy of the committee's organization chart.)	___	___
2. Does a top management representative chair the committee?	___	___
3. Are major users of computer-processed information represented on it?	___	___
4. Is the internal audit department represented?	___	___
5. Does the committee have prescribed, documented responsibilities? (Attach a copy of the committee's charter.)	___	___
RESPONSIBILITIES		
6. Does the committee:		
--Establish agencywide policies for ADP?	___	___

QUESTIONNAIRE 1

	YES	NO
--Approve short- and long-range plans for developing and implementing new computer systems?	___	___
--Evaluate the need for new computer equipment?	___	___
--Insure that new equipment is acquired in the most economical and expeditious manner?	___	___

REPORTING REQUIREMENTS

7. Are executive ADP management committee minutes, staff reports, and memorandums sent directly to the agency head?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

INTERNAL AUDIT

An internal audit organization, which conducts independent reviews and prepares reports on its findings, is one of the essential tools of management, complementing other elements of top management control.

Work of the auditor has expanded significantly with the evolution of computers. To help maintain professionalism in audit work, GAO has issued standards for auditing computer-based systems.

"The auditor shall:

1. Review general controls in data processing systems to determine whether (a) the controls have been designed according to management direction and known legal requirements and (b) the controls are operating effectively to provide reliability of, and security over, the data being processed.

2. Review application controls of installed data processing applications upon which the auditor is relying to assess their reliability in processing data in a timely, accurate, and complete manner."

In addition, it should be the objective of all audit organizations and auditors to review the design and development of new data processing systems or applications and significant modifications to them.

The internal audit function should normally be a separate entity within the agency and should report to the agency head or deputy head. This arrangement permits effective communication of audit findings with minimum conflicts of interest and provides auditor independence.

AUDIT PROCEDURES

Use background material collected in section I along with additional interviews and:

1. Complete the following questionnaire 2 on internal audit.
2. Complete the appropriate section of top management controls profile 1, which is included at the end of this section.
3. On the basis of the level of potential risk determined on the top management controls profile 1, consult the top management controls matrix at the end of this section for guidance on additional audit steps.

INTERNAL AUDIT

Generally accepted Government auditing standards concerning computer-based systems state that the auditor shall

--review the general controls in data processing systems, and

--review application controls of installed data processing applications.

An additional objective should be to review the design and development of new data processing systems and significant modifications to them. The internal audit function should be independent and should report to the agency head or deputy head.

The auditor should determine the extent of internal audit coverage of agency ADP activities, and the level of internal audit reporting.

	YES	NO
ADP INVOLVEMENT		
1. Is the agency's ADP-related internal audit function documented? (If so, obtain a copy.)	___	___
2. Has internal audit periodically reviewed the ADP function?	___	___
3. Has internal audit developed an overall audit plan which includes ADP reviews?	___	___
4. Does internal audit have an ADP team within its staff?	___	___
5. Are members of the ADP audit team qualified in the ADP audit area?	___	___
GENERAL CONTROLS REVIEW CAPABILITY		
6. Does internal audit review general controls in computer-based systems to determine whether controls have been designed according to management direction and legal requirements?	___	___
7. Does internal audit review general controls in computer-based systems to assure that the controls are operating effectively to provide		

	YES	NO
reliability of, and security over, the data being processed?	___	___
8. As part of its general controls reviews, does internal audit make sure that each of the following are adequate:		
--Organizational controls?	___	___
--Physical facilities controls?	___	___
--Personnel controls?	___	___
--Security controls?	___	___
--Operating system controls?	___	___
--Hardware controls?	___	___
APPLICATION CONTROLS REVIEW CAPABILITY		
9. Does internal audit review the application controls in computer-based systems upon which they are relying to assess their reliability in processing data in a timely, accurate, and complete manner?	___	___
10. Do these control reviews determine whether the computer-based systems conform to agency and Federal standards?	___	___
11. Do these control reviews determine whether the systems conform to the latest approved design specifications?	___	___
12. Are periodic audits designed to test internal controls and reliability of data processed?	___	___
13. Does internal audit verify the information on ADP output reports against related source documents?	___	___
14. Does internal audit use test data to insure the reliability of computer programs?	___	___

QUESTIONNAIRE 2

	YES	NO
15. Are automated data retrieval and analysis packages or specially written computer programs used for evaluating data records?	___	___
16. Are audit test data stored under internal audit control?	___	___
17. Does internal audit supervise the running of test data?	___	___
18. Are audit retrieval programs stored under internal audit control?	___	___
19. Does internal audit supervise the running of audit retrieval programs?	___	___

SYSTEMS DESIGN, DEVELOPMENT, AND MODIFICATION REVIEW CAPABILITY

20. Does internal audit review the design and development of new data processing systems or applications?	___	___
21. Does internal audit review significant modifications to systems or applications?	___	___
22. As part of its design, development, and modification review function, does internal audit make sure that all systems:		
--Carry out the policies management has prescribed for the system?	___	___
--Provide the controls and audit trails needed for management, auditor, and operational review?	___	___
--Will be efficient and economical in operation?	___	___
--Conform with applicable legal requirements?	___	___
--Are documented in a manner that will provide the understanding of the system required for appropriate maintenance and auditing?	___	___

QUESTIONNAIRE 2

	YES	NO
REPORTING REQUIREMENTS		
23. Is internal audit located outside the staff or line management function of units under audit?	___	___
24. Does internal audit report to the agency head or deputy head?	___	___
25. Does internal audit maintain copies of memorandums and reports of all (both internal and external) ADP review efforts?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

EXTERNAL AUDITS AND STUDIES

Within the Federal Government, GAO performs many external audits of ADP. These include

--Government-wide reviews including multiple agency management and use of a particular ADP function;

--evaluations of agency planning for future ADP resources;

--reviews of agency selection, acquisition, and use of computer hardware and software; and

--approvals of agency accounting systems.

External audits and studies are also performed by certified public accounting firms and consultants. These provide top management with an independent appraisal of ADP operations. Top management has a responsibility to make sure proper corrective actions are taken on recommendations.

AUDIT PROCEDURES

Use background material obtained in section I and

1. Complete the following questionnaire 3 on external audits and studies. Pay particular attention to the computer-based system being evaluated.
2. Complete the appropriate section of top mangement controls profile 1, which is included at the end of this section.
3. On the basis of the level of potential risk determined on the top management controls profile 1, consult the top management controls matrix at the end of this section for guidance on additional audit steps.

EXTERNAL AUDITS AND STUDIES

External reviews and studies conducted by GAO, private accounting firms, or consultants provide a third party appraisal of agency ADP operations.

The auditor should determine the extent of external review coverage for the past 1 to 3 years and whether the agency has implemented recommendations.

	YES	NO
GAO ADP REVIEWS		
1. Has the agency been included in a Government-wide ADP review?	___	___
2. Were agency ADP operations free of deficiencies?	___	___
3. If not, has the agency taken corrective measures?	___	___
4. Has the agency's ADP planning process ever been reviewed?	___	___
5. Were agency ADP planning processes free of deficiencies?	___	___
6. If not, has the agency taken corrective measures?	___	___
7. Have the agency's ADP procurement activities ever been reviewed?	___	___
8. Were agency ADP procurement activities free of deficiencies?	___	___
9. If not, has the agency taken corrective measures?	___	___
GAO SYSTEM APPROVALS		
10. Has the application system under review ever been subjected to a GAO system approval review?	___	___
11. Was the agency system free of deficiencies?	___	___
12. If not, has the agency taken corrective measures?	___	___
13. Was the system approved?	___	___

QUESTIONNAIRE 3

PRIVATE ACCOUNTING FIRMS AND CONSULTANTS

		YES	NO
14.	Has the agency contracted with private firms to evaluate its ADP activities?	___	___
15.	Were agency ADP activities free of deficiencies?	___	___
16.	If not, has the agency taken corrective measures?	___	___
17.	If a financial computer-based system is involved, was the system reviewed by a private accounting firm?	___	___
18.	Were both general and application controls reviewed?	___	___
19.	Was the financial computer-based system free of deficiencies?	___	___
20.	If not, has the agency taken corrective measures?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

PROFILE 1

TOP MANAGEMENT CONTROLS PROFILE

On the basis of questionnaire responses and other information obtained relating to the following control characteristics, how much risk (low, medium, or high) do you believe is involved in relying on the agency's top management controls to assure effective ADP operations? Refer to appendix II for more information on assessing risk.

Control characteristic	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level of potential risk
EXECUTIVE ADP MANAGEMENT COMMITTEE					
Committee representation					
Committee responsibilities					
Committee reporting requirements					

TOP MANAGEMENT CONTROLS PROFILE

Control characteristic	Is the control in place?	Is the control effective?	In some alternate control in place?	Is the alternate control effective?	Level of potential risk
INTERNAL AUDIT					
ADP involvement					
General controls review capability					
Application controls review capability					
Systems design, development, and modification review capability					
Reporting requirements					
EXTERNAL AUDITS AND STUDIES					
GAO ADP reviews					
GAO system approvals					
Private accounting firms and consultants					

TOP MANAGEMENT CONTROLS MATRIX

If the degree of risk determined on the previous profile warrants additional audit work (i.e., medium to high risk), the following matrix should help the auditor select appropriate audit steps to complete the review.

	document the data flow	observe operations	obtain user satisfaction	process test data	perform computer program analysis	perform data retrieval analysis	analyze job accounting data	report deficiencies	suggest additional audit
Executive ADP Management Committee									
Committee Representation								●	
Committee Responsibilities								●	
Committee Report Requirements								●	
Internal Audit									
ADP Involvement								●	●
General Control Reviews	●	●	●			●	●	●	●
Application Control Reviews	●	●	●	●	●	●	●	●	
System Design, Development and Modification Reviews			●	●	●			●	
Reporting Requirements								●	
External Audits and Studies									
GAO ADP Reviews								●	●
GAO System Approvals								●	●
Private Accounting Firms and Consultants								●	●

SECTION V

GENERAL CONTROLS OVER THE DATA PROCESSING FUNCTION

General controls normally apply to all processing carried out within a data processing installation and are independent of computer applications because several different applications are normally processed in the same installation. General controls include

--organizational controls;

--system design, development and modification controls;

--data center management controls;

--data center protection controls;

--system software controls; and

--hardware controls.

The effectiveness of these general controls must be considered when evaluating computer-based systems because weaknesses in general controls can affect all applications processed.

ORGANIZATIONAL CONTROLS

Effective controls need to be established over operations of the data processing department because of the concentration of functions brought about by the computer. The agency organizational structure must provide assurances that assets are safeguarded and that reliable information is produced.

A key organizational control involves a separation of duties so that activities of one employee act as a check on those of another and so that no one employee controls the handling and

recording of a transaction from beginning to end. These controls include

--separating the data processing function from other agency functions,

--separating different data processing functions within the data processing department, and

--providing for separation of duties within user departments.

The data processing department normally provides a service for other departments that includes recording and processing data. To maintain a division of duties among the initiation, authorization, and recording functions, source documents are usually originated and approved outside the data processing department.

To assure effective controls within the data processing department, certain functions should also be separated. For example, the system design and programming function should be separated from computer operations to make sure that no person or group has the ability to implement new systems or revise old ones without prior approval and thorough checking. Also, the functions of systems analysis, application programming, and system programming should be separated. A data control group, independent of other operational functions, should be established to review and balance computer input and output and act as a liaison with user departments. A computer file library, staffed by a full-time librarian, should control all punched cards, magnetic tapes, and disks used in computer operations to make sure that only authorized persons have access to computer files. When a data base management system (DBMS) is

used, a data base administrator should be responsible for operation and control of the data base.

The overall organizational plan should provide a well-controlled working environment. There should be a clear-cut line of responsibility between every subordinate and supervisor, a job rotation policy, and a policy of mandatory vacations for department personnel. Excessive personnel turnover and absentee rates are often good indicators of organizational control problems.

AUDIT PROCEDURES

Use the background material obtained in section II and:

1. Complete the following questionnaire 4 on organizational controls.
2. Complete the appropriate section of profile 2 on general controls.
3. On the basis of the level of potential risk determined on the general controls profile 2, consult the general controls matrix 2 at the end of this section for guidance on additional audit steps.

ORGANIZATIONAL CONTROLS

A key organizational control is an adequate separation of duties, which includes

--separating the data processing functions from other agency functions,

--separating different data processing functions within the data processing department, and

--providing for separation of duties within user departments.

Clear-cut lines of supervision, job rotation, and mandatory vacations can also improve internal control.

The auditor should determine the extent of separation of duties.

	YES	NO
SEPARATION OF DUTIES		
1. Is the ADP function independent from other agency operations?	___	___
2. Are all ADP employees prohibited from having authority, or duties in any other department?	___	___
3. Are the following functions performed by a different individual or group:		
--Systems analysis?	___	___
--Application programming?	___	___
--Acceptance testing?	___	___
--Program change control?	___	___
--Data control?	___	___
--Production control and scheduling?	___	___
--Computer equipment operation?	___	___
--Data base management?	___	___
--System software maintenance?	___	___

QUESTIONNAIRE 4

	YES	NO
--Computer files maintenance?	___	___
--Source document origination?	___	___
--Source document conversion to machine-readable format?	___	___

PERSONNEL POLICIES

4.	Is there a direct line of responsibility between every subordinate and supervisor?	___	___
5.	Is a personnel rotation plan in effect within the different functional areas in the ADP department?	___	___
6.	Are ADP department personnel required to take regularly scheduled vacations?	___	___
7.	Does the ADP department have a low turnover rate?	___	___
8.	Does the ADP department have a low absentee rate?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

SYSTEM DESIGN, DEVELOPMENT, AND MODIFICATION CONTROLS

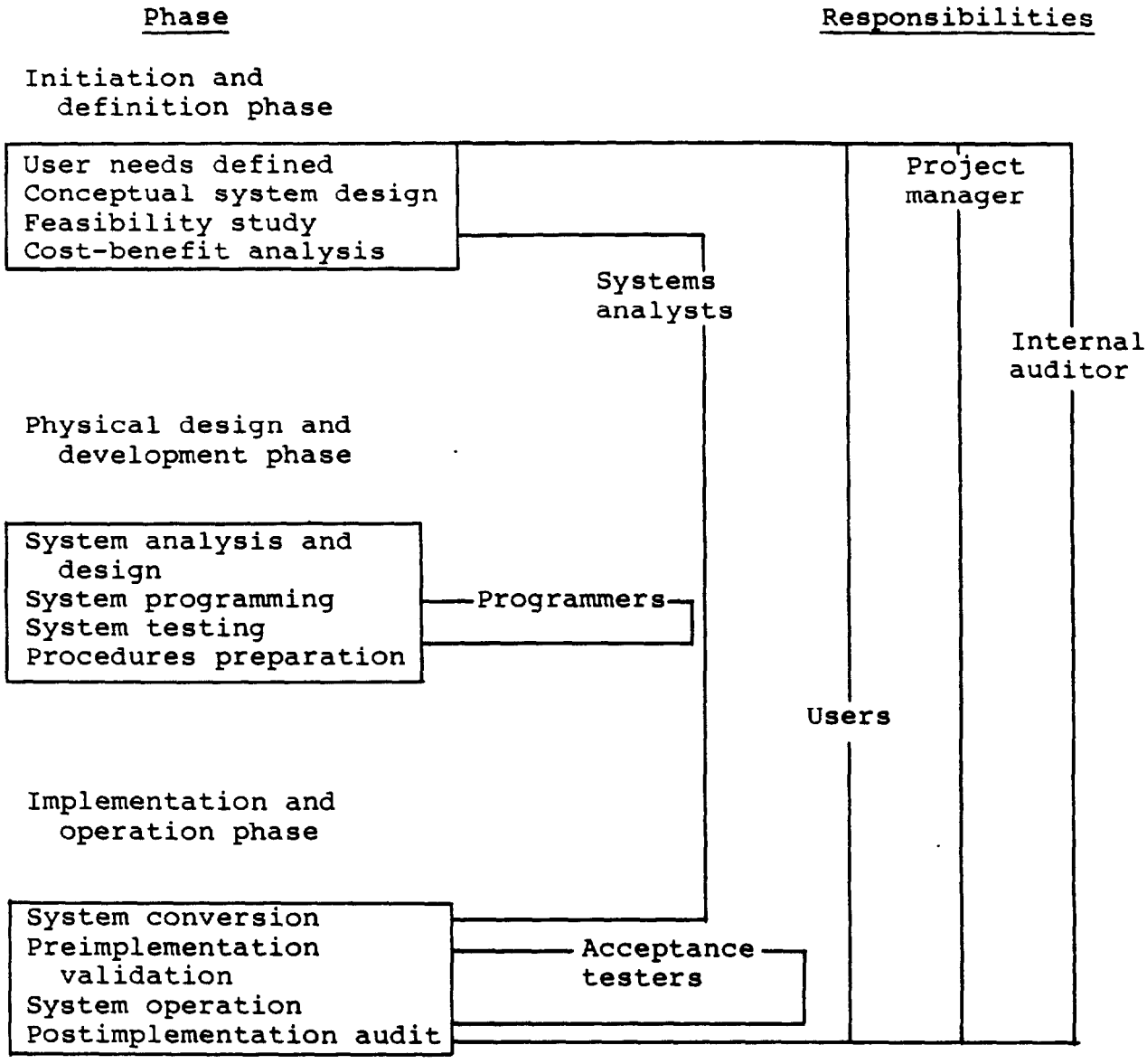
The adequacy and effectiveness of controls in computer-based systems begin with methods and procedures used during system design, development, and modification. Proper controls over these processes help make sure that systems are built to meet user requirements, are developed economically, are thoroughly documented and tested, and contain appropriate internal controls and audit trails. To accomplish these goals, a structured methodology, such as a System Development Life Cycle (SDLC), should be established and followed.

System Development Life Cycle

SDLC is a commonly accepted control technique used to divide an entire system development process into distinct phases so that management can review the process at key decision points. This technique is as applicable during initial system design as it is during the modification process; thus, appropriate elements of it should be used whenever changes are made to a system. SDLC is particularly advantageous because it promotes communications between programmers and systems analysts, acceptance testers, users, internal auditors, and management personnel.

The diagram and description of SDLC on the following page represents a composite approach using several authoritative sources.

System Development Life Cycle 1/



1/Gordon B. Davis, "Introduction to Computers" (New York: McGraw-Hill Book Company, 1977), pp. 59-64; Stanford Research Institute "Systems Auditability and Control Study," Control Practices Report (Altamonte Springs, Fla., The Institute of Internal Auditors, 1977), pp. 99-109; U.S. Department of Commerce, National Bureau of Standards, "Guidelines for Documentation of Computer Programs and Automated Data Systems," FIPS No. 38, Feb. 1976; U.S. Department of Commerce, National Bureau of Standards, "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase," FIPS No. 64, Aug. 1979.

System development life cycle phases

SDLC is divided into phases containing various activities. Each activity, or step, should be completed before the next is started. At the completion of each step, all previous work is reviewed and a "go/no go" decision is made. This progression through phases and steps provides a structured approach to the development process.

Initiation and definition phase--At the beginning of this phase, the user defines needs and objectives that are expected to be achieved from the proposed project. These needs are used to develop a conceptual system design. This design is used to make a feasibility study to determine the system's technical and operational feasibility. Finally, a cost-benefit analysis is performed to make sure that the project will produce the desired results economically.

Physical design and development phase--In this phase, a detailed system design is created and then used to prepare computer programs. Once the programs have been completed, each program, interrelated subsystems, and then the entire system, is tested to make sure that all components of the system are fully compatible and operational. Later, both manual and automated processing procedures are finalized for subsequent implementation of the system.

Implementation and operation phase--This phase begins with preparation of needed procedures for converting to newly designed programs and for building new files. This phase also includes parallel operations of both old and new systems, if applicable.

After conversion is completed, the entire system is subjected to an acceptance test to make sure that it performs in accordance with all functional and performance specifications, including desired controls, and meets user needs and objectives. Once the system is certified to be accurate and complete, it is placed in operation. The final step, or postimplementation audit, should be conducted after the system has been operational for several months. This audit, which is a review of the entire system, including both manual and automated processes, helps make sure that the system (1) includes internal controls needed to produce consistently reliable results and (2) operates in accordance with approved design specifications and agency and Federal standards.

System development life cycle responsibilities

In addition to providing decision points in the system development process, SDLC defines specific responsibilities for personnel involved in the process. These responsibilities are established at the outset of the project and provide for performance and management accountability. Thus, management gains the control mechanism needed in the development process.

Project manager--A project manager is usually responsible for control and coordination of the system development project. This project manager, subject to approval of a project management steering committee, is normally authorized to make decisions on personnel resources, scheduling, cost and budget, and most technical project matters. As leader of a team composed of persons

with mixed skills, the manager must provide a well-defined and structured environment within which system development can progress in an orderly manner. The project manager must also serve as the interface between users, programmers, analysts, acceptance testers, and top management.

Systems analysts--Systems analysts are responsible for translating user needs into a conceptual system design. This conceptual system is then used by systems analysts and users to make sure that the system is technically and operationally feasible and can produce the desired results at a minimum cost. After design is completed the systems analysts

--create detailed system design specifications used for detailed programming;

--review program documentation, after programming has been completed, to make sure that the detailed design specifications have been followed;

--review program test procedures and results to make sure that each program has been thoroughly tested and that each program and the entire system is fully operational;

--complete preparation of accurate system documentation, including instructions for users, control personnel, and operating personnel; and

--prepare procedures and documentation for system conversion so that the system can be validated and, once validated, begin operation.

Programmers--Programmers are responsible for preparing computer programs in accordance with systems analyst design specifications. After programming is completed, the programmer tests each program to make sure that it is fully operational and documents each program and the types of tests performed. This documentation should be accurate, complete, and up to

date because it is critically important to persons responsible for all other phases of the system development life cycle.

Acceptance testers--Acceptance testers or quality assurance staff are responsible for performing comprehensive preimplementation tests of all new systems and all modifications to existing systems. This testing determines whether the entire system, including both manual and automated processes, is functioning as specified by the user and as designed by the systems analyst. No system should be placed in operation without the acceptance tester's written certification that the entire system performs in accordance with all functional performance specifications. For these reasons, acceptance testers must control all planned system changes so that no changes can be made to any program without their prior approval. Emergency modifications to existing systems must also be validated, although conditions may result in such validation being performed after the fact. Thus, all changes, both planned and emergency, are subject to review and approval by acceptance testers.

Internal auditor--Internal auditors are responsible for assuring top management that all systems operate in conformance with management standards and approved design specifications and also include internal controls needed to produce consistently reliable results. The internal auditor should also act as a user to make sure that all systems contain necessary audit trails. To accomplish these tasks, the internal auditor should review each step as it is completed. Once the system is operational, the internal auditor has a continuing responsibility to review

both general and application controls to assure that the system continues to perform in accordance with management policy and produces consistently reliable results.

Key system development audit areas

Key areas in SDLC that require specific audit attention include documentation, program testing and system acceptance, and program change control. Deficiencies in any of these areas generally result in unreliable application system processing.

Documentation

Documentation is the process of describing on paper how a computer-based system operates. The objective of good documentation is to provide a clear, understandable description of the system. Good documentation increases the ease and accuracy of computer program maintenance and provides the basis for evaluating internal controls in the system.

Types of documentation that should be developed are included in Federal Information Processing Standards (FIPS) Publication No. 64, "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase" and FIPS Publication No. 38, "Guidelines for Documentation of Computer Programs and Automated Data Systems," prepared by the National Bureau of Standards, Department of Commerce. This documentation includes the following:

--Project request document. Provides the means for a user organization to request the development, procurement, or modification of software or other ADP-related services.

--Feasibility study document. Provides an analysis of the objectives, requirements, and system concepts;

an evaluation of alternative approaches; and identification of a proposed approach.

--Cost-benefit analysis document. Provides managers, users, designers, and auditors with adequate cost-benefit information to analyze and evaluate alternative approaches.

--Functional requirements document. Provides a basis of mutual understanding between users and designers of the computer-based system including system requirements, operating environment, and development plan.

--Data requirements document. Provides data description and technical information about data collection requirements.

--System specifications. Details the requirements, operating environment, and design characteristics for a system or subsystem.

--Program specifications. Details the requirements, operating environment, and design characteristics of individual computer programs.

--Data base specifications. Details the identification, logical characteristics, and physical characteristics of a particular data base.

--Users manual. Describes functions performed by the computer system in non-ADP terminology and serves as a reference document for preparing input data and parameters and for interpreting system outputs.

--Program maintenance manual. Provides information necessary to understand system's computer programs, operating environment, and maintenance procedures.

--Test plan. Provides a strategy for testing the computer-based system, including detailed specifications, descriptions, and procedures for all tests, and test data reduction and evaluation criteria.

--Test analysis report. Documents test results and findings, presents demonstrated capabilities and deficiencies for review, and provides the basis for preparing a statement of system readiness for implementation.

The act of preparing documentation helps prevent incomplete economic evaluations or inadequate specifications. Documentation facilitates communications and subsequent system modifications

and may act as a deterrent to fraudulent manipulations of systems. Documentation provides the means for effective system review by management, users, technical personnel, and auditors. It is essential for correcting design errors and for system maintenance.

Program testing and system acceptance

Programs which make up the application being reviewed should be thoroughly tested to assure accurate and reliable processing. Since programming errors can be made in either the symbolic language or program logic, error checking should be performed at several different stages in program development. This checking should include

--conducting a programmer/supervisor desk check or manual stepwise review of the program before it is released for assembly or compilation;

--reviewing results of assembly or compilation and correcting errors disclosed by these translator routines;

--running the computer program using test data and comparing results with predefined results;

--using various programming software packages to optimize program efficiency, test logic patterns, snap-shot program operation at key processing points, etc.; and

--running the computer program in parallel with the old system but under actual operating conditions for a certain period.

After programs, subsystems, and then the entire system have been tested, system acceptance begins. This is a process in which persons independent of those responsible for system implementation, check the entire system before it becomes operational. The goal is to make sure that the system functions as user requirements dictate and conforms with data processing

standards and procedures. This evaluation should be designed to exercise the application for errors of omission and errors of commission. As such, test files should contain sufficient data to test both valid and invalid conditions, the results of which should again be compared with predefined results.

The system acceptance process is the last line of defense against implementing an application with major errors. It serves as a "detective" control over the preceding phases of the development project. It gives users, internal auditors, designers, implementers, and other concerned parties an opportunity to view the system in final form before it becomes operational. If satisfied with results of the system acceptance process, acceptance testers should certify its accuracy and completeness in writing.

Program changes

Regardless of the magnitude of the modification, a positive means must be established to control all program changes. Controls should be established to prevent unauthorized and potentially inaccurate computer program changes from being incorporated into the live production environment. Both scheduled and emergency changes need to be controlled so that continued integrity of a computer-based system is maintained.

There are several steps that can be taken to provide for proper program change control. They include

--establishing a formal change request and authorization form, an approval procedure for controlling programmers' access to source coding maintained in a source program library, and a testing and system acceptance procedure for each program change;

--assuring that all program changes, both scheduled and emergency, are subjected to the system acceptance process;

--limiting the number of times a year in which program changes can be made, except for emergency changes; and

--using program library system software packages to control access to program libraries (both source and load libraries), since most of these packages have password protection and control log features to limit and document library accesses.

Effective program change controls help maintain the integrity of applications and can be used to develop a list of changes which provide an audit trail of the computer-based system's evolution. Even though these controls may frustrate programmers and sometimes cause delays in fixing applications, they are beneficial because they encourage data processing personnel to exercise more caution over changes to accepted production systems.

AUDIT PROCEDURES

Use the background material obtained in section II and:

1. Complete questionnaire 5 on system design, development and modification controls. Pay particular attention to the computer-based system being evaluated.
2. Complete the appropriate section of profile 2 on general controls.
3. On the basis of the level of potential risk determined on the general controls profile 2, consult the general controls matrix 2 at the end of this section for guidance on additional audit steps.

SYSTEM DESIGN, DEVELOPMENT, AND MODIFICATION CONTROLS

The adequacy and effectiveness of controls in computer-based systems begin with the methods and procedures used during the system development process. The agency should have a structured design, development, and modification process which provides adequate separation of duties and assures user, management, and internal auditor participation. Additional key elements are adequate documentation, effective computer program testing, effective system acceptance testing, and effective computer program change control procedures.

The auditor should evaluate the total system development process used by the agency, paying strict attention to the key elements outlined above.

	YES	NO
SYSTEM DEVELOPMENT LIFE CYCLE		
1. Does the agency have a formal, management controlled approach for system development?	___	___
2. Does the system development process include the following steps:		
--User needs definition?	___	___
--Conceptual system design?	___	___
--Feasibility study?	___	___
--Cost-benefit analysis?	___	___
--Detailed system analysis and design?	___	___
--Programming?	___	___
--Testing?	___	___
--Procedure preparation?	___	___
--Conversion?	___	___
--System acceptance?	___	___
--Operations?	___	___
--Postimplementation audit?	___	___

QUESTIONNAIRE 5

		YES	NO
3.	Are formal requests for new or revised systems prepared by users and submitted with proper authorization signatures?	___	___
4.	Are these users' needs used to develop the conceptual system design?	___	___
5.	Is this conceptual design used to determine the technical and operational feasibility of the system?	___	___
6.	Is a cost-benefit analysis performed to make sure that the conceptual system will produce desired results economically?	___	___
7.	Were additional hardware and/or system software needs considered in the cost-benefit analysis?	___	___
8.	If so, is the additional hardware and/or system software requirement consistent with the agency's short- and long-range plans?	___	___
9.	Was the detailed system design consistent with the conceptual design and was it based on the feasibility study and cost-benefit analysis?	___	___
10.	Was the detailed system design used to prepare computer programs?	___	___
11.	Upon completion of all programming, is each program, interrelated subsystem, and the entire system thoroughly tested?	___	___
12.	Are program and system test results reviewed and signed by the systems analyst?	___	___
13.	Were all processing procedures--both manual and automated--prepared before implementation and reviewed to make sure that the detailed design specifications were followed?	___	___
14.	Are there effective procedures to insure that no data is lost or erroneously changed during conversion to the newly designed system?	___	___

QUESTIONNAIRE 5

	YES	NO
15. Was sufficient computer time allocated for the conversion process?	___	___
16. Was the newly designed system tested in parallel with the old system?	___	___
17. Was sufficient time allocated for parallel processing to allow for adequate comparison of results from both processes?	___	___
18. Was the system "acceptance tested" to insure that it performed in accordance with functional and detailed performance specifications, including desired controls, and meets user needs and objectives?	___	___
19. Was this system acceptance performed by a group independent of the programmers and analysts who designed the system?	___	___
20. Does the system acceptance process evaluate both manual and automated procedures?	___	___
21. Does the system acceptance group certify in writing that the computer-based system performs in accordance with all functional and performance specifications?	___	___
22. Are all scheduled and emergency computer program modifications evaluated by the independent system acceptance group?	___	___
23. Does the system acceptance group control all changes to the computer-based system in order to maintain its integrity on a continuing basis?	___	___
24. When the system is ready for initial operation, is its implementation co-ordinated with all personnel involved and other systems affected?	___	___
25. After the system is in operation for several months, is a postimplementation audit of the entire system--both manual and automated--performed by the internal audit staff?	___	___

QUESTIONNAIRE 5

	YES	NO
26. Are at least the following personnel (or their equivalents) involved in the system development process:		
--Project manager?	___	___
--Users?	___	___
--Systems analysts?	___	___
--Programmers?	___	___
--Acceptance testers?	___	___
--Internal auditors?	___	___
27. Are duties of the different personnel assigned to the development project clearly separated?	___	___
28. Is each person assigned to the development project aware of his/her responsibility?	___	___
29. Have specific tasks and time frames for completing tasks been established for each member of the development project?	___	___
30. Is the project manager authorized to make decisions on personnel resources, scheduling, costs, budgets, and most technical project matters?	___	___
31. Is the project manager sufficiently supported by top management to accomplish the system development project?	___	___
32. Have adequate resources been provided to successfully complete the system development project?	___	___
33. Does top management track system development projects to make sure that objectives and time schedules are being met?	___	___
34. Do users actively participate in system development projects?	___	___

QUESTIONNAIRE 5

	YES	NO
35. Is the user the final authority on whether the system meets its intended purpose (i.e., does the user have the final "go/no go" decision to place the system in operation)?	___	___
36. Are all interested parties represented on the development team?	___	___
37. If not, has a mechanism been established so they can provide input to the team?	___	___
38. Are documentation and programming standards adhered to during the system development project?	___	___
DOCUMENTATION		
39. Do agency standards exist for documenting different data processing functions?	___	___
40. Has a project request document been prepared to provide the means for a user to request the development, procurement, or modification of software or other ADP-related services?	___	___
41. Does the project request document include the following:		
--A statement of objectives to be accomplished by the proposed project?	___	___
--A description of the service to be performed?	___	___
--The reason for the request?	___	___
--A description of how the requested project relates to other systems?	___	___
--A statement on privacy and security considerations?	___	___
--A list of those organizations that will be affected by the proposed project?	___	___
--A list of pertinent reference documents on the project?	___	___

QUESTIONNAIRE 5

	YES	NO
42. Has the project request document been annotated by the receiving organization with the following:		
--The date the request was received?	___	___
--The individual assigned to investigate the request?	___	___
--The disposition of the request?	___	___
--An estimated cost for completing a feasibility study or other analysis, and the project as a whole?	___	___
--Any additional information such as problems encountered or references to other pertinent information?	___	___
43. Has a feasibility study document been prepared to provide the following:		
--An analysis of the objectives, requirements, and system concepts?	___	___
--An evaluation of alternative approaches?	___	___
--An identification of a proposed approach?	___	___
44. Does the document include the following:		
--A description of the requirements of the proposed system?	___	___
--A statement of the major performance objectives of the proposed system?	___	___
--An analysis of existing systems which currently address the proposed system's requirements and objectives?	___	___
--A detailed description of the proposed system?	___	___
--A discussion of alternative systems or approaches?	___	___

QUESTIONNAIRE 5

	YES	NO
--The rationale for recommending the proposed system?	___	___
--A proposed schedule for system development?	___	___
45. Has a cost-benefit analysis document been prepared to give managers, users, designers, and auditors adequate cost and benefit information to analyze and evaluate alternative approaches?	___	___
46. Does the document include the following:		
--A description of alternative systems or approaches?	___	___
--The cost of development and operation of each alternative?	___	___
--The benefits which could be attained through the development of each alternative?	___	___
--A comparative cost-benefit summary?	___	___
--A sensitivity analysis assessing the extent to which costs or benefits would be affected by changes in key factors?	___	___
47. Has a functional requirements document been prepared to provide the basic understanding between users and designers of the system?	___	___
48. Does the document include:		
--A statement of objectives to be met by the new computer-based system?	___	___
--A description of existing methods and procedures?	___	___
--A description of proposed methods and procedures?	___	___
--A summary of expected improvements?	___	___
--A summary of impacts?	___	___

QUESTIONNAIRE 5

	YES	NO
--Cost considerations of the proposed computer-based system?	___	___
--A description of alternative proposals?	___	___
--The performance requirements of the new system?	___	___
--A description of inputs and outputs?	___	___
--A description of data elements, dictionaries, tables, and reference files?	___	___
--A description of contingency steps to be taken in the event of hardware/software failures?	___	___
--A description of the equipment needed to process the system?	___	___
--A description of system software needed to support the system?	___	___
--A description of interfaces with other systems?	___	___
--The security and privacy requirements of the system?	___	___
--A description of controls over and within the system?	___	___
--A plan for developing and implementing the proposed system?	___	___
49. Has a data requirements document been prepared to provide a data description and technical information about data collection requirements?	___	___
50. Does it describe:		
--All required data?	___	___
--Data collection requirements, responsibilities, procedures and impacts?	___	___

QUESTIONNAIRE 5

	YES	NO
51. Have detailed system/subsystem specifications been developed for the computer-based system?	___	___
52. Do they include:		
--An overall narrative description of the system?	___	___
--Its performance requirements?	___	___
--The equipment configuration needed to process the system?	___	___
--The system software needed to support the system?	___	___
--The interfaces with other systems?	___	___
--The security and privacy requirements of the system?	___	___
--The operational controls over the system?	___	___
--The design characteristics of the system, including a system flowchart?	___	___
53. Have detailed program specifications been developed for all programs of the system?	___	___
54. Do these specifications include the following:		
--A general narrative description of the program and its functions?	___	___
--The program's performance requirements?	___	___
--The equipment required to operate the program?	___	___
--The system software needed to support the program?	___	___
--A description of all interactions by computer operators?	___	___
--The storage requirements of the program, including the amount of		

QUESTIONNAIRE 5

	YES	NO
internal storage, and the amount and type of off-line storage?	___	___
--The security and privacy requirements of the program?	___	___
--The controls over and within the program?	___	___
--Lists of constants, codes, and tables used?	___	___
--The operating procedures of the program?	___	___
--The input record formats and descriptions?	___	___
--A description of the program's logic, including flowcharts and decision tables, supplemented by narrative explanations?	___	___
--The output record formats and descriptions?	___	___
--The logical and physical characteristics of all data bases used by the program including file layouts and data element definitions?	___	___
--Source program listing?	___	___
--Object program listing?	___	___
55. Have detailed specifications been developed for data bases used by the computer-based system?	___	___
56. Do these specifications include the following:		
--The data base identifications?	___	___
--The system(s) using the data base?	___	___
--The labeling and tagging conventions used when accessing the data base?	___	___
--Any special instructions for using it?	___	___

QUESTIONNAIRE 5

	YES	NO
--The system software needed to support it?	___	___
--Its logical characteristics?	___	___
--Its physical characteristics?	___	___
57. Has a users manual been developed which documents the functions of the computer-based system?	___	___
58. Does this manual include:		
--A narrative description of the computer-based system?	___	___
--A description or diagram of the computer-based operation?	___	___
--A description of the equipment needed to process the system?	___	___
--The structure and role of each system component?	___	___
--The performance capabilities of the system?	___	___
--A description of all data files used by the system?	___	___
--A description of the inputs, the flow of data through the processing cycle, and the outputs?	___	___
--The step-by-step procedures required to initiate processing?	___	___
--The requirements for preparing and entering input data?	___	___
--The requirements relevant to each output, such as format, frequency, etc.?	___	___
--A list of error codes or conditions generated by the system and the corrective actions to be taken by the user?	___	___
--The detailed instructions necessary to intiate, prepare, process, and receive a query applicable to the data base?	___	___

QUESTIONNAIRE 5

	YES	NO
59. Has an operations manual been developed which describes the computer-based system and its operational environment for computer operations personnel?	___	___
60. Does this manual include:		
--A diagram showing the inputs, outputs, data files, and sequence of operations of the computer-based system?	___	___
--An inventory of all programs included in the system?	___	___
--An inventory of each permanent file that is referenced, created, or updated by the system?	___	___
--A list of the various runs possible and a summary of each run's purpose?	___	___
--A description of the manner in which progressive advances from one run to another is made to complete the entire run cycle?	___	___
--The job control statements needed for each run?	___	___
--Operator instructions for each run?	___	___
--The input and output files for each run?	___	___
--The output reports produced for each run?	___	___
--The output reports that need to be reproduced by other means?	___	___
--The restart/recovery procedures for each run?	___	___
--Any emergency procedures?	___	___
--A description of procedures for running the computer-based system through remote devices?	___	___

QUESTIONNAIRE 5

	YES	NO
61. Does the operations manual exclude:		
--Program logic charts or decision tables?	___	___
--Copies of program listings?	___	___
62. Are program listings inaccessible to computer operations personnel?	___	___
63. Are computer operations personnel denied access to other program and system documentation?	___	___
64. Has a program maintenance manual been developed which gives the maintenance programmer sufficient information to understand the programs, their operating environment, and their maintenance procedures?	___	___
65. Does this manual include:		
--A detailed description of each program in the computer-based system?	___	___
--The equipment needed to process it?	___	___
--The system software needed to support the application programs?	___	___
--A description of the data base being used by the application programs?	___	___
--A description of the programming conventions used to develop the application programs?	___	___
--A description of all error conditions, their sources, and procedures for their correction?	___	___
--Program listings and flowcharts of decision tables?	___	___
66. Has a plan been documented to test the computer-based system?	___	___

QUESTIONNAIRE 5

		YES	NO
67.	If so, does it include the detailed specifications, descriptions, and procedures for all tests?	___	___
68.	Does it include test data reduction and evaluation criteria?	___	___
69.	Has a test analysis report been developed which documents the test analysis results and findings?	___	___
70.	If so, does it present the demonstrated capabilities and deficiencies of the computer-based system?	___	___
71.	Is the report used to prepare a statement of the system's readiness for implementation?	___	___
72.	Is all documentation periodically reviewed to insure that it is current and complete and adheres to established standards?	___	___
73.	Are copies of all documentation stored off the premises?	___	___
74.	If so, is the stored documentation periodically compared and updated with that being used?	___	___
75.	Is there written evidence of who performed the systems and programming work?	___	___
76.	Do documented procedures exist for controlling all system documentation?	___	___

PROGRAM TESTING AND SYSTEM ACCEPTANCE

77.	Are all computer programs desk checked by the programmer and his/her supervisor before program assembly or compilation?	___	___
78.	Are all computer programs reviewed after assembly or compilation to insure that errors disclosed by these translator routines are corrected?	___	___

QUESTIONNAIRE 5

	YES	NO
79. Is test data, as opposed to live data, used to test computer programs?	___	___
80. Is each program, subsystem, and then the entire system, tested?	___	___
81. Is test data treated just like live data, as opposed to having special codes entered in the test data to indicate it is not normal production data?	___	___
82. Are sufficient volumes of test transactions entered which have a wide range of valid and invalid conditions?	___	___
83. Is sufficient time allocated for thorough testing?	___	___
84. Have sufficient staff members been allocated for testing purposes?	___	___
85. Are there test cases which evaluate the following:		
--Mainline and end-of-job logic?	___	___
--Each routine?	___	___
--Each exception?	___	___
--Abnormal end-of-job conditions?	___	___
--Combinations of parameter cards and switch settings?	___	___
--Unusual mixtures and sequences of data?	___	___
86. Does the test data include cases which test for the following types of valid conditions:		
--Codes?	___	___
--Characters?	___	___
--Fields?	___	___
--Combinations of fields?	___	___
--Transactions?	___	___
--Calculations?	___	___

QUESTIONNAIRE 5

	YES	NO
--Missing data?	___	___
--Extraneous data?	___	___
--Amounts?	___	___
--Units?	___	___
--Composition?	___	___
--Logic decisions?	___	___
--Limit or reasonable checks?	___	___
--Sign?	___	___
--Record matches?	___	___
--Record mismatches?	___	___
--Sequence?	___	___
--Check digit?	___	___
--Crossfooting of quantitative data?	___	___
--Control totals?	___	___
87. Are programming aid software packages used to improve computer programs' efficiency and effectiveness?	___	___
88. Are new programs run parallel to old ones to help assure their accuracy?	___	___
89. Are all computer-based systems subjected to a system acceptance process?	___	___
90. Does this system acceptance evaluate whether the entire system, both manual and automated processes, is performing in accordance with system specifications and processing standards?	___	___
91. Is system acceptance performed by individuals independent of the analysis, design, and development of the system?	___	___
92. Once system acceptance has been completed, is a written certification that the		

		YES	NO
	entire system performs in accordance with all functional and performance specifications required before the system can be placed in operation?	___	___
93.	Is system acceptance performed using test data similar to, but independent of, program testing data?	___	___
94.	Are system acceptance transactions tested just like live transactions, as opposed to having special codes entered in the transaction to indicate that it is not normal production data?	___	___
95.	Are sufficient volumes of system acceptance transactions entered and processed which have a wide range of valid and invalid conditions?	___	___
96.	Is sufficient time allowed for system acceptance purposes?	___	___
97.	Have sufficient staff members been allocated for system acceptance purposes?	___	___
98.	Are there system acceptance test transactions which evaluate the following:		
	--Mainline and end-of-job logic?	___	___
	--Each routine?	___	___
	--Each exception?	___	___
	--Abnormal end-of-job conditions?	___	___
	--Combinations of parameter cards and switch settings?	___	___
	--Unusual mixtures and sequences of data?	___	___
99.	Does system acceptance data include cases which test for the following types of valid conditions:		
	--Codes?	___	___
	--Characters?	___	___
	--Fields?	___	___

QUESTIONNAIRE 5

	YES	NO
--Combinations of fields?	___	___
--Transactions?	___	___
--Calculations?	___	___
--Missing data?	___	___
--Extraneous data?	___	___
--Amounts?	___	___
--Units?	___	___
--Composition?	___	___
--Logic decisions?	___	___
--Limit or reasonableness checks?	___	___
--Sign?	___	___
--Record matches?	___	___
--Record mismatches?	___	___
--Sequence?	___	___
--Check digit?	___	___
--Crossfooting of quantitative data?	___	___
--Control totals?	___	___

PROGRAM CHANGES

100.	Are computer programs revised only after written request by users and approval by user department management?	___	___
101.	Do these written requests describe the proposed changes and reasons for them?	___	___
102.	Do these requests include security/ privacy specifications?	___	___
103.	Is a change request form or other means of documentation used to originate program modifications?	___	___
104.	If so, are all change request forms sequentially numbered and accounted for?	___	___

QUESTIONNAIRE 5

		YES	NO
105.	Are program modifications thoroughly tested to make sure that the modification functions properly?	___	___
106.	Are program modifications subjected to system acceptance before being placed in operation?	___	___
107.	Is there a limit on the number of times programs can be changed?	___	___
108.	Are departments that initiate changes in master files or program instructions furnished with a notice or other documentation showing changes actually made?	___	___
109.	Do users make the final decision on whether the modification meets their needs?	___	___
110.	Is program documentation changed to reflect program modifications?	___	___
111.	Is system documentation changed to reflect program modifications?	___	___
112.	Is operations documentation changed to reflect program modifications?	___	___
113.	Is user documentation changed to reflect program modifications?	___	___
114.	Are procedures in place to determine if any other system is affected by the program modifications?	___	___
115.	Does the volume of regularly scheduled program modifications indicate a problem with programs, procedures, or the computer-based system?	___	___
116.	Do computer operations personnel have a list of individuals to notify if a computer-based system requires an emergency or immediate modification?	___	___
117.	Are individuals on the above list the only application programmers allowed in the computer room?	___	___

QUESTIONNAIRE 5

		YES	NO
118.	Is access to other data files and programs denied to the programmer making an emergency modification?	___	___
119.	Is the programmer making the emergency modification denied access to the data files that the program was using when the problem occurred?	___	___
120.	Do computer operations personnel document the problems and give that documentation to the ADP department manager?	___	___
121.	Is the responsible user always notified that an emergency modification has been made?	___	___
122.	Is the system's project manager always notified that an emergency modification has been made?	___	___
123.	Are all emergency modifications made to both the source module and the executable load module?	___	___
124.	Does the programmer making the emergency modification complete a statement and leave it with the computer operator as to the problem encountered, and the fix made?	___	___
125.	Is the individual making the emergency modification required to perform sufficient testing to assure that the emergency modification will function properly?	___	___
126.	Are procedures established to insure that the emergency modification is immediately subjected to a system acceptance test?	___	___
127.	Are procedures established so that the system-accepted emergency modification will be incorporated into the next production version of the system?	___	___
128.	Does the volume of emergency modifications indicate a problem with programs, procedures, or the computer-based system?	___	___

		YES	NO
129.	Are outdated source programs deleted from the production source program library?	___	___
130.	Are outdated load modules deleted from the executable load module library?	___	___
131.	Are job control statements relating to outdated programs discarded?	___	___
132.	Is documentation relating to outdated programs discarded?	___	___
133.	Is there a procedure to prevent suspended programs from being used by mistake?	___	___
134.	Is a special library used for source programs or executable load modules during the testing and system acceptance phases?	___	___
135.	Is an executable load module library used for production processing?	___	___
136.	Does the executable load module library keep track of the day, date, sequence, who made the change, and the change, etc.?	___	___
137.	Are computer programs protected from unauthorized access?	___	___
138.	Does the agency use automated methods (such as a program library system software package) to restrict access to computer programs?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

DATA CENTER MANAGEMENT CONTROLS

The accuracy and completeness of information maintained and processed by an agency's data processing function depend in part on controls over operations of the data center. Inadequate controls or failure to comply with procedures can result in errors in data preparation and handling, production scheduling, file updating, and output report preparation. Certain key areas of the data center's operation should be well controlled to help prevent or reduce the probability of erroneous or fraudulent processing.

Input/output control and scheduling

Within the center, a control group should be established to receive all data for processing, to see that all errors detected during processing are corrected, and to insure that all output reports are properly distributed. This group should be responsible for scheduling all work to be processed. This procedure permits computer operators to concentrate on physical operations of the computer and limits contact between operators and various user departments.

The group normally maintains control logs of anticipated and received inputs. It records, summarizes, and reconciles totals to interim and final output totals for each production application. The group also makes sure that all input data is properly authorized.

The group should use an error log to account for errors made during production processing and to make sure they are corrected and reentered into the system. The group determines the nature

of the error and forwards it to the proper source for correction. Error logs can also identify for supervisors the magnitude of errors and needed corrective action.

The disposition of computer produced output reports is also the function of the control group. All output reports should be visually scanned for general accuracy and completeness before being distributed. Reruns of aborted or erroneous processing should be scheduled by the group. All control totals should be balanced with those received from the user department.

Effective scheduling of production applications is also an important part of the control group's function. These schedules must be established to accommodate input availability, data preparation time, computer hardware resources and availability, and time required for processing and output distribution. The scheduling process can become quite complex in a multiprogramming environment where more than one application is being processed simultaneously.

Production scheduling and input/output controls may be bypassed when remote job entry (RJE) devices are used by an application. An RJE device permits users to submit work directly into the computer and receive output reports from their RJE station. In this environment, the computer is normally used to schedule the work; different jobs accumulate in a queue for processing. As required computer resources become available, jobs are released from the queue and necessary tapes or disks are mounted. Having a control group manage operations of RJE devices is essential to maintaining integrity of the application.

Malfunction reporting and preventive maintenance

Since failures of the computer system can result in errors and omissions in computer data, formal procedures should be established for reporting the occurrence of hardware and software malfunctions. Such reporting provides a measure of the adequacy of preventive maintenance, the level of vendor maintenance service provided, and the rate of failure associated with the computer-based system.

Operations logs kept manually by operators provide a method of recording computer operations and a starting point for analysis. These logs should account for all computer processing time, including downtime for preventive maintenance, abnormal job terminations, and job reruns. In addition, console logs should automatically record computer operations. Regular analysis of operation and console logs helps identify causes of malfunctions and facilitate corrective measures. This analysis may disclose that a given vendor is not providing adequate service; therefore, management attention should be directed toward compliance with contract provisions.

Some malfunctions may occur because computer operations personnel are not performing preventive maintenance according to agency or vendor procedures. These deficiencies normally show up as computer malfunctions. Special care should be used when analyzing operations logs so that the causes of all malfunctions are discovered.

User billing/chargeout procedures

An agency data processing department incurs significant costs in providing data processing services to users. These services require use of various pieces of equipment and supplies. Costs should be reported and charged to users on the basis of resources used, time required for processing, and response time requested by users. System development costs plus costs for additional overhead items, such as space, lighting, and air conditioning, must also be apportioned to users. All costs should be derived on a fair and equitable basis, in accordance with agency policy and procedures, documented user/ADP department agreements, and Federal standards. For criteria, refer to GAO's Federal Government Accounting Pamphlet Number 4, "Guidelines for Accounting for Automatic Data Processing Costs," dated 1978; and Office of Management and Budget Circular A-121 "Cost Accounting, Cost Recovery, and Inter-Agency Sharing of Data Processing Facilities," dated September 16, 1980.

Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used. Care should be exercised so that users are not charged for preventive maintenance or reruns caused by errors made by the data processing department.

AUDIT PROCEDURES

Use the background material obtained in section II and:

1. Complete questionnaire 6 on data center management controls.

2. Complete the appropriate section of profile 2 on general controls.
3. On the basis of the level of potential risk determined on the general controls profile 2, consult the general controls matrix 2 at the end of this section for guidance on additional audit steps.

DATA CENTER MANAGEMENT CONTROLS

The accuracy and completeness of information processed by an agency's data processing function depends, in part, on the controls over the operations of the data center. The main areas of control include

--input/output control and scheduling,

--malfunction reporting and preventive maintenance, and

--user billing/chargeout procedures.

The auditor should determine the adequacy of the controls over the center and the level of management exercised.

	YES	NO
INPUT/OUTPUT CONTROL AND SCHEDULING		
1. Has a formal control group been established within the data center?	___	___
2. Have formal input/output control procedures been established? (If so, attach a copy.)	___	___
3. Is the control group responsible for recording and controlling all production data processed by the data processing department?	___	___
4. Does the control group keep logs of all computer-based systems?	___	___
5. Do these logs include the following:		
--Name of application?	___	___
--Record counts and predetermined control totals of input transactions?	___	___
--Run-to-run totals?	___	___
--Record counts and predetermined control totals of error transactions?	___	___
--Record counts and predetermined control totals of updated master files?	___	___

		YES	NO
	--Record counts and predetermined control totals of output transactions?		
6.	Are all totals balanced during and after the application processing?	___	___
7.	Are all errors disclosed during processing controlled by the control group to insure that they are corrected promptly?	___	___
8.	Does a supervisor initial each log to indicate that a review has been performed?	___	___
9.	Does the control group require an authorization document or a transmittal sheet to accompany all input transactions?	___	___
10.	Does the group visually scan all output reports for general accuracy and completeness?	___	___
11.	Does the group distribute output reports according to a formal schedule?	___	___
12.	Is the group responsible for scheduling production runs and other workloads?	___	___
13.	Is it responsible for rescheduling of aborted or erroneous processing?	___	___
14.	Have formal scheduling procedures been established? (If so, attach a copy.)	___	___
15.	Is a priority scheme used for scheduling work?	___	___
16.	Is there a schedule of all computer-based systems which includes:		
	--A brief description of the function of each?	___	___
	--The date of approval?	___	___
	--The identification number?	___	___
17.	Is the mix of jobs aimed at getting the proper performance out of the data center's resources?	___	___
18.	If an RJE is used, has a control group been established to govern its operation?	___	___

QUESTIONNAIRE 6

	YES	NO
19. Does the computer system schedule the work submitted through the RJE?		
20. Is the group responsible for all negotiable instruments?	___	___
21. Have formal procedures been established governing the requisition and accounting for all blank stock of negotiable instruments? (If so, attach a copy.)	___	___
22. Is the receipt of negotiable instruments inventoried by two people at the time of delivery?	___	___
23. Are negotiable instruments, damaged or voided during processing, destroyed in the presence of two or more people?	___	___
24. When negotiable instruments are being processed by the computer, are two or more people present?	___	___
25. Are all negotiable instruments periodically inventoried by the control group?	___	___
MALFUNCTION REPORTING AND PREVENTIVE MAINTENANCE		
26. Has a formal malfunction reporting procedure been established for the data processing department? (If so, attach a copy.)	___	___
27. Are computer operators required to keep logs of all computer processing actions?	___	___
28. Do these logs record:		
--Startup?	___	___
--Errors?	___	___
--Reruns?	___	___
--Recoveries?	___	___
--Shutdowns?	___	___
--Shift changes?	___	___

QUESTIONNAIRE 6

	YES	NO
--Maintenance?	___	___
--Other?	___	___
29. Are all processes and operator decisions recorded on the operations log?	___	___
30. Does a supervisor initial each log to indicate that a review has been performed?	___	___
31. Does the computer system automatically produce a log of all system operations?	___	___
32. Does the console log list:		
--Date?	___	___
--Job name and/or number?	___	___
--Program name and/or number?	___	___
--Start/stop times?	___	___
--Files used?	___	___
--Record counts?	___	___
--Halts (programmed and unscheduled)?	___	___
33. If the system does not have a console typewriter, does some other method afford adequate control and record the activities performed by both the computer and operator?	___	___
34. Is all computer time accounted for from the time the computer is turned on, until it is shut down?	___	___
35. Are disposition notes entered on the console log showing corrective actions taken when unscheduled program halts occur?	___	___
36. Are job reruns recorded on the console log?	___	___
37. Is the reason for each rerun recorded?	___	___

QUESTIONNAIRE 6

	YES	NO
38. Are log pages sequentially numbered?	___	___
39. Is the log reviewed and signed at the end of each shift by a supervisor and filed as a permanent record?	___	___
40. Are logs independently examined to detect operator problems and unauthorized intervention?	___	___
41. Have formal preventive maintenance procedures been established for the data processing department? (If so, attach a copy.)	___	___
42. Is there documented evidence of the type and time of maintenance performed?	___	___
43. Is a schedule for machine maintenance published and followed?	___	___
44. Is sensitive data removed from all on-line storage devices before equipment is turned over to maintenance personnel?	___	___
USER BILLING/CHARGEOUT PROCEDURES		
45. Are there documented procedures for user billing/chargeout?	___	___
46. Are there user/data processing department billing/chargeout agreements? (If so, attach copies.)	___	___
47. Are the user billing/chargeout procedures effectively tied into a job accounting system for the data processing department's resources?	___	___
48. Are the user billing/chargeout procedures based on the number of transactions processed?	___	___
49. Are they based on an artificial "computer accounting unit"?	___	___
50. Are there adequate procedures for determining the share of overhead costs for billing users?	___	___
51. Are additions to the equipment, software, etc., justified on the basis of resource utilization and user needs?	___	___

QUESTIONNAIRE 6

	YES	NO
52. Are there adequate procedures for determining why costs are not charged to users?	___	___
53. Is there an equitable procedure for charging reruns of production jobs so that user errors are charged to users and data processing department errors are not charged to users?	___	___
54. Are present data processing department costs in line with budgeted costs?	___	___
55. Is the method of charging the data processing department's costs equitable?	___	___
56. Is the method of charging the data processing department's costs in the interest of minimizing the use of agency resources?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

DATA CENTER PROTECTION CONTROLS

Computers, information, and data are assets that should be managed properly and protected against theft, loss, unauthorized manipulation, fraudulent activities and natural disasters. To minimize these risks, data center protection controls need to be established. These include

- --limiting access to the center, system documentation, computer programs, and outputs,
- --establishing and enforcing strict procedures over maintenance, storage, and access to computer-processed magnetic tapes, disk packs, and other data storage media, and
- --establishing and maintaining preventive procedures that help protect critical files, programs, and system documentation from fire or other natural disasters.

The effectiveness of these controls helps assure reliability of data processed.

Security and access

Within the data processing department, security procedures need to be established over personnel, facilities, hardware, software, data, and documentation. Before these procedures are established, an analysis should be performed to determine the level of risk and the potential adverse impact that unauthorized or malicious acts could have on the agency. The responsibility for performing such an analysis should be formally assigned within the agency. This analysis should be periodically updated. A risk analysis should also be performed before design specifications for new computer installations are approved. Risk analysis procedures should be consistent with Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1 "Security of Federal Automated Information Systems," dated July 27, 1978.

Employees who run the data center can usually cause more damage or erroneous processing than outsiders. Therefore, procedures should be established to screen all employees before they are hired. Screening should consider the sensitivity of functions that employees perform. Also they should be required to sign agreements with the agency which detail their responsibilities in maintaining adequate protection over the data center and the data being processed. In addition, procedures should be established to immediately restrict terminating employees from the data center or other critical data processing department operations. The agency's personnel policies should be consistent with Federal Property Management letter 732-7.

Access to the computer area should be limited to authorized personnel. Doors and other access ways should be equipped with locks, security badge readers, or other means to restrict unauthorized access. Both exterior walls and walls inside the computer area around critical data or forms should be of solid construction from floor to ceiling. At least two people should be in the area at all times. Data processing personnel should be present when custodial or maintenance personnel are in the area.

Critical documents or forms, such as blank checks or bond stock, should be adequately controlled. Access to input forms, such as source documents, should also be restricted. These forms should be accounted for and periodically inventoried. They should be prenumbered whenever possible. Also, two or more people should be present when critical forms are received, inventoried, processed, destroyed, or distributed.

Files

The data processing department is directly responsible for data that it maintains for user departments. Formal documented procedures need to be established governing all data processed and maintained. A library, established within the data center and staffed by a full-time librarian during all shifts, should be responsible for issuing and storing magnetic tapes, disks, or other data storage media. Operations personnel's access to the library should be restricted. The librarian should also maintain control logs or use automated methods, such as a file maintenance system software package, which records the acceptance and issuance of files in and out of the library.

Labels should be affixed to all active tapes or disks unless these media are controlled by automated methods. These labels should agree with library inventory records. To help reduce the possibility of incorrectly issuing and using active tapes, a separate area within the library should be set aside for work, inactive, or scratch tapes.

Disaster recovery

Procedures should be established to help protect critical files, programs, and system documentation from fire or other natural disasters. These procedures should be formally documented and periodically updated and tested. They should contain the detailed steps computer operations personnel should take in the event of an emergency. They should be required reading.

The data center should be equipped with both smoke and fire detection devices. Floors, walls, ceilings, and draperies

should be made of noncombustible material. Portable fire extinguishers should also be easily available, and computer operations personnel should be trained in their use.

Power and air-conditioning circuits and switches should be easily accessible within the data center. Air intakes and the air-conditioning units themselves should be protected against the introduction of noxious substances. Alternate power sources or other electrical backup devices should be installed to limit the impact of a power shortage or blackout.

Formal backup arrangements should also be established with another compatible data center. Copies of critical files, programs, and documentation should be stored at an offsite location. Steps should be taken to make sure that the offsite materials are periodically updated and that the backup center has sufficient capacity to process the additional workload. Periodic tests of the backup arrangements should also be performed.

AUDIT PROCEDURES

Use the background material obtained in section II and:

1. Complete questionnaire 7 on data center protection controls.
2. Complete the appropriate section of profile 2 on general controls.
3. On the basis of the level of potential risk determined on the general controls profile 2, consult the general controls matrix 2 at the end of this section for guidance on additional audit steps.

DATA CENTER PROTECTION CONTROLS

Computer resources and data should be protected against unauthorized access to reduce erroneous or fraudulent activities. Formal documented procedures should be established describing actions to be taken in the event of fire or other natural disasters.

The auditor should evaluate protection controls over the data center and the adequacy of emergency procedures and backup arrangements.

	YES	NO
SECURITY AND ACCESS		
1. Has overall agencywide responsibility for conducting periodic risk analyses been formally assigned? (If so, to whom?)	___	___
2. Does the risk analysis measure vulnerability related to the potential for the following:		
--Fraud or theft?	___	___
--Inadvertent error or improper disclosure of information?	___	___
--Financial loss?	___	___
--Harm to individuals or infringement on privacy rights?	___	___
--Loss of proprietary data and harm to agency activities?	___	___
3. Has a specific timetable for conducting risk analyses been established?	___	___
4. Is the interval between risk analyses commensurate with the sensitivity of the information processed?	___	___
5. Is the interval between risk analyses at most every 5 years?	___	___
6. Do agency procedures require that a risk analysis be performed before the approval of design specifications for computer installations?	___	___

QUESTIONNAIRE 7

		YES	NO
7.	Do agency procedures require that a risk analysis be performed whenever there is a "significant change" to the physical facility, hardware, or operating system software?	___	___
8.	Has the agency defined "significant change"?	___	___
9.	Is the definition of "significant change" commensurate with the sensitivity of the information processed by the installation?	___	___
10.	Are requirements established for conducting risk analyses for Government-owned contractor-operated facilities as well as Government operated facilities?	___	___
11.	Do agency plans provide for assessing risks related to computer services provided by other agencies and those provided through commercial services?	___	___
12	Has overall agencywide responsibility for computer security been formally assigned? (If so, to whom?)	___	___
13.	Has the agency assigned responsibility for computer security at each headquarters and field organization?	___	___
14.	Do the individuals assigned responsibility for computer security have both computer and security experience?	___	___
15.	Are all employees required to sign an agreement regarding their role and responsibility in the department and the ownership and use of data processing equipment and information within the data center?	___	___
16.	Have personnel security policies for screening employees been established and implemented?	___	___
17.	Do these policies provide for levels of screening commensurate with the sensitivity of the position or function?	___	___

QUESTIONNAIRE 7

	YES	NO
18. Have screening requirements for contractor/ service personnel been established and implemented?	___	___
19. Are the personnel policies consistent with FPM letter 732-7?	___	___
20. When an employee is terminated, are the following precautions taken immediately:		
--The employee is denied access to the data processing department?	___	___
--The employee is denied access to any data, program listings, etc.?	___	___
--All other employees are informed of the employee's termination?	___	___
21. Is there a procedure to be followed if an employee becomes a suspected security risk?	___	___
22. Is access to the computer area limited to only authorized personnel?	___	___
23. Do combination locks, security badges, or other means restrict access to the computer room?	___	___
24. Are combinations on locks or similar devices periodically changed?	___	___
25. Are account codes, authorization codes, passwords, etc. controlled to prevent unauthorized use?	___	___
26. Are restricted entrances and emergency exits equipped with tamperproof automatic alarm systems that signal when doors are opened?	___	___
27. Are exterior walls, tape library walls, storage room walls, etc., of solid construction from floor to ceiling?	___	___
28. Are data processing personnel trained to challenge improperly identified visitors?	___	___

QUESTIONNAIRE 7

		YES	NO
29.	Are data processing personnel counseled to report all cases of security intrusions (either intentional or inadvertent) of which they become aware?	___	___
30.	Is access to the computer area by custodial, electrical, and other in-house maintenance personnel controlled?	___	___
31.	Must vendor and support personnel provide positive identification before they can be admitted to the computer area?	___	___
32.	Must data processing personnel be present when service personnel are in the area?	___	___
33.	Are at least two individuals always present in the computer room at all times?	___	___
34.	Is there a method or procedure to restrict access to source documents and blank input forms to authorized employees only?	___	___
35.	Are all critical forms (i.e., negotiable instruments, identification cards, etc.) stored in a secure location and are they accounted for periodically?	___	___
36.	Are source documents, blank input forms, and other critical forms prenumbered for accountability?	___	___
37.	Are procedures in place to limit access to critical forms during their intermediate storage and transportation such as dual custody and mail and message carrier controls?	___	___
38.	Is there a procedure for joint authorization releases from the storage area?	___	___
39.	Is the receipt of critical forms inventoried by two people at the time of delivery?	___	___
40.	Have controls been established over the issuance of critical forms for jobs being scheduled for processing?	___	___

QUESTIONNAIRE 7

	YES	NO
41. When critical forms are processed by the computer, are two or more people always present?	___	___
42. Are copies of critical outputs that need to be destroyed kept in a secure location until they can be destroyed?	___	___
43. When critical outputs are destroyed, are at least two people present?	___	___

FILES

44. Is the responsibility for issuing and storing magnetic tapes, disk packs, or other data storage media assigned to a librarian?	___	___
45. Is this duty the librarian's chief responsibility?	___	___
46. Are library procedures documented?	___	___
47. Is access to the library always limited to the responsible librarian(s)?	___	___
48. Is there a librarian on duty at all times when the data center is being used?	___	___
49. Does the agency use automated methods (such as a file management system software package) to restrict access to computerized files?	___	___
50. Are sensitive files (such as security classification or privacy act restrictions) properly identified as such, and appropriately secured?	___	___
51. Are all data files logged in and out to prevent release to unauthorized personnel?	___	___
52. Are all files expeditiously returned to the library after use?	___	___
53. Are tape and disk inventory records kept?	___	___
54. Are tape and disk status records kept?	___	___
55. Have external labeling procedures been documented?	___	___

	YES	NO
56. Are external labels affixed to active tapes and/or disks?	___	___
57. Do labels tie in with inventory records?	___	___
58. Are work or scratch tapes or disk packs kept in a separate area of the library?	___	___

DISASTER RECOVERY

59. Have emergency procedures been documented?	___	___
60. Do they include steps to take in the event of a natural disaster by fire, water damage, etc., and intentional damage by sabotage, mob action, bomb threats, etc.?	___	___
61. Are employees familar with the emergency procedures?	___	___
62. Is the computer center separated from adjacent areas by fire resistant partitions, walls, etc.?	___	___
63. Have noncombustible flooring, ceilings, and/or draperies been used in the data center?	___	___
64. Are any activities conducted adjacent to the center that might endanger it by flood, fire, or explosion?	___	___
65. Is smoking prohibited in the center?	___	___
66. Are center personnel trained periodically in fire-fighting techniques and assigned individual responsibilities in case of a fire?	___	___
67. Are emergency procedures for handling minor and major fires prominently posted throughout the data center?	___	___
68. Are heat and smoke detectors installed in the following areas:		
--In the ceiling?	___	___
--Under raised floors?	___	___
--In the air return ducts?	___	___

QUESTIONNAIRE 7

		YES	NO
69.	Do these devices alert the local fire department as well as internal personnel?	___	___
70.	Are portable fire extinguishers located in strategic and accessible areas?	___	___
71.	Are they vividly marked?	___	___
72.	Are they periodically tested?	___	___
73.	Are emergency exits and evacuation routes clearly labeled?	___	___
74.	Are battery-powered emergency lights placed in strategic locations to assist in evacuation should power be interrupted?	___	___
75.	Is the computer center protected by an automatic fire suppressing system?	___	___
76.	Are emergency switches for cutting off power easily accessible at the exits of the center?	___	___
77.	Does emergency power shutdown include the air-conditioning system?	___	___
78.	Is the center equipped with temperature and humidity gauges which automatically activate signals if either goes outside the normal range?	___	___
79.	Is the center air-conditioned by a separate system?	___	___
80.	Is the air-conditioning system sufficiently protected from unauthorized access?	___	___
81.	Is the air-conditioning system (duct linings, filters, etc.) made from noncombustible materials?	___	___
82.	Are air intakes protected against introduction of noxious substances?	___	___
83.	Is backup air-conditioning available?	___	___
84.	Is the source of electric power sufficiently reliable to assure continued operations?	___	___

QUESTIONNAIRE 7

		YES	NO
85.	Is the source of electric power sufficiently protected from unauthorized access?	___	___
86.	Is an alternate power source available?	___	___
87.	Is the computer center backed up by an uninterruptible power source system?	___	___
88.	Are there provisions for retaining and/or copying master files and a practical means of reconstructing a damaged or destroyed file?	___	___
89.	Are sufficient generations of files maintained to facilitate reconstruction of records (grandfather-father-son routine)?	___	___
90.	Is at least one file generation kept at a location other than the file storage area?	___	___
91.	Are copies of critical files stored at a remote location and restricted from unauthorized access?	___	___
92.	Are duplicate application programs kept at a remote location and restricted from unauthorized access?	___	___
93.	Are duplicate system software programs kept at a remote location and restricted from unauthorized access?	___	___
94.	Are duplicate copies of critical documentation kept at a remote location and restricted from unauthorized access?	___	___
95.	Is there backup computer capacity within the computer center?	___	___
96.	Is this backup capacity in the same building but in a different computer center?	___	___
97.	Is there backup capacity at an offsite location?	___	___
98.	Have critical locations been provided with the following backup devices:		
	--Terminals?	___	___

	YES	NO
--Modems?	___	___
--Communication lines?	___	___
99. Have these backup arrangements been documented?	___	___
100. Have they been formally agreed to by all parties concerned?	___	___
101. Has a priority scheme been established in the event that backup arrangements must be used?	___	___
102. Are backup procedures periodically tested at the backup data center?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

SYSTEM SOFTWARE CONTROLS

As computers become more sophisticated, many operations previously performed manually are automated within system software. "System software" is defined as any program or system that helps interconnect and/or control the elements of input, output, processing, data, and application programs. Typically, this software is provided by outside vendors. It usually falls into one of the following categories:

--Operating systems.

--System utilities.

--Program library systems.

--File maintenance systems.

--Security software.

--Data communications systems.

--Data base management systems.

Any one category is usually a complete system and could be the basis for a complete audit itself. This section of the guide, however, is intended to be a first-cut evaluation to determine overall relationships between the application and the system software and the extent to which system software controls influence accuracy and reliability of the application. Detailed procedures needed to thoroughly evaluate specific types of system software will be included in later supplements of this guide.

During the first-cut evaluation of system software controls, the auditor has several areas of concern. They are:

--Types and uses of system software.

--Reliance on system software to perform certain control or critical processes.

--Controlling access to system software.

--Controlling changes to system software.

The depth of evaluation depends on the first two areas because they identify the agency reliance on system software.

Types and uses of system software

Most agencies with late second generation or newer equipment heavily use an operating system to

--manage the resources of the computer with a minimum of operator intervention,

--help programmers and operators control the operations and allocation of peripheral devices and other computer resources, and

--minimize the difference between a given manufacturer's line of computers, thus facilitating the transfer of application programs.

In addition, many system utilities, such as copy programs, sorts, etc., are heavily used. To get a better understanding of system software, the auditor should obtain complete technical descriptions and documentation from vendors.

In sophisticated computer centers, system software is used to control application programs, tape and disk computer files, and other resources requiring greater security. For example, program library systems, or packages, normally control all application programs, including access, change, and conversion from source to object code. Most of these packages contain a complete audit trail feature that records all changes made to application programs, including identification of programmers making changes. When properly implemented, this system software helps promote better security and backup of application programs.

File management systems, or packages, perform similar functions concerning security and backup of tape and disk files. These packages help reduce manual library functions and in many cases eliminate the need for external file labels. Audit trails are also normally available that show when a particular file was created and used and by whom.

Security software packages are one of the newer methods of automating access controls. Overall, these are designed to control access to the computer system by identifying and verifying persons who try to gain access to various system resources. Typically, these packages control terminals; remote job entry stations; individual tape, disk, or mass storage data sets; individual application programs; and other system software, such as operating systems, data base management systems, etc. These packages normally provide an audit trail of all accesses, including authorized uses and unauthorized attempts.

For those applications using on-line terminals, data communications software is normally used to provide an interface between messages to and from terminals; the operating system; data files; or if present, the DBMS. In addition, this system software typically

--controls the access to and use of terminals,

--polls and receives messages from computer terminals or other computers,

--addresses and sends messages back to terminals or other computers,

--edits input and output messages,

--handles error situations,

--reroutes messages when a particular terminal or communication line is inoperative, and

--performs on-line formatting on visual display terminals.

When data throughout an agency has been combined into a single data base to eliminate redundancy and improve access, a DBMS is normally used to create and update the data base, retrieve data from it, and provide controls over its use. The DBMS provides for sharing of data by several users and permits many different application programs to access the single data base. The DBMS provides the interface between the application program's logical view of the data base and the computer system's physical storage of the data base.

The advantages of a DBMS include:

--Redundancy in magnetically stored data can be reduced.

--Inconsistent data between different files can be avoided.

--Magnetically stored data can be shared by several users.

--Standards for data storage, such as standard formats and codes, can be enforced.

--Security restrictions for different users can be applied.

--Data integrity can be maintained.

--Conflicting data requirements of different users can be resolved.

The disadvantages of a DBMS include:

--Additional main memory and direct access storage devices may be required.

--Highly skilled data processing personnel must be either hired or trained.

--The DBMS can be expensive.

Agency reliance on system software

Depending on the type of system software being used, different levels of reliance are placed on software to control data processing functions. The auditor should first identify the types and uses of system software that affect the computer-based system being reviewed and then determine the level of agency reliance on that software.

Operating systems, by their very nature, are normally heavily relied upon for general operation of computer hardware. As such, they warrant further investigation. The auditor should determine whether

--one application program can access main memory or data storage areas or files being used by another application program;

--important security and accuracy features, such as error handling for invalid data types or formats, are fully used and are not being overridden by application programs or system programmers;

--access to and use of privileged instructions, such as input/output instructions that would enable reading or writing of data from another user's file is restricted; and

--scheduling functions are self-processing or require extensive operator intervention.

The use of system utility software varies greatly among agencies. The most commonly used utilities are copy and sort programs. Regardless of type, the auditor should determine whether

--utilities are properly controlled,

--control features within the utilities are properly used, and

--utilities can be used to bypass control features of other computer-based systems or system software packages.

Program library systems, when implemented and operated properly, can add another level of control over agency application programs. Because these software packages can be vulnerable to misuse and inadvertent error, the auditor should determine whether

--adequate manual procedures exist which support and enhance the reliability of the program library system,

--control features of the program library system are fully used and cannot be overridden or bypassed, and

--the program libary system consistently and accurately performs its function of controlling application programs.

File maintenance systems are very similar to program library systems, except that they help control automated data files instead of application programs. File maintenance systems can increase the level of control if implemented and operated properly. The auditor should determine whether

--adequate manual procedures exist which support and enhance the reliability of the file maintenance system,

--control features of the file maintenance system are fully used and cannot be overridden or bypassed, and

--the file maintenance system consistently and accurately performs its function of controlling automated data files.

Security software can be used to provide an extra level of protection. To assure that reliance on this software does not create a false sense of security, the auditor should determine whether

--proper security control features are being used and

--security controls can be bypassed or overridden.

For applications using telecommunications, data communications software can be used to provide the interface between users' terminals and the computer-based system. In most cases, this system software provides additional security and reliability controls. The auditor should determine whether

--only the right people can use the right terminal for the right purposes;

--controls exist to assure that no transactions are lost, added to, or changed during transmission; and

--all control procedures of the data communications software are being used and cannot be bypassed or overridden.

For applications in the data base environment, a DBMS can be used to control and maintain the agency's data base. The auditor should determine whether

--the DBMS can be relied upon to consistently maintain accurate and reliable data,

--security over different data elements is provided restricting access to only authorized users, and

--proper backup is provided for the data base.

Controlling access to system software

In keeping with the concept of separation of duties, the responsibility for controlling and maintaining system software should be separated from that of applications. A distinction is normally made between system programmers and application programmers. Thus, access to all system software should be restricted to system programmers.

System programmers usually have complete knowledge of and access to all system software. Because of the complexity of system software, system programmers normally have higher technical skills than application programmers. Their job is to make

sure that system software continues to function accurately with a high degree of reliability. This concentration of functions, however, causes a control problem because the system programmer can control the entire operation of agency computers. As a result, activities of system programmers need to be controlled to reduce their ability to perform unauthorized or otherwise damaging acts which could adversely affect the accuracy and reliability of agency systems. A primary control is strong supervision. Even through supervisors may lack the technical proficiency needed to provide close supervision, adequate supervision is still critical. In addition, periodic security background investigations should be conducted.

In a data base environment, a data base administrator is the key person who usually has complete access to and control over the data base management system. This person is normally responsible for preserving the integrity of the data base, maintaining data definitions, and preventing unauthorized use of or change to the data base. Data base administrator activities, like the systems programmer, require careful control in the form of increased supervision and cross-checks with data base users. For example, a data base administrator may intiate DBMS changes that a system programmer implements. The data base administrator, however, should be the only person having complete access to the entire data base and the only one who changes access levels for other data base users.

Controlling changes to system software

Control procedures over changes to system software need to be established and followed. For more details refer to

discussions on program change controls in the section on system design, development, and modification controls. Controls should help maintain software integrity and prevent unauthorized or inaccurate software changes. Although most changes are initiated as maintenance changes described by the software vendor, system software changes should be controlled by

--establishing formal change procedures and forms which require supervisory authorization before implementation,

--assuring that all changes are thoroughly tested, and

--removing critical files and/or application programs from the computer area while the system programmer is making the change.

AUDIT PROCEDURES

Use the background material obtained in section II and:

1. Complete questionnaire 8 on system software controls. Pay particular attention to the types of system software interacting with the computer-based system being evaluated.
2. Complete the appropriate section of profile 2 on general controls.
3. On the basis of the level of potential risk determined on the general controls profile 2, consult the general controls matrix 2 at the end of this section for guidance on additional audit steps.

SYSTEM SOFTWARE CONTROLS

Many control operations previously performed manually have been automated in "system software," which is defined as any program or system that helps interconnect and/or control the elements of input, output, processing, data, and application programs. System software normally falls into one of the following categories: (1) operating systems, (2) system utilities, (3) program library systems, (4) file maintenance systems, (5) security software, (6) data communications systems, and (7) data base management systems.

The auditor should determine

--types and uses of system software,

--reliance on system software to perform critical control or critical processes,

--who has access to interworkings of system software, and

--how well the changes to system software are being controlled.

	YES	NO
OPERATING SYSTEMS		
1. Is an operating system used to control the inner workings of the computer hardware? (If "no," skip to question 17.)	___	___
2. Has the vendor or developer provided a complete, documented description of the operating system's design and operation?	___	___
3. Does the operating system prohibit one application program from accessing memory or data of another application program that is processing simultaneously?	___	___
4. Is the operating system "read protected"? (This prohibits an application program from accessing operating system instructions, password tables, and/or other authorization algorithms.)	___	___
5. Does the operating system prohibit operators from entering data or changing memory values at the computer console?	___	___

QUESTIONNAIRE 8

	YES	NO
6. Is the use of privileged instruction of the operating system strictly controlled?	___	___
7. Does the operating system control all input/output functions of data files?	___	___
8. Are operating system instructions, password tables, and/or other authorization algorithms protected from unauthorized access when the computer system fails?	___	___
9. Has the integrity of the operating system been tested after initial installation?	___	___
10. Does the operating system prohibit application programs from overriding or bypassing errors which are detected during processing?	___	___
11. Must all application programs or other system software be run only when the operating system is operational?	___	___
12. Is an audit trail of all operating system actions maintained either on the automatic console log or the computer system's job accounting data?	___	___
13. Is each use of the computer system's "load" button recorded?	___	___
14. Is the button physically protected?	___	___
15. Is the computer system's internal clock adequately protected from unauthorized access?	___	___
16. Does the operating system adequately and accurately schedule all jobs run on the computer system?	___	___
SYSTEM UTILITIES		
17. Are utility programs used to perform frequently repeated functions? (If "no," skip to question 25.)	___	___
18. Has the vendor or developer of the system utilities provided a complete, documented description of their design and operation?	___	___

QUESTIONNAIRE 8

	YES	NO
19. Must the operating system be operational when utility programs are used?	___	___
20. Is there a complete directory of all available utilities?	___	___
21. Is access to system utility documentation denied to computer operators?	___	___
22. Is a supervisory authorization required before installation and use of new versions of utility programs?	___	___
23. Can controls that detect processing errors in system utilities be overridden or bypassed?	___	___
24. Can system utilities be used to override or bypass controls within other system software or application programs?	___	___

PROGRAM LIBRARY SYSTEMS

25. Is a program library system used to control application programs? (If no, skip to question 35.)	___	___
26. Has the vendor or developer of the program library system provided a complete, documented description of the system's design and operation?	___	___
27. Does the program library system:		
--Restrict access to application programs?	___	___
--Control movement of programs from test to production modes?	___	___
--Control movement of programs from source code to object code?	___	___
--Control changes to application programs?	___	___
28. Are program library system functions adequately supported by proper manual procedures?	___	___
29. Are control functions performed by the program library system protected so they cannot be bypassed?	___	___

QUESTIONNAIRE 8

	YES	NO
30. Does the program library system provide an audit trail of all changes made to application programs?	___	___
31. Does the program library system prevent the existence of more than one version of a source code program?	___	___
32. Does the program library system prevent the existence of more than one version of an object code program?	___	___
33. Are obsolete programs removed regularly from the:		
--Source code library?	___	___
--Object code library?	___	___
34. Are computer operators denied access to all libraries maintained by the program library system?	___	___
FILE MAINTENANCE SYSTEMS		
35. Is a file maintenance system used to control all tape and disk data sets? (If no, skip to question 43.)	___	___
36. Has the vendor or developer of the file maintenance system provided a complete documented description of its design and operation?	___	___
37. Does the file maintenance system:		
--Restrict access to automated data files?	___	___
--Control the establishment, use and retention of automated data files?	___	___
38. Are file maintenance system functions adequately supported by proper manual procedures?	___	___
39. Are control functions performed by the file maintenance system protected so that they cannot be overridden or bypassed?	___	___

QUESTIONNAIRE 8

	YES	NO
40. Does the file maintenance system provide an audit trail of all uses and accesses of all automated data files?	___	___
41. Does the file maintenance system prohibit more than one data file from having the same volume serial number?	___	___
42. Have external labels been removed from all tape data files since the file maintenance system became operational?	___	___
SECURITY SOFTWARE		
43. Is separate security software used to provide additional control over the agency's computer resources? (If no, skip to question 53.)	___	___
44. Has the vendor or developer of the security software provided a complete documented, description of its design and operation?	___	___
45. Is the security software used to control access to:		
--Terminals?	___	___
--Remote job entry stations?	___	___
--Individual automated data files?	___	___
--Individual application programs?	___	___
--Other system software?	___	___
46. Are security software functions adequately supported by proper manual procedures?	___	___
47. Can the control functions performed by security software be overridden or bypassed?	___	___
48. Does the security software provide an audit trail of:		
--All authorized uses of computer resources under control?	___	___
--All unauthorized attempted access?	___	___

QUESTIONNAIRE 8

	YES	NO
49. Does security software control access to data separately from access to other computer resources?	___	___
50. Is security software transparent to the following:		
--All application programs?	___	___
--All other system software?	___	___
51. Is there a list of all individuals detailing what computer resources they have access to?	___	___
52. Do supervisors review it periodically?	___	___

DATA COMMUNICATIONS SYSTEMS

53. Is a data communications system used to provide the interface between terminals and the computer-based system? (If no, skip to question 78.)	___	___
54. Has the vendor or developer of the data communications system provided a complete, documented description of its design and operation?	___	___
55. Does the data communications system:		
--Control access to and use of terminals?	___	___
--Poll and receive messages from computer terminals or other computers?	___	___
--Address and send messages back to computer terminals or other computers?	___	___
--Edit and format input and output messages?	___	___
--Handle error situations?	___	___
--Reroute traffic when terminals or lines are inoperative?	___	___
--Perform on-line formatting on visual display terminals?	___	___

QUESTIONNAIRE 8

	YES	NO
56. Are data communications system functions adequately supported by proper manual procedures?	___	___
57. Are functions of the data communications system protected so that they cannot be overridden or bypassed?	___	___
58. Is a built-in hardware identification code checked by the data communications system to insure that no unauthorized terminals are being used?	___	___
59. Does the data communications system use a table of authorized terminal addresses to allow polling with the communications network?	___	___
60. Are user authorization codes or passwords required by the data communications system to:		
--Access the computer system?	___	___
--Access application programs?	___	___
--Access other system software?	___	___
--Enter transactions?	___	___
61. Are different authorization codes required to enter different transactions?	___	___
62. Does the authorization code identify the individual using the terminal?	___	___
63. Are user authorization codes controlled to restrict unauthorized use?	___	___
64. Are user authorization codes periodically changed?	___	___
65. Is a nonprinting/nondisplaying or obliteration facility used when keying in and acknowledging user authorization codes?	___	___
66. Is a terminal identification check performed by the data communications system so that various transaction types can be limited to authorized data entry stations?	___	___

QUESTIONNAIRE 8

	YES	NO
67. If a security matrix or table is used to control access to the application system, is it properly protected to prevent unauthorized access?	___	___
68. Is a message header used by the data communications system to identify:		
--Source of the message, including proper terminal and user authorization code?	___	___
--Message sequence number, including the total number of message segments?	___	___
--Transaction type code?	___	___
--Transaction authorization code?	___	___
69. Is this message header validated by the data communications system for:		
--Proper sequence number from the identified terminal?	___	___
--Proper transaction code and/or user authorization code for the terminal or user?	___	___
--Number of message segments received equal to the count indicated in the message header?	___	___
--Proper acknowledgment from the terminal at the end of a transmission?	___	___
--Balancing of debit/credit totals derived from adding all message segments and comparing with corresponding totals in the message header?	___	___
70. Does the data communications system use an end-of-transmission trailer which includes:		
--Message and segment counts?	___	___
--Value totals, including debits and credits?	___	___
--An ending symbol?	___	___

QUESTIONNAIRE 8

	YES	NO
71. Are trailer counts and totals reconciled with header counts and totals by the data communications system?	___	___
72. Does the data communications system:		
--Send acknowledgments to the terminal indicating receipt of messages?	___	___
--Periodically test line and terminal operating status with standardized test messages and responses?	___	___
73. Does the data communications system use buffering to queue messages when a device, such as a terminal, is busy?	___	___
74. Is a transaction log of sequence-numbered and/or time-of-day-noted transactions maintained by the data communications system?	___	___
75. Does the transaction log record the:		
--Orginating terminal?	___	___
--User authorization code?	___	___
--Message identification?	___	___
--Transaction type code?	___	___
--Time of day that the transaction was logged?	___	___
--Transaction data?	___	___
76. Is the transaction log used to:		
--Provide part of the audit trail?	___	___
--Account for all error messages?	___	___
--Record, with control totals, all retrievals made by a particular terminal?	___	___
77. Are all messages awaiting transmission logged by the data communications system before being put into the transmission queue, and then purged after transmission?	___	___

QUESTIONNAIRE 8

	YES	NO
DATA BASE MANAGEMENT SYSTEMS		
78. Is a data base management system used to control and maintain the agency's data base? (If "no," skip to question 93.)	___	___
79. Has the vendor or developer of the data base management system provided a complete documented description of its design and operation?	___	___
80. Does the data base management system:		
--Provide security over data base accesses?	___	___
--Control the addition, modification, and deletion of data?	___	___
--Provide the interface between individual application programs and specific data items in the data base?	___	___
81. Are data base management system functions adequately supported by proper manual procedures?	___	___
82. Are functions of the data base management system protected so that they cannot be overridden or bypassed?	___	___
83. Is the use of restricted instructions logged and checked periodically?	___	___
84. Does the data base management system use authorization codes or passwords to control access to data items?	___	___
85. Does the data base management system record unsuccessful attempts to access the data base?	___	___
86. Does the data base management system record which application programs have accessed each data item within the data base?	___	___
87. Does this log indicate whether the application program:		
--Read a data item?	___	___

	YES	NO
--Updated a data item?	___	___
--Created a new data item?	___	___
--Deleted a data item?	___	___
88. Are all errors discovered by the data base management system logged for followup?	___	___
89. Are failures in the data base management system documented for supervisory review?	___	___
90. Can the data base management system fairly and reliably identify and charge individual users of the data base for their actual usage?	___	___
91. Has a data dictionary been developed and maintained documenting the following:		
--Attributes of each data item?	___	___
--Security over each data item?	___	___
92. Does the data dictionary document the following for each data item:		
--Its name?	___	___
--Any synonyms?	___	___
--Its source?	___	___
--Frequency of change?	___	___
--Person responsible for its accuracy?	___	___
--Person responsible for updating it?	___	___
--Person responsible for deleting it?	___	___
--People eligible to read it?	___	___
--Any special authorizations required to update, read, or delete it?	___	___
--Its relationship with all other data items?	___	___
--Tests for correctness to be applied?	___	___

QUESTIONNAIRE 8

	YES	NO
--Application programs which can update, read, or delete it?	___	___
--Which output reports it appears on and the application programs that produce those reports?	___	___
--Its data format?	___	___
--Its position in the logical data structure(s)?	___	___

SYSTEM PROGRAMMERS

93.	Has the responsibility for controlling and maintaining system software (system programming) been separated from application programming?	___	___
94.	Do system programmer responsibilities include:		
	--Maintaining all system software?	___	___
	--Advising on selection of new system software?	___	___
	--Writing internal or specialized system software?	___	___
	--Modifying vendor-supplied system software?	___	___
95.	Do system programmers possess high level technical skills needed to adequately perform their functions?	___	___
96.	Are application programmers prohibited from performing system programmer functions?	___	___
97.	Are system programmers adequately supervised?	___	___
98.	Do supervisors have sufficient technical skills to adequately monitor system programmer actions?	___	___
99.	Are periodic security background investigations performed on system programmers?	___	___

QUESTIONNAIRE 8

	YES	NO
100. Are system programmers prohibited from operating the computer system?	___	___

DATA BASE ADMINISTRATOR

101. With the advent of the data base management system, has a data base administrator position been established?	___	___
102. Do data base administrator responsibilities include:		
--Designing a logical structure for the data base and deciding on a physical data storage strategy?	___	___
--Advising on selection of the data base management system?	___	___
--Developing the data dictionary?	___	___
--Selecting data search strategies?	___	___
--Directing conversion of application system data files to the data base?	___	___
--Establishing security, privacy, and accuracy controls?	___	___
--Organizing archival data storage?	___	___
--Resolving errors of data base management system failures?	___	___
--Evaluating performance of the data base management system?	___	___
--Reorganizing the data base when necessary?	___	___
103. Does the data base administrator possess high-level technical skills needed to adequately perform the function?	___	___
104. Is the administrator authorized to resolve conflicting requirements from different user departments?	___	___
105. Does the administrator insure that user requirements are met?	___	___

QUESTIONNAIRE 8

	YES	NO
106. Does the administrator insure that agency requirements are met?	___	___
107. Does the administrator advise agency officials on organizational structure changes that are necessary because of the data base?	___	___
108. Does the administrator make sure that adequate testing is performed before changes to the data base management system are implemented?	___	___
109. Are controls established to determine when it is necessary to reorganize either the physical or logical structure within the data base in order to maintain an acceptable level of performance?	___	___
110. After the data base is reorganized, does the data base administrator ascertain that control totals for the reorganized data base are reconciled with control totals existing before the reorganization?	___	___
111. Does the administrator make sure that it is technically impossible to access the data base without using the data base management system?	___	___
112. Is separation of duties clearly defined between the data base administrator and the following:		
--System programmers?	___	___
--Application programmers?	___	___
--System analysts?	___	___
--Others?	___	___
113. Is the data base administrator function properly documented?	___	___

SYSTEM SOFTWARE CHANGES

114. Have formal documented system software change procedures been established?	___	___

QUESTIONNAIRE 8

		YES	NO
115.	Are change request forms or other documentation used to originate system software modifications?	___	___
116.	If so, are all change request forms sequentially numbered and accounted for?	___	___
117.	Are system software modifications thoroughly tested to make sure that modifications function properly?	___	___
118.	Are system software modifications subjected to a system acceptance before being placed in operation?	___	___
119.	Is all relevant documentation changed to reflect system software modifications?	___	___
120.	Does the volume of regularly scheduled system software modifications indicate a problem with the software, procedures, or application?	___	___
121.	Do computer operations personnel have a list of system programmers to notify if system software requires an emergency or immediate modification?	___	___
122.	Are individuals on the above list the only system programmers allowed in the computer room?	___	___
123.	Is access to data files and application programs denied to the system programmer making a system software modification?	___	___
124.	Is the system programmer, when making an emergency modification, denied access to data files and application programs that were operating when the problem occurred?	___	___
125.	Does the system programmer making an emergency system software modification complete a statement and leave it with the computer operator as to the problem encountered and fix made?	___	___
126.	Are procedures established to ensure that emergency system software modifications are immediately subjected to a system acceptance?	___	___

QUESTIONNAIRE 8

	YES	NO
127. Are procedures established so that the accepted emergency modification will be incorporated into the next operational version of system software?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

HARDWARE CONTROLS

Most electronic computer equipment has a high degree of reliability. However, the potential for malfunction still exists because (1) electronic components may be subjected to extreme heat or humidity, power disturbances, mishandling, and normal wear and (2) mechanical operations are susceptible to failure in the timing, speed, or movement of mechanical parts. Controls need to be established in the computer hardware which detect these malfunctions. This is especially important because improved performance and faster speed of new computer equipment have recently been achieved by eliminating some hardware controls commonly found in older computer systems. Auditors should not assume hardware controls are built into computers, instead, they should confirm that hardware controls exist.

Types of hardware controls

Hardware controls are based primarily on the concept of redundancy. This usually involves adding an element to a process or to the code for a particular data item--the sole purpose of which is for error detection. Various types of hardware controls follow.

> Redundant character check. A character attached to a data item developed from the characteristics of the data item to which it is attached. Developing a redundant character usually involves a computation of bits. After an operation such as moving a data item within the computer system, the computation used to obtain the redundant character is repeated to derive a second character. The first and second redundant characters are compared, and, if they are the same, it is assumed the transfer occurred without error.
>
> Parity bit. The most common form of a redundant character. The computer system represents numbers, alphabetic characters, and other characters in binary form for internal processing. A parity bit is associated with the unit of

bits that represent a single number or character called a byte. Depending on the computer manufacturer, parity of the byte is established as either odd or even. Thus, a character or number is converted into binary form; the bit pattern representing the character is summed; and the parity bit is set to a 1 or 0, depending on whether the computer is an odd or even parity machine. (See figure below for an example of odd parity.)

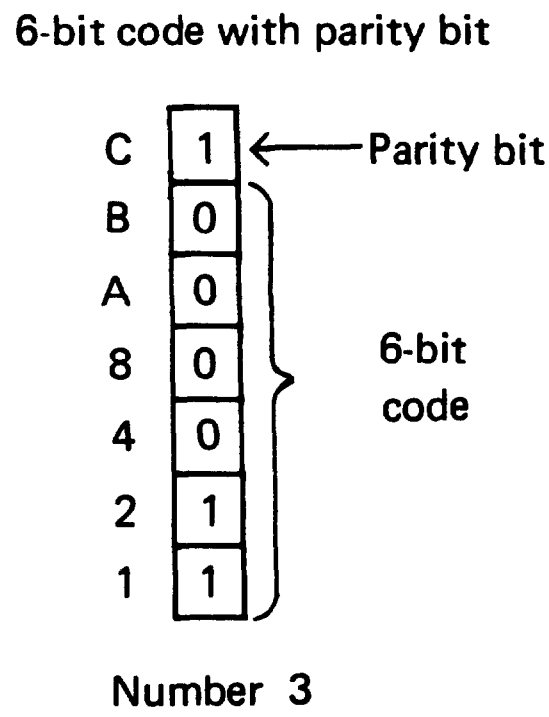


Figure - 1

Duplicate process check. Performing the same process twice and comparing the two results. Any difference between the two results signals an error. The duplicate process check can also be used as a complementary action, such as reading after writing to check what was written.

Echo check. Sending a command to a particular device to perform an operation and the receiving device returning a signal indicating type of action taken. Echo checking can also be used to compare data sent to data received by "echoing" to the sender each data item received.

Validity check. Comparing results of an operation against all valid results. Any result not fitting in with the set of valid results is considered incorrect.

Equipment check. Computer checks to see if equipment is functioning properly instead of checking results of an operation.

Hardware controls of computer components

Hardware controls normally incorporated in computer components are described below.

Central processing unit

Controls within the CPU are designed to detect several equipment problems. First, they help make sure that all data being transmitted through internal circuitry is transmitted accurately, avoiding problems with improper timing that could destroy or alter data. Second, they help avoid invalid operations. Typical controls include parity bit, redundant character checking, and validity checking of memory address numbers, operation codes, and data representations. The CPU usually has an automated mechanism to prevent it from performing certain operations at the wrong time. For example, an input/output interlock prevents the CPU from asking for new data while still processing existing data in memory.

Card reader

Because of the speed of mechanical operations and the need for precise alignment and timing, certain controls need to be incorporated within card reader machines. These include (1) dual reads, where the card is read by two different read stations and both operations are compared for consistency, (2) hole counts, where both read stations count the number of holes in a card and compare totals, and (3) validity checks for valid combinations of card punches. Proper alignment of brushes or photoelectric cells is essential. Preventive maintenance should be performed regularly on card readers to maintain accurate operation.

Card punch

Most card punches read the card after punching and compare results and hole counts, or use echo checking to verify that the correct punch dies were activated for punching the right holes. Both approaches are widely used.

Printer

There are two basic types of printers--impact and non-impact. Impact printers normally use a mechanically driven type-face which is physically pressed against the ink ribbon and paper. Nonimpact printers usually form a character or number image by use of electrical charges, ink jets, thermal devices, or laser technology. The most common controls in both types of printers are (1) echo checking the character and position of the print mechanism before printing and (2) validity checking of printer signals. For impact printers, proper printer synchronization is essential.

Magnetic tape drive

Problems with magnetic tape drives usually involve the physical movement of tape and parts of the tape drive, defects in magnetic tapes, and positioning and operation of the tape drive's read/write head. Basic controls used in magnetic tape drives include (1) parity checking of both individual characters and blocks of characters, (2) read after write check, where data is immediately read after being written and results are compared for errors, and (3) character, record, or block counts of the number of characters written or read that are compared with those normally accumulated in the tape trailer record at time of creation.

Most tape errors are caused by surface defects on the magnetic tape. Backspacing and repeating the read or write operation may dislodge dust or oxide particles on the tape and permit a successful operation. If the error persists, the computer should discontinue processing or skip the block of records or data which cannot be read and note the operation on an error listing for subsequent corrective action. In this case, the bypassed data should be controlled to make sure the problem is resolved.

Direct access storage device

Hardware controls within direct access storage devices are similar to those in magnetic tape drives. The reliability of processing is normally increased due to reduced operator handling. Major controls used include (1) parity checking of both individual and blocks of characters, (2) read after write,

where results are compared for differences, and (3) validity checks of storage address codes. Other hardware or software controls should be established to assure that the recorded data can be retrieved and it will not be inadvertently erased or written over with other data.

Data communications

As data is transferred between different devices, errors in data communications usually occur because of distances involved, speeds of transmission, and equipment malfunctions. Furthermore, the inherent complexity of a data communications environment dictates that additional hardware controls be used which are transparent to users. Major controls include (1) validity checking of hardwired terminal identification codes and data characters being transmitted, (2) specially conditioned transmission lines to reduce noise, fading, and amplitude and frequency distortion, (3) parity checking of both individual and blocks of characters, and (4) echo checking of characters entered compared with characters received. Other hardware-oriented controls that can be incorporated in the data communications system include encryption of sensitive data to reduce the effectiveness of wiretapping and automatically storing data at intermediary points when lines or other devices are inoperative. These controls are designed to make sure that only valid data is entered, transmitted, and received and that no data is lost, accessed, or tampered with along the way.

AUDIT PROCEDURES

Use the background material obtained in section II and:

1. Complete questionnaire 9 on hardware controls.
2. Complete the appropriate section of profile 2 on general controls.
3. On the basis of the level of potential risk as determined on the general controls profile 2, consult the general controls matrix 2 at the end of this section for guidance on additional audit steps needed.

HARDWARE CONTROLS

Even though most computer equipment has a high degree of reliability, malfunctions can still occur which affect the accuracy and reliability of computer data. Therefore, controls need to be established within the hardware which can detect equipment errors. This is important because improved performance and faster speed of new computers have recently been achieved by eliminating some previously used hardware controls.

The auditor should determine that proper hardware controls exist and if not, determine if alternate controls have been established.

	YES	NO
CENTRAL PROCESSING UNIT		
1. Are built-in parity bits used by the CPU to insure that all data elements transmitted through the internal circuitry are transmitted correctly?	___	___
2. Is redundant character checking used by the CPU to insure the correctness of data processing?	___	___
3. Are validity checks used by the CPU to insure that only valid operation codes are used?	___	___
4. Does the CPU perform validity checks on the numbers used to access memory to insure that only valid numbers are used?	___	___
5. Does the CPU have automatic interlock controls to prevent the equipment from performing certain operations at the wrong time?	___	___
CARD READER		
6. Are dual read controls (reading and comparing at two separate read stations) used to detect errors in reading cards?	___	___
7. Are hole count controls (counting punched holes and comparing counts at two separate read stations) used to detect errors in reading cards?	___	___
8. Are validity checks used to compare card punches read against valid combinations?	___	___

QUESTIONNAIRE 9

	YES	NO
CARD PUNCH		
9. Are read compare controls used to compare card contents with data which was to be punched?	___	___
10. Are hole count controls used to compare hole counts of the card which was punched with the hole count which was to be punched?	___	___
11. Are echo check controls used to verify that punch dies were activated to punch the required holes?	___	___
PRINTER		
12. Are echo check controls used just before printing to verify that the proper print position will be activated?	___	___
13. Are validity check controls used to verify the signals transmitted to the printer against the set of valid signals?	___	___
14. Are print synchronization controls used to check timing of the printer to determine that print hammers of impact printers are activated at the moment when appropriate characters are in the correct position?	___	___
MAGNETIC TAPE DRIVE		
15. Are parity checks (both individual and blocks of characters) made to insure that all data elements on magnetic tape are transmitted correctly?	___	___
16. Does the magnetic tape drive perform read after write comparisons to insure that data was recorded correctly?	___	___
17. Are tape trailer label totals used by the computer to verify the number of characters, records, and/or blocks read with totals maintained on the label?	___	___
18. Are read errors handled by backspacing the tape one record or block and repeating the operation?	___	___

QUESTIONNAIRE 9

	YES	NO
19. If backspacing does not successfully read the record or block after repeated attempts, does the computer discontinue processing?	___	___
20. Are programmers prevented from bypassing unprocessable records or blocks?	___	___
21. If processing is allowed to continue, have alternate manual controls been established to control bypassed records or blocks?	___	___
DIRECT ACCESS STORAGE DEVICE		
22. Are parity checks (both individual and blocks of characters) made to insure that all data elements on the direct access storage device are transmitted correctly?	___	___
23. Are read-after-write checks performed to insure that the record just written was correctly recorded?	___	___
24. Are validity check controls used to verify the address locations against the set of valid addresses?	___	___
25. Are address comparisons made to verify the address of the location at which data is to be written with the address called for by the instructions?	___	___
DATA COMMUNICATIONS		
26. Is a unique hardwired identification code, requiring no human intervention for its use, incorporated into each terminal device?	___	___
27. Is this identification code checked and validated by the computer to insure that no unauthorized terminals are being used?	___	___
28. Does the communications system avoid using the public switchboard (PBX) as a means of reducing the error rate and the chance of wiretapping data transmissions?	___	___

QUESTIONNAIRE 9

		YES	NO
29.	Are voice grade lines used to reduce data transmission errors and maintain integrity of data transmitted?	___	___
30.	Are data communications lines conditioned for improved accuracy and physical security?	___	___
31.	Are scrambling or encryption techniques used in transmitting sensitive data?	___	___
32.	Is an automatic store and forward capability used to maintain control over messages queued for an inoperative or a busy communications device?	___	___
33.	If leased lines are used, is an automatic backup capability used to ensure that when the lines fail, an automatic switchover is accomplished for the length of the outage?	___	___
34.	Is a message intercept function used to receive messages directed to inoperable or unauthorized terminals?	___	___
35.	Are parity checks used to detect errors in transmission of data?	___	___
36.	Are validity checks used to compare character signals transmitted with the set of valid characters?	___	___
37.	Is echo checking used to verify each character so that erroneous data is detected?	___	___
38.	Are forward error correcting techniques used for the detection and reporting of data communications errors using sophisticated redundancy codes?	___	___
39.	Are techniques available for detecting erroneous retransmissions of data?	___	___
40.	Are modems equipped with loop-back switches for fault isolation?	___	___

QUESTIONNAIRE 9

	YES	NO
41. Are modems which handle both voice and data communications used to enable computer operators and terminal operators to communicate in case of problems?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers, and identify alternate control procedures.

PROFILE 2

GENERAL CONTROLS PROFILE

Based on questionnaire responses and other information obtained relating to the following control characteristics, how much risk (low, medium or high) do you believe is involved in relying on the agency's general controls to assure effective ADP operation and accurate, reliable data processing? Refer to appendix II for more information on assessing risk.

Control characteristic	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level of potential risk?
ORGANIZATIONAL CONTROLS					
Separation of duties					
Personnel policies					
SYSTEM DESIGN, DEVELOPMENT, AND MODIFICATION CONTROLS					
System development life cycle					
Documentation					
Program testing and system acceptance					
Program changes					
DATA CENTER MANAGEMENT CONTROLS					
Input/output control and scheduling					

GENERAL CONTROLS PROFILE

Control characteristic	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level of potential risk?
Malfunction reporting and preventive maintenance					
User billing/ chargeout procedures					
DATA CENTER PROTECTION CONTROLS					
Security and access					
Files					
Disaster recovery					
SYSTEM SOFTWARE CONTROLS					
Operating systems					
System utilities					
Program library systems					
File maintenance systems					
Security software					
Data communications systems					
Data base management systems					

GENERAL CONTROLS PROFILE

Control characteristic	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level of potential risk?
System programmers					
Data base administrator					
System software changes					
HARDWARE CONTROLS					
Central processing unit					
Card reader					
Card punch					
Printer					
Magnetic tape drive					
Direct access storage device					
Data communications					

MATRIX 2

GENERAL CONTROLS MATRIX

If the degree of risk determined on the previous profile warrants additional audit work (medium to high risk), the following matrix should help the auditor select appropriate audit steps to complete the review.

Organizational Controls	document the data flow	observe operations	obtain user satisfaction	process test data	perform computer program analysis	perform data retrieval analysis	analyze job accounting data	report deficiencies	suggest additional audit
Separation of Duties	●	●						●	
Personnel Policies		●						●	●
System Design, Development, and Modification Controls									
System Development Life Cycle		●	●					●	
Documentation	●	●		●	●			●	
Program Testing and System Acceptance		●		●	●			●	
Program Change Controls		●		●	●		●	●	
Data Center Management Controls									
Input/Output Scheduling and Control	●	●						●	●
Malfunction Reporting and Preventive Maintenance		●	●				●	●	●
User Billing/Charges Out Procedures		●	●				●	●	●
Data Center Protection Controls									
Security and Access Controls		●					●	●	
File Controls	●	●					●	●	
Disaster Recovery Controls		●						●	

MATRIX 2

GENERAL CONTROLS MATRIX

System Software Controls	document the data flow	observe operations	obtain user satisfaction	process test data	perform computer program analysis	perform computer retrieval analysis	analyze job accounting data	report deficiencies	suggest additional audit
Operating Systems	●	●		●			●	●	●
System Utilities	●	●		●			●	●	●
Program Library Systems	●	●		●			●	●	●
File Maintenance Systems	●	●		●			●	●	●
Security Software	●	●		●			●	●	●
Data Communications Systems	●	●		●			●	●	●
Data Base Management Systems	●	●		●			●	●	●
System Programmers		●						●	●
Data Base Administrator		●						●	●
System Software Changes		●		●			●	●	●
Hardware Controls									
Central Processing Unit	●	●		●				●	
Card Reader	●	●		●				●	
Card Punch	●	●		●				●	
Printer	●	●		●				●	
Magnetic Tape Drive	●	●		●				●	
Direct Access Storage Device	●	●		●				●	
Data Communications	●	●		●				●	

SECTION VI

CONTROLS OVER THE COMPUTER APPLICATION

Certain controls should be incorporated directly into the application to help insure accurate and reliable processing. Although these controls may be unique to a particular application, they can normally be grouped according to various stages of data processing. Major processes include

--data origination,

--data input,

--data processing, and

--data output.

Application controls are primarily concerned with data being processed. Collectively, they form a network of controls in a system which help produce accurate and reliable information. Evaluations of application controls should be integrated with an evaluation of general controls because weaknesses in general controls may adversely affect any application processed.

TYPES OF APPLICATIONS

Simply stated, computer applications represent the tasks or functions the computer is to perform. In this audit guide, applications include those in financial systems (payroll, inventory, etc.); management information systems used by agencies to help administer programs (welfare systems, tax administration systems, etc.); or sophisticated command and control weapon systems or weather-tracking systems. In all these applications, data origination, input, processing, and output are involved. What may differ in each is the size of the computer, structure of

the data base, number of transactions, complexity of the computer programs, and types of hardware components.

In evaluations of application controls, the auditor should pay strict attention to the methods of processing used for data input, processing, and output.

Data input, for example, normally takes one of two forms: batch or on-line. In batch input systems, data is accumulated in a group or batch over a given period. The data is then entered into the computer, a batch at a time, to promote efficient processing and better control. Accumulation of time and attendance reports into office or department batches is a typical example. The number of documents in a batch may vary. Batches may include a specified number of documents, or they may include different numbers of documents if the size is determined by an identifier, such as office code, department, etc. Depending on the data input technology used, batching is normally done

--after input documents are manually prepared but before conversion into machine-readable format or

--after terminal entry (either through key-to-tape or key-to-disk devices or through terminals connected directly to the computer).

The key to remember is that from this point on, individual data is referenced, recalled, corrected, and controlled by the batch in which it was included. In on-line input systems, each transaction is processed one at a time through a terminal connected directly to the computer. Individual data in this input mode is referenced, recalled, corrected, and controlled by the transaction itself.

Data processing is normally done in batch or in real time. In batch processing systems, one or more batches of data are processed step by step through the computer programs constituting the application. Even if input is on-line, the data can be batch processed if the computer receives and stores the data for subsequent processing. In real time systems, data is processed as it is received with no intermediate accumulation. In purest form, real time refers to any system in which the processing of data input into the system to obtain a result occurs virtually simultaneously with the event generating the data.

Data can be output as batch or on-line. Output from the processing step can be distributed as a batch of hard copy documents or as an intermediate display or printout on a computer terminal. In many cases, both forms are used by the same application.

As can be seen, different applications can be made up of various combinations of the processing methods described above. The auditor must understand these methods and be familiar with applicable control techniques in order to evaluate a particular application.

DATA ORIGINATION CONTROLS

These are designed to insure the accuracy, completeness, and timeliness of data before it is converted into machine-readable format and entered into the computer. It is important to establish control of the data as close to the point of origination as possible, since the remainder of application processing depends upon the accuaracy of source data. The main control areas of data origination are

--source document origination,

--source document authorization,

--source document data collection and input preparation,

--source document error handling, and

--source document retention.

Source document origination controls

These controls include the procedures and methods used to insure the proper and timely recording of data on source documents. User procedures are a primary control. They should include written instructions on the preparation, flow, scheduling, and keying requirements for all source documents. These procedures should be part of the computer application users manual and should describe precisely the steps to be followed in preparing a source document.

Another important control involves the design of source documents. Special purpose forms should be used to make sure the preparer initially records a transaction correctly and in a uniform format. For example, rather than just providing a blank ("_____") for a social security number, a well-designed form would include the following instead: "_ _ _ - _ _ - _ _ _ _." Other source document design characteristics that promote accurate and reliable data include

--preprinted sequential numbers that insure source document accountability;

--transaction identification codes that aid in identifying and tracing data through the computer application; and

--cross-reference fields, normally filled with the preprinted sequential document number, that facilitate cross-referencing of computerized data and source documents.

Blank source documents and other input forms should be stored in a secure location to prevent unauthorized access. Further, access to source documents and other input forms should be carefully controlled during intermediate storage and movement during the processing cycle. The concept of dual custody, where a member of the data processing department and a member of the user department must jointly authorize the release, movement, and acceptance of source documents, has been proven to be an effective control over source document handling.

Source document authorization controls

Controls need to be established to make sure that all source documents are properly authorized before being entered into the application. The process of authorization should include more than just initiating or reviewing a source document. It should also include actual approval of the source document for processing. The most common type of authorization control is a signature. It helps provide audit evidence to identify the person who originated, reviewed, and approved the source document. Such a process also helps maintain an adequate separation of duties within the user department. In some systems, approval authorization may be limited to specific types of transactions or specific types of actions (control bypassing, system overrides, or manual adjustments). In any event, the authorization and approval process should be documented in the users manual.

Source document data collection and input preparation

To help make sure that all source documents are collected and properly prepared for input into the application, a control group should be established in the user department. This group should make sure that all source documents are accounted for, are complete and accurate, are properly authorized, and are processed in a timely manner. Some common techniques used by this group follow.

--Turnaround transmittal documents which help control the movement of source documents between users and the data processing department. They should be prepared as close to the source as possible and used throughout the processing cycle. Copies should not only accompany the source documents in their movement, but should also be returned to the originating office.

--Batching techniques which help control source documents by combining transactions into batches by transaction type, originating office, or number of transactions. Each batch should be assigned a unique identifiable batch serial number to provide accountability.

--Record counts of the number of source documents to be processed individually or within a batch, the number of batches, and the total number of batched transactions.

--Predetermined control totals which are established by summing certain fields of input transactions. These totals can be financial (total amount of sales or payroll amounts) or hash totals of fields which are not usually summed (inventory stock numbers or social security numbers).

--Control logs which are kept by the control group to record the flow of transactions or batches during the processing cycle.

In a well-controlled application, turnaround transmittal documents and control logs are used to record batch numbers, record counts, and predetermined control totals for reconciliation during subsequent processing.

Source document error handling

Controls need to be established to insure that all transactions found to be in error at this stage of processing are corrected and reentered in a timely manner. Written error-handling procedures should be developed and followed to provide user personnel with comprehensive instructions for source document error detection, correction, and reentry. These procedures, which should be incorporated in the users manual, should include

--types of errors that can be made,

--corrective steps to be followed, and

--methods to be used for reentering source documents which have been corrected.

The control group should be responsible for detecting errors and assuring that all source documents with errors are corrected and reentered in a timely manner. Error logs are normally used to account for erroneous source documents and to monitor outstanding erroneous transactions to make sure that they are corrected and reentered quickly. The group should immediately notify source document originators of errors detected by initial scanning of the source documents.

Source document retention

Controls over the retention of source documents should be established so that lost or destroyed data can be recreated. Each type of source document should have a specific retention period based on either legal requirements or management policy. If possible, the retention date should be preprinted on the source document to help in the destruction process. This

retention date can be used as a cross-index locator when source documents are stored in a sequence other than expiration date.

Source documents should be stored in a logical sequence to facilitate easy retrieval. The storage area should preclude unauthorized access. A copy of the source document should be kept in the storage area anytime the original source document is removed. On reaching their expiration dates, source documents should be purged from the retention area and destroyed in accordance with security classifications.

AUDIT PROCEDURES

Use background material obtained in section III and:

1. Complete the following questionnaire 10 on data origination controls.
2. Complete the appropriate section of profile 3 on application controls.
3. On the basis of the level of potential risk determined on the application controls profile 3, consult the application controls matrix 3 at the end of this section for guidance on additional audit steps.

DATA ORIGINATION CONTROLS

Data origination controls are used to insure the accuracy, completeness, and timeliness of data before it is converted into machine-readable format and entered into the computer application. Controls over the data must be established as close to the point of origination as possible. Additionally, controls must be maintained throughout this manual process to make sure that the data reaches the computer application without loss, unauthorized addition or modification, or other error. The main areas of control are

--source document origination,

--source document authorization,

--source document data collection and input preparation,

--source document error handling, and

--source document retention.

The auditor should determine the adequacy of controls over the manual preparation, collection, and processing of source documents to make sure that no data is added, lost, or altered before it is entered into the computer system.

	YES	NO
SOURCE DOCUMENT ORIGINATION		
1. Do documented procedures exist that explain the methods for proper source document origination, authorization, data collection, input preparation, error handling, and retention?	___	___
2. Are duties separated to make sure that no one individual performs more than one of the following operations:		
--Originating data?	___	___
--Inputting data?	___	___
--Processing data?	___	___
--Distributing output?	___	___

QUESTIONNAIRE 10

	YES	NO
3. Are source documents designed to minimize errors and omissions such that:		
--Special purpose forms are used to guide the initial recording of data in a uniform format?	___	___
--Preprinted sequential numbers are used to establish controls?	___	___
--Each type of transaction has a unique identifier?	___	___
--Each transaction has a cross-reference number which can be used to trace information to and from the source document?	___	___
4. Is access to source documents and blank input forms restricted to authorized personnel only?	___	___
5. Are source documents and blank input forms stored in a secure location?	___	___
6. Is authorization from two or more accountable individuals required before the release of source documents and blank input forms from storage?	___	___
SOURCE DOCUMENT AUTHORIZATION		
7. Are authorizing signatures used for all types of transactions?	___	___
8. Is evidence of approval required for specific types of critical transactions (control bypassing, system overrides, manual adjustments)?	___	___
9. Are duties separated within the user department to make sure that one individual does not prepare more than one type of transaction (establishing new master records plus changing or updating master records)?	___	___
10. Are duties separated within the user department to make sure that no one individual performs more than one of the following phases of data preparation:		
--Originating the source document?	___	___

	YES	NO
--Authorizing the source document?	___	___
--Controlling the source document?	___	___

SOURCE DOCUMENT DATA COLLECTION AND INPUT PREPARATION

11.	Does the user department have a control group responsible for collecting and completing source documents?	___	___
12.	Does this control group verify the following for source documents:		
	--They are accounted for?	___	___
	--They are complete and accurate?	___	___
	--They have been appropriately authorized?	___	___
	--They are transmitted in a timely manner?	___	___
13.	Does this control group independently control data submitted for transmittal to the data processing department for conversion or entry by using:		
	--Turnaround transmittal documents?	___	___
	--Batching techniques?	___	___
	--Record counts?	___	___
	--Predetermined control totals?	___	___
	--Logging techniques?	___	___
	--Other? (Describe.)	___	___
14.	When the user department is responsible for its own data entry, is there a separate group which performs this input function?	___	___
15.	Are source documents, transmitted for conversion, transported in accordance with their security classifications?	___	___

SOURCE DOCUMENT ERROR HANDLING

16.	Do documented procedures exist that explain the methods for source document error detection, correction, and reentry?	___	___

QUESTIONNAIRE 10

	YES	NO
17. Do they include:		
--Types of error conditions that can occur?	___	___
--Correction procedures to be followed?	___	___
--Methods to be used for the reentry of source documents which have been corrected?	___	___
18. Does the control group identify errors to facilitate the correction of erroneous information?	___	___
19. Does the control group follow the same verification and control procedures described in questions 12 and 13 when receiving corrected source documents?	___	___
20. Are error logs used to insure timely followup and correction of unresolved errors?	___	___
21. Are source document originators immediately notified by the control group of all errors?	___	___
SOURCE DOCUMENT RETENTION		
22. Are source documents retained so that data lost or destroyed during subsequent processing can be recreated?	___	___
23. Does each type of source document have a specific retention period which is preprinted on the document?	___	___
24. Are source documents stored in a logical manner to facilitate retrieval?	___	___
25. Is a copy of the source document kept in the originating department whenever the document leaves the department?	___	___
26. Is access to records kept in the originating department restricted to authorized personnel only?	___	___

QUESTIONNAIRE 10

	YES	NO
27. Are source documents, on reaching their expiration dates, removed from storage and destroyed in accordance with security classifications?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

DATA INPUT CONTROLS

These are designed to insure the accuracy, completeness and timeliness of data during its conversion into machine-readable format and entry into the application. As described earlier, data can be input in either a batch or on-line mode. Each will be discussed separately below. The main control areas of data input are

--data conversion and entry,

--data validation and editing, and

--data input error handling.

The critical interface between user departments and the data processing department is also of particular importance in this section.

Batch--data conversion and entry

Controls over the conversion and entry of data into an application should be documented in written procedures. These should describe the step-by-step process of converting data from source documents into machine-readable format, including the keying requirements, type of data entry device to be used, and processing schedules to be followed. They should also describe control steps to be followed at various points in this phase of processing. A key point for the auditor to consider when reviewing these procedures and observing actual data conversion and entry is the degree to which duties have been separated within the process. It is desirable that different individuals originate, input, process data, and distribute output.

Within each user department, a control group should be established to make sure that all source documents are converted into machine-readable format and entered into the application. Depending on the design of the application and the functions performed by the data processing department, the user department control group may or may not control both functions of data conversion and data entry. Nevertheless, this control group should account for and process all source documents originating in its department that are being sent to the data processing department or other service organization for processing. Techniques to accomplish this control function include:

--Turnaround transmittal documents which provide an audit trail of source documents processed, number processed, and control totals developed. These documents normally consist of two copies. One is maintained by the user department; the other accompanies the source documents and is annotated by the receiving department with control information and returned to the user department and reconciled with the first copy.

--Batching techniques which accumulate source documents into batches for further processing and help provide control against loss or manipulation. Batches may be accompanied by the turnaround transmittal document.

--Record counts of the number of source documents being forwarded. These counts are usually made by batch or by total documents processed. The counts are normally recorded on the turnaround transmittal document and should be verified by the receiving organization when batches of source documents are received.

--Predetermined control totals, or hash totals, of selected fields on source documents. Like record counts, these totals should be recorded on the turnaround transmittal document and verified by the receiving organization when batches of source documents are received.

--Control logs which are used by the control group to record the movement of source documents between operations so that no source documents are added, lost, or manipulated. Control logs usually contain batch number, record counts, and predetermined control totals corresponding to the batches of source documents being processed.

These techniques should be used for both data conversion and data entry. Both operations should be performed as close to the preparation of the source documents as possible.

Batch--data validation and editing

While data is being converted into machine-readable format and entered into the application, certain validation and editing techniques should be used to insure that data is being processed properly. Some of these techniques are concerned with detecting keying errors. These include:

--Key verification, where a second person (preferably a different individual) reads the same source document and keys data into a verifier. This verifier machine compares the depressed key with the hole in the punched card or its electronic equivalent. Differences are noted for subsequent correction. In a punched card system, a small perforation on the right margin of the card indicates the card has passed the verification process. When errors are found, a notch is automatically punched above the column which is in error.

--Preprogrammed keying formats where formats for data conversion and entry are incorporated directly into the data entry device to insure that data is recorded in the proper fields, formats, and characters.

Other techniques are used to insure valid data content, include:

--Editing, where individual fields and combinations of fields are checked for valid content, format, size, sign, etc.

--Date validation, where for example, transaction dates are automatically compared with a table of valid dates stored in the system.

These data validation and editing techniques should be performed as early as possible and should be performed for all input data fields even though an error may have been detected in an earlier field of the same transaction.

If these techniques are permitted to be overridden or bypassed, this override/bypass capability should be restricted to supervisory personnel only and limited to as few situations as possible. All uses of the capability should be automatically recorded by the system and subsequently analyzed on a regular basis for appropriateness and correctness by higher supervisory personnel.

During data entry, the application should automatically develop batch record counts and control totals similar to those developed by the user department control group. These record counts and control totals should be reconciled either automatically by the application or by a control group within the data processing department. Any discrepancies should be corrected before further processing.

Batch--data input error handling

Transactions with errors detected during the data input phase of processing need to be controlled to make sure they are corrected and reentered in a timely manner. Written procedures should explain the process of identifying, correcting, and reprocessing data which has been rejected. For each error condition in a transaction, an error message should be displayed on an error listing which describes the type of error and the corrective action to be taken.

All transactions which have been determined to be in error by data validation and editing routines should be rejected from further processing and automatically controlled by entering them into an error suspense file. Transactions entered into the suspense file should be annotated with

--codes indicating the type of data error,

--date and time the transaction was processed and the error was made, and

--the identity of the user who originated the transaction.

Control counts and totals should be developed automatically during data input suspense file processing and used in reconciling input transactions processed.

The data processing control group should independently control all rejected input transactions. To do this, it should use turnaround transmittal documents, batching techniques, record counts, predetermined control totals, and control logs. Errors not caused by data conversion or data entry mistakes should be returned to user departments through their control group. All other errors should be corrected by the data processing department as soon as possible.

The automated suspense file provides an effective means of controlling and following up on transactions which have been rejected by the application. Periodically, the file should be analyzed to determine the extent to which transaction errors are being made and the status of uncorrected transactions. Management should use this information to help improve application processing by holding subordinates accountable for either unacceptable error rates or unacceptable delays in correcting data.

The procedures for processing corrected transactions should be the same as those for processing original transactions, with the addition of supervisory review and approval before reentry. If the correction is valid, the system should purge the related erroneous transactions from the suspense file. If the correction is invalid, the system should add it to the file together with the original rejected transaction. Suspense file record counts and control totals should be adjusted accordingly after a correction has been processed.

Throughout the batch input process, ultimate responsibility for completeness and accuracy remains with the user.

On-line--data conversion and entry

Many data conversion and data entry controls used in batch systems apply to on-line systems as well. These include

--detailed written procedures,

--separation of duties, and

--user department control groups.

Additional controls, however, are needed over operations of computer terminals being used for data conversion and entry into the on-line environment.

Data entry terminals should be located in physically secure rooms. When terminals are not in use, these rooms should be locked or the terminals themselves should be secured by lockable covers. In addition, supervisors should sign on or initialize each terminal before operators begin work and sign off each terminal at the end of the day. Operators should be required to enter passwords before they are allowed to enter data. These

passwords should be changed periodically. They should not be displayed or printed when entered or acknowledged by the computer system. The computer should check passwords against a data access matrix to make sure they are valid and to restrict access or use of terminals for only those transactions a particular operator has been authorized to enter. In some situations, computer terminals may be used for either data entry or query functions. If so, the terminal designated as a query-only terminal may be in a less secure area; however, passwords should still be used to control terminal use.

Unauthorized attempts to use terminals should be automatically recorded and reported by the computer system. These reports should include the

--physical location of the terminal,

--date and time of the unauthorized attempt,

--number of attempts, and

--operator identification and supervisor's code.

The system should be designed to automatically lock up a terminal after a predetermined number of unauthorized attempts to use it. The locked-up terminal should be permitted to return to operation only by special intervention of supervisors through a master command terminal.

Top managers have a responsibility to periodically review unauthorized usage reports, terminal authority levels, and operator access levels to help make sure that terminal use is properly controlled. Further, they should make sure that passwords are periodically changed, especially when a purported or real security violation occurs or when an operator changes job

functions, separates, or no longer needs the same level of access. Top managers may delegate this responsibility to a full-time security officer.

Additional data conversion and entry controls should be built into the computer terminal hardware. Typical features include

--built-in terminal identification codes, which are used to automatically validate authorization levels;

--terminal logs, which record all transactions processed;

--time and date stamps, which are posted to all messages being transmitted; and

--record counts, which are automatically accumulated.

At the beginning of each message, a header message segment should be automatically generated by the terminal. This message header should contain a message number, terminal and operator identification, date and time of entry, and a transaction code describing the type of transaction being processed. The message header helps provide an audit trail of all transactions entered and messages sent from a given terminal. Terminals should also annotate messages indicating the end of a message and the end of a transmission.

Other types of hardware controls that are built into terminals include parity checking of each character entered and of each message transmitted. Messages should also be checked for valid characters.

On-line--data validation and editing

In on-line systems, different techniques are used to make sure that data being entered is accurate and reliable. These validation and editing techniques include:

--Preformatting, where predesigned formats are used to guide the terminal operator so that data is entered in the proper fields with correct lengths, codes, signs, and characters.

--Interactive display, which permits the terminal operator to interact directly with the system during data entry. This technique helps the operator correct inputs because error conditions are highlighted at the time of entry.

--Computer-aided instruction which uses both preformatting and interactive display to guide the operator through data entry by prompting the operator on actions to be taken.

Many systems use intelligent terminals which have the capability of being programmed to perform most of the data validation and editing routines. These terminals help to minimize transmission traffic because they edit the data before transmission to the host computer system. These terminals can also be used to accumulate control totals as well.

Similar to batch input, on-line data validation and editing should be performed as early as possible in the transaction processing cycle to insure that errors are detected and corrected quickly. Transactions and data fields should be edited for valid characters, sign, format, content, etc. This editing should be on all data fields even though an error may have been detected in an earlier field of the same transaction. Transaction dates should also be validated. Overriding or bypassing data validation and editing errors should be restricted to supervisors. Each use of the override/bypass feature should be automatically logged by the application and analyzed for appropriateness and corrrectness. Record counts and control totals should also be generated through the on-line input process and be used to validate the completeness of data entry.

On-line--data input error handling

Controls over on-line input error handling are essentially the same as those for a batch system. The major difference is that error messages are transmitted directly to the terminal rather than included in a batch error listing. Key points to evaluate include the following:

--Are easily understood error messages created for all transactions and data fields so that terminal operators can take corrective action?

--Does an automated suspense file control all rejected transactions to insure timely and accurate correction?

--Are procedures for processing corrected transactions, the same as those for processing original transactions, with the addition of supervisory review and approval before reentry?

AUDIT PROCEDURES

Use background material obtained in section III and:

1. Complete the following questionnaire 11 on data input controls.
2. Complete the appropriate section of profile 3 on application controls.
3. On the basis of the level of potential risk determined on the application controls profile 3, consult the application controls matrix 3 at the end of this section for guidance on additional audit steps.

DATA INPUT CONTROLS

Data input controls insure the accuracy, completeness, and timeliness of data during its conversion into machine-readable format and entry into the application. Data input can be accomplished in two different ways: batch and on-line. The main areas of control include

--data conversion and entry,

--data validation and editing, and

--data input error handling.

Also of particular importance is the critical interface between the user department and the data processing department.

The auditor should determine the adequacy of both manual and automated controls over data input to make sure that data is input accurately with optimum use of computerized validation and editing, and that error handling procedures facilitate the timely and accurate resubmission of all corrected data.

	YES	NO
BATCH--DATA CONVERSION AND ENTRY		
1. Do documented procedures exist that explain the methods for data conversion and entry?	___	___
2. Are duties separated to make sure that no one individual performs more than one of the following operations:		
--Originating data?	___	___
--Inputting data?	___	___
--Processing data?	___	___
--Distributing output?	___	___
3. Does the data processing department have a control group responsible for data conversion and entry of all source documents received from user departments?	___	___
4. Does the data processing control group return all turnaround transmittal documents to the user department to make sure that no documents were added or lost?	___	___

QUESTIONNAIRE 11

	YES	NO
5. Does the data processing control group account for all batches of source documents received from the user department to make sure that no batches were added or lost?	___	___
6. Does the data processing control group independently develop record counts which are balanced with those of the control group in the user department, and are all discrepancies reconciled?	___	___
7. Does the data processing control group independently develop predetermined control totals which are balanced with those of the control group in the user department, and are all discrepancies reconciled?	___	___
8. Does the data processing control group keep a log or record showing the receipt of user department source documents, and their actual disposition, and are there provisions to make sure that all documents are accounted for?	___	___
9. Does the data processing control group independently control data submitted for conversion by using:		
--Turnaround transmittal documents?	___	___
--Batching techniques?	___	___
--Record counts?	___	___
--Predetermined control totals?	___	___
--Logging techniques?	___	___
--Other? (Describe)	___	___
10. Are conversion operations established as close to the origination of the source documents as possible?	___	___
11. Do conversion operations record document information directly onto machine-readable media (keypunch cards, key to tape, key to disk, or key to terminal) as opposed to intermediate media, such as coding documents?	___	___

QUESTIONNAIRE 11

	YES	NO
12. Does the data processing department have a schedule by application that shows when data requiring conversion will be received and needs to be completed?	___	___
13. Are turnaround transmittal documents returned to the data processing control group accounted for to make sure that no documents were added or lost during conversion?	___	___
14. Are all batches of documents returned to the data processing control group accounted for to make sure that no batches were added or lost during conversion?	___	___
15. Are all record counts, developed during conversion, balanced with those of the data processing control group, and are all discrepancies reconciled?	___	___
16. Are all predetermined control totals developed during conversion, balanced with those of the data processing control group and are all discrepancies reconciled?	___	___
17. Are all converted documents returned to the data processing control group logged in and accounted for?	___	___
18. Does the data processing control group independently control data submitted for data entry by using:		
--Turnaround transmittal documents?	___	___
--Batching techniques?	___	___
--Record counts?	___	___
--Predetermined control totals?	___	___
--Logging techniques?	___	___
--Other? (Describe)	___	___
19. Are data entry operations established as close to the origination of the source data as possible?	___	___
20. Does the data processing department have a schedule by application that shows		

QUESTIONNAIRE 11

	YES	NO
when data requiring entry will be received and needs to be completed?	___	___
21. Must all documents entered into the application be signed or marked in some way to indicate that they were entered into the system thereby preventing accidental duplication or reuse of the data?	___	___
22. Are turnaround transmittal documents returned to the data processing control group accounted for to make sure that no documents were added or lost during data entry?	___	___
23. Are all batches of documents returned to the data processing control group accounted for to make sure that no batches were added or lost during data entry?	___	___
24. Are all record counts, developed during data entry, balanced with those of the data processing control group, and are all discrepancies reconciled?	___	___
25. Are all predetermined control totals, developed during data entry, balanced with those of the data processing control group, and are all discrepancies reconciled?	___	___
26. Are all input documents returned to the data processing control group logged in and accounted for?	___	___
27. Are all input documents retained in a manner which enables tracing them to related originating documents and output records?	___	___

BATCH--DATA VALIDATION AND EDITING

28. Is key verification used to check the accuracy of all keying operations?	___	___
29. Are keying and verifying functions performed on a document done by different individuals?	___	___
30. Are preprogrammed keying formats used to insure that data is recorded in the proper field, format, etc.?	___	___
31. Is data validation and editing performed as early as possible in the data flow to		

QUESTIONNAIRE 11

	YES	NO
insure that the application rejects any incorrect transaction before its entry into the system?	___	___
32. Is data validation and editing performed for all input data fields even though an error may be detected in an earlier field of the same transaction?	___	___
33. Are the following checked for validity on all input transactions:		
--Individual and supervisor authorization or approval codes?	___	___
--Check digits on all identification keys?	___	___
--Check digits at the end of a string of numeric data that is not subjected to balancing?	___	___
--Codes?	___	___
--Characters?	___	___
--Fields?	___	___
--Combinations of fields?	___	___
--Transactions?	___	___
--Calculations?	___	___
--Missing data?	___	___
--Extraneous data?	___	___
--Amounts?	___	___
--Units?	___	___
--Composition?	___	___
--Logic decisions?	___	___
--Limit or reasonableness checks?	___	___
--Signs?	___	___
--Record matches?	___	___

QUESTIONNAIRE 11

	YES	NO
--Record mismatches?	___	___
--Sequence?	___	___
--Balancing of quantitative data?	___	___
--Crossfooting of quantitative data?	___	___
34. Are special routines used which automatically validate and edit input transaction dates against a table of cutoff dates?	___	___
35. Are all persons prevented from overriding or bypassing data validation and editing problems?	___	___
36. If not, are the following true:		
--This override capability is restricted to supervisors in only a limited number of acceptable circumstances?	___	___
--Every system override is automatically logged by the application so that these actions can be analyzed for appropriateness and correctness?	___	___
37. Are batch control totals submitted by the data processing control group used by the computer-based system to validate the completeness of batches received as input into the application?	___	___
38. Are record counts submitted by the data processing control group used by the computer-based system to validate the completeness of data input into the application?	___	___
39. Are predetemined control totals submitted by the data processing control group used by the computer-based system to validate the completeness of data input into the application?	___	___
BATCH--DATA INPUT ERROR HANDLING		
40. Do documented procedures exist that explain the process of identifying, correcting, and reprocessing data rejected by the application?	___	___

QUESTIONNAIRE 11

		YES	NO
41.	Are error messages displayed with clearly understood corrective actions for each type of error?	___	___
42.	Are error messages produced for each transaction which contains data that does not meet edit requirements?	___	___
43.	Are error messages produced for each data field which does not meet edit requirements?	___	___
44.	Is all data that does not meet edit requirements rejected from further processing by the application?	___	___
45.	Is all data rejected by the application automatically written on an automated suspense file?	___	___
46.	Does the automated suspense file also include:		
	--Codes indicating error type?	___	___
	--Date and time the transaction was entered?	___	___
	--Identity of the user who originated the transaction?	___	___
47.	Are record counts automatically created by suspense file processing to control these rejected transactions?	___	___
48.	Are predetermined control totals automatically created by suspense file processing to control these rejected transactions?	___	___
49.	Are rejected transactions caused by data conversion or entry errors corrected by the data processing department control group?	___	___
50.	Does the data processing department control group independently control data rejected by the application by using:		
	--Turnaround transmittal documents?	___	___
	--Batching techniques?	___	___
	--Record counts?	___	___
	--Predetermined control totals?	___	___
	--Logging techniques?	___	___

QUESTIONNAIRE 11

	YES	NO
--Other? (Describe)	___	___
51. Are rejected transactions not caused by data conversion or entry errors corrected by the user originating the transaction?	___	___
52. Does the user department's control group independently control data rejected by the application by using:		
--Turnaround transmittal documents?	___	___
--Batching techniques?	___	___
--Record counts?	___	___
--Predetermined control totals?	___	___
--Logging techniques?	___	___
--Other? (Describe)	___	___
53. Is the automated suspense file used to control followup, correction, and reentry of transactions rejected by the application?	___	___
54. Is the automated suspense file used to produce, for management review, analysis of:		
--Level of transaction errors?	___	___
--Status of uncorrected transactions?	___	___
55. Are these analyses used by management to make sure that corrective action is taken when error levels become too high?	___	___
56. Are these analyses used by management to make sure that corrective action is taken when uncorrected transactions remain on the suspense file too long?	___	___
57. Are progressively higher levels of management reported to as these conditions worsen?	___	___
58. Are debit- and credit-type entries (as opposed to delete- or erase-type commands) used to correct rejected transactions on the automated suspense file?	___	___
59. Is the application designed so that it cannot accept a delete- or an erase-type command?	___	___

QUESTIONNAIRE 11

	YES	NO
60. Do valid correction transactions purge the automated suspense file of corresponding rejected transactions?	___	___
61. Are invalid correction transactions added to the automated suspense file, along with the corresponding rejected transactions?	___	___
62. Are record counts appropriately adjusted by correction transactions?	___	___
63. Are predetermined control totals appropriately adjusted by correction transactions?	___	___
64. Are all corrections reviewed and approved by supervisors before reentry?	___	___
65. Are procedures for processing corrected transactions the same as those for processing original transactions with the addition of supervisory review and approval before reentry?	___	___
66. Does ultimate responsibility for the completeness and accuracy of all application processing remain with the user?	___	___
ON-LINE--DATA CONVERSION AND ENTRY		
67. Do documented procedures exist that explain the methods for data conversion and entry?	___	___
68. Are duties separated to make sure that no one individual performs more than one of the following operations:		
--Originating data?	___	___
--Inputting data?	___	___
--Processing data?	___	___
--Distributing data?	___	___
69. Is a separate group within the user department responsible for performing data entry operations?	___	___
70. Does the user department's control group independently control data to be entered into the application by using:		

QUESTIONNAIRE 11

	YES	NO
--Turnaround transmittal documents?	___	___
--Batching techniques?	___	___
--Record counts?	___	___
--Predetermined control totals?	___	___
--Logging techniques?	___	___
--Other? (Describe)	___	___
71. If the user department's control group does not control data entry, is at least simultaneous entry and recording of source data performed at the point of origination?	___	___
72. Must all documents entered into the computer application be signed or marked in some way to indicate that they were in fact entered into the system to protect against accidental duplication or reuse of the data?	___	___
73. Are data entry terminal devices locked in a physically secure room, allowing only query terminal devices to be located outside the secure room?	___	___
74. Must supervisors sign on each terminal device to initialize terminals before any operators can sign on to begin work?	___	___
75. Is the work that may be entered on a terminal restricted by the authority level assigned to each terminal device (data entry vs. query)?	___	___
76. Is password control in existence to prevent unauthorized use of the terminal devices?	___	___
77. Are nonprinting, nondisplaying, or obliteration facilities used when keying and acknowledging passwords and authorization codes?	___	___
78. Is an immediate report produced of unauthorized attempts to access the system via terminal devices?	___	___
79. Does this report include:		
--Location of the terminal device?	___	___

QUESTIONNAIRE 11

		YES	NO
	--Date and time of the violation?	___	___
	--Numer of attempts?	___	___
	--Identification of the operator at the time of the violation?	___	___
80.	Is a terminal lockup used to prevent unauthorized access to the terminal device after a certain predetermined number of incorrect attempts to access the system?	___	___
81.	Does the system automatically shut down the terminal in question and allow intervention only by specially assigned data processing department supervisors?	___	___
82.	Is a data access matrix used to restrict use or access levels by checking user identifications (passwords)?	___	___
83.	Is each individual user of the on-line system limited to certain types of application transactions?	___	___
84.	Are master commands that control the operation of the application restricted to a limited number of supervisory data processing personnel and master command terminals only?	___	___
85.	Does top management periodically review the propriety of the terminal authority levels?	___	___
86.	Is top management required to review the propriety of terminal authority levels in the event of a purported or real security violation?	___	___
87.	Are individual's passwords changed periodically?	___	___
88.	Are individual's passwords changed in the event of a purported or real security violation?	___	___
89.	Are passwords deleted once an individual changes his job function, separates, no longer needs the same level of access, or no longer needs access at all?	___	___

QUESTIONNAIRE 11

		YES	NO
90.	Is a usage log, or the data access matrix, showing purpose of user accesses reviewed by top management to identify unauthorized usage?	___	___
91.	Has the security officer initiated an aggressive review program to determine that controls are fully operational?	___	___
92.	Do terminal hardware features include the following:		
	--Built-in terminal identifications which automatically validate proper terminal authorization?	___	___
	--Terminal logs which record all transactions processed?	___	___
	--Messages which are automatically date and time stamped for logging purposes?	___	___
	--Record counts which are automatically accumulated for logging purposes?	___	___
93.	Does each message contain an identifying message header that includes:		
	--Message number?	___	___
	--Terminal and user identification?	___	___
	--Date and time?	___	___
	--Transaction code?	___	___
94.	Does each message contain indicators for:		
	--End of message?	___	___
	--End of transmission?	___	___
95.	Is parity checking used to check each character?	___	___
96.	Is parity checking used to check each message or message block?	___	___
97.	Is the message content checked for valid characters?	___	___

QUESTIONNAIRE 11

		YES	NO
ON-LINE--DATA VALIDATION AND EDITING			
98.	Are preprogrammed keying formats used to make sure that data is recorded in the proper field, format, etc.?	___	___
99.	Is interactive display used to allow the terminal operator to interact with the system during data entry?	___	___
100.	Are computer-aided instructions, such as prompting, used with on-line dialog to reduce the number of operator errors?	___	___
101.	Are intelligent terminals used to allow front-end validation, editing, and control?	___	___
102.	Is data validation and editing performed as early as possible in the data flow to insure that the application rejects any incorrect transaction before its entry into the system?	___	___
103.	Is data validation and editing performed for all input data fields even though an error may be detected in an earlier field of the same transaction?	___	___
104.	Are the following checked for validity on all input transactions:		
	--Individual and supervisor authorization or approval codes?	___	___
	--Check digits on all identification keys?	___	___
	--Check digits at the end of a string of numeric data that is not subjected to balancing?	___	___
	--Codes?	___	___
	--Characters?	___	___
	--Fields?	___	___
	--Combinations of fields?	___	___
	--Transactions?	___	___
	--Calculations?	___	___

	YES	NO
--Missing data?	___	___
--Extraneous data?	___	___
--Amounts?	___	___
--Units?	___	___
--Composition?	___	___
--Logic decisions?	___	___
--Limit or reasonableness checks?	___	___
--Signs?	___	___
--Record matches?	___	___
--Record mismatches?	___	___
--Sequence?	___	___
--Balancing of quantitative data?	___	___
--Crossfooting of quantitative data?	___	___
105. Are special routines used which automatically validate and edit input transaction dates against a table of cutoff dates?	___	___
106. Are all persons prevented from overriding or bypassing data validation and editing errors?	___	___
107. If not, are the following true:-		
--This overrride capability is restricted to supervisors in a limited number of acceptable circumstances?	___	___
--All system overrides are automatically logged by the application so that these actions can be analyzed for appropriateness and correctness?	___	___
108. Are batch control totals generated by the terminal, concentrator, or application used by the user department control group to validate the completeness of batches received as input data?	___	___

QUESTIONNAIRE 11

	YES	NO
109. Are record counts generated by the terminal, concentrator, or application used by the user department control group to validate the completeness of data input?	___	___
110. Are predetermined control totals generated by the terminal, concentrator, or application used by the user department's control group to validate the completeness of data input?	___	___

ON-LINE--DATA INPUT ERROR HANDLING

111. Do documented procedures exist that explain the process of identifying, correcting, and reprocessing data rejected by the application?	___	___
112. Are errors displayed or printed immediately upon detection for immediate terminal operator correction?	___	___
113. Are error messages displayed with clearly understood cross-referenced corrective actions for each type of error?	___	___
114. Are error messages produced for each transaction which contains data that does not meet edit requirements?	___	___
115. Are error messages produced for each input data field which does not meet edit requirements?	___	___
116. Is all data rejected by the application automatically written on an automated suspense file?	___	___
117. Does the automated suspense file include:		
--Codes indicating error type?	___	___
--Date and time the transaction was entered?	___	___
--Identity of the user who originated the transaction?	___	___
118. Are record counts automatically created by suspense file processing to control these rejected transactions?	___	___
119. Are predetermined control totals automatically created by suspense file processing to control these rejected transactions?	___	___

QUESTIONNAIRE 11

		YES	NO
120.	Are rejected transactions caused by data entry errors corrected by the terminal operator?	___	___
121.	Are rejected transactions not caused by data entry errors corrected by the user originating the transaction?	___	___
122.	Does the user department control group independently control data rejected by the application by using:		
	--Turnaround transmittal documents?	___	___
	--Batching techniques?	___	___
	--Record counts?	___	___
	--Predetemined control totals?	___	___
	--Logging techniques?	___	___
	--Other? (Describe)	___	___
123.	Is the automated suspense file used to control followup, correction, and reentry of transactions rejected by the application?	___	___
124.	Is the automated suspense file used to produce, for management review, analysis of the following:		
	--Level of transaction errors?	___	___
	--Status of uncorrected transactions?	___	___
125.	Are these analyses used by management to make sure that corrective action is taken when error levels become too high?	___	___
126.	Are these analyses used by management to make sure that corrective action is taken when uncorrected transactions remain on the suspense file too long?	___	___
127.	Are progressively higher levels of management reported to as these conditions worsen?	___	___
128.	Are debit- and credit-type entries (as opposed to delete- or erase-type commands) used to correct rejected transactions on the suspense file?	___	___

QUESTIONNAIRE 11

		YES	NO
129.	Is the application designed so that it cannot accept a delete- or an erase-type command?	___	___
130.	Do valid correction transactions purge the automated suspense file of corresponding rejected transactions?	___	___
131.	Are invalid correction transactions added to the automated suspense file along with the corresponding rejected transactions?	___	___
132.	Are record counts appropriately adjusted by correction transactions?	___	___
133.	Are predetermined control totals appropriately adjusted by correction transactions?	___	___
134.	Are all corrections reviewed and approved by supervisors before reentry?	___	___
135.	Are the procedures for processing corrected transactions the same as those for processing original transactions, with the addition of supervisory review and approval before reentry?	___	___
136.	Does ultimate responsibility for the completeness and accuracy of all application processing remain with the user?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

DATA PROCESSING CONTROLS

These help insure the accuracy, completeness, and timeliness of data while it is being processed by the computer. Data is normally processed in either a batch or real-time mode. Each is discussed separately below. The main control areas over computer processing involve

--data processing integrity,

--data processing validation and editing, and

--data processing error handling.

Of particular importance in this section are those controls over files and other systems which interface with the application being reviewed.

Batch--data processing integrity

Controls over computer processing of data should be documented in written procedures. This documentation is normally found in computer operator instructions, program run books, and history logs.

Operator instructions describe the step-by-step procedures that the operator should take when operating the system. These instructions should include

--system startup procedures,

--backup assignments,

--emergency procedures,

--system shutdown procedures,

--error message debugging instructions, and

--system and job status reporting instructions.

These procedures should be designed to limit the operator intervention in the processing cycle and prohibit unauthorized operator access to the computer-based system.

Computer program run books include additional instructions for operators on processing applications. A separate book is normally prepared for each application and includes

--definitions of input sources, input data, and data formats;

--descriptions of setup procedures;

--descriptions of all halt conditions;

--descriptions of restart procedures and checkpoints;

--descriptions of data storage requirements;

--copies of printer carriage control tapes;

--descriptions of expected output data and formats;

--descriptions of output and file dispositions upon completion;

--copies of normal console run sheets;

--types of console message instructions; and

--copies of system flowcharts.

Computer program run books should exclude detailed program logic charts, block diagrams, decision tables, and copies of actual program listings so that computer operators cannot alter or otherwise modify the computer program for unauthorized purposes. Many operator procedures are now being performed by the computer's operating system and are therefore not documented in a run book. If so, the operator should still have written procedures covering the work steps to be followed.

A history log records all events performed by the computer during processing of an application and the actions taken or interventions made by operators. In particular, the log should record

--hardware failure messages,

--software failure messages,

--processing halts,

--abnormal terminations of jobs,

--operator interventions,

--error messages, and

--other unusual occurrences during processing.

For better control, this log should be printed on both a line printer and the computer console. Supervisors within the data processing department should be routinely required to review and sign off on the log noting problems that have occurred and corrective action taken.

The department should establish a control group which is responsible for controlling all data processing operations. This group should be responsible for scheduling all work to be done by the data processing department; controlling access to and use of job control cards; developing, maintaining, and reconciling record counts and control totals; and maintaining control logs that document the movement of work through the various data processing operations. The group should also make sure that proper versions of input, work, and output files are used and that any restarts are performed properly. The control group should maintain a close relationship with control groups within user departments.

Several techniques can be used to insure accurate and reliable data processing. They include

--samples of master files which are drawn periodically so that the data can be independently verified to source documents,

--transaction codes or other unique identifiers which direct the transaction to the proper application system or program,

--run-to-run totals or computer generated control totals which are automatically reconciled between various steps of processing, and

--file label checking which (1) compares internal file header labels with anticipated file identifiers to insure that the proper file is being used and (2) compares the record count of total records processed with the external trailer label to insure that all records on a file were processed.

These techniques should not be overridden or bypassed. They should be used on all transactions and files being processed, especially those of interfacing systems.

Batch--data processing validation and editing

Even though data should be validated and edited during conversion to machine-readable format, certain other validation and editing routines should be performed while the computer is processing the data. This data validation and editing should be performed as early as possible in the data flow, especially before updating master files, to insure that erroneous data is rejected from further processing. Validation and editing should be done on all data fields even though an error may have been detected in an earlier field of the same transaction.

Many validation and editing routines used in the data input phase are also used in the data processing phase, particularly on transactions or files which come from other

applications. These include checking the data for proper length, sign, content, etc. Other validation and editing routines usually performed during data processing include relationship editing between related fields within a transaction and between the transaction and master file records to be updated. Validation and editing routines can be "table driven," where transaction data is compared with tables of valid dates, codes, etc. These tables may require too much storage to make the comparisons during the input phase; therefore, they are made during the data processing phase.

Overriding or bypassing data processing validation and editing routines should be restricted to supervisors and permitted only in a limited number of situations. All uses of the override/bypass should be automatically recorded by the system and analyzed for appropriateness and correctness by higher supervisory personnel.

The application should automatically develop batch record counts and control totals similar to those developed by the user department control group during data input. These record counts and control totals should be reconciled either automatically by the application or by the data processing control group. Any discrepancies should be corrected before further processing.

A transaction history file should also be maintained which records the transaction, the date and time of processing, and a before-and-after picture of the master file being updated. This transaction history file not only provides the audit trail for data processed, but can be used as a backup file for reconstruction of missing or improperly altered master records.

Batch--data processing error handling

Transactions with errors detected during the data processing phase need to be controlled to insure that they are corrected and reentered in a timely manner. Written procedures should explain the process of identifying, correcting, and reprocessing data which has been rejected. For each error condition within a transaction, an error message should be displayed on an error listing which clearly describes the type of error and the corrective action to be taken.

All transactions which have been determined to be in error by the data validation and editing routines should be rejected from further processing and automatically controlled by entering them into an error suspense file. Transactions entered into this file should be annotated with

--codes indicating the type of data error,

--date and time the transaction was processed and the error was made, and

--identity of the user who originated the transaction.

Record counts and control totals should be developed automatically during suspense file processing and used in reconciling all transactions processed.

The data processing control group should independently control all rejected transactions. To do this, it should use turnaround transmittal documents, batching techniques, record counts, predetermined control totals, and control logs. Errors not caused by improper processing procedures should be returned to user departments through their control group. All other

errors should be corrected by the data processing department as soon as possible.

The automated suspense file provides an effective means of controlling and following up on rejected transactions. Periodically, this file should be analyzed to determine the extent to which transaction errors are being made and the status of uncorrected transactions. Management should use this information to help improve application processing by holding subordinates accountable for either unacceptable error rates or unacceptable delays in correcting data.

The procedures for correcting transactions should be the same as for processing original transactions, with the addition of supervisory review and approval before reprocessing. If the correction is valid, the system should purge the related erroneous transaction from the suspense file. If the correction is invalid, the system should add it to the suspense file together with the original rejected transaction. Suspense file record counts and control totals should be adjusted accordingly after a correction has been processed. Ultimate responsibility for completeness and accuracy of all application processing remains with users.

Real-time--data processing integrity

Many of the controls used to maintain data processing integrity in batch-oriented systems apply to real-time systems as well. These controls include

--detailed written operating procedures,

--proper separation of duties, and

--a data processing department control group.

Furthermore, many of the different control techniques used to insure the accuracy and reliability of data also apply. They include

--evaluating periodic samples of master records,

--using transaction codes,

--checking file header and trailer labels,

--maintaining a history log of all events which have occurred on the computer, and

--controlling transactions and files that come from other systems.

However, additional controls should be used to control real-time processing. The data processing control group, in addition to scheduling and controlling work done on the computer, should be required to monitor all terminal activity and investigate and correct any problems. It should also monitor, investigate, and correct computer operator interventions and deviations from processing procedures. The group should balance and reconcile record counts and control totals developed during real-time processing.

Additional control techniques which should be used in real-time processing include

--automatic logging of all transactions processed so that a complete audit trail is available,

--date and time stamping on all transactions to provide accountability, and

--concurrent update protection so that two transactions cannot try to update a single master record simultaneously.

These controls should help insure data processing integrity in a real-time environment.

Real-time--data processing validation and editing

As with batch processing, real-time processing validation and editing should be done as early as possible in the processing cycle to insure that errors are detected and corrected quickly. Transactions and data fields should be edited for valid characters, sign, format, content, etc. This editing should be performed on all data fields even though an error may have been detected in an earlier field of the same transaction. Relationship edits should be performed between related fields within the transaction and between the transaction and master file records to be updated. Transaction dates should also be validated.

Overriding or bypassing data validation and editing errors should be restricted to supervisors and permitted only in a limited number of situations. Every use of the override/bypass feature should be automatically recorded by the application and analyzed for appropriateness and correctness. Record counts and control totals should also be generated and used to validate the completeness of real-time processing.

Real-time--data processing error handling

The controls over real-time data processing error handling are essentially the same as those for batch systems. The major difference is that error messages are usually transmitted directly to terminals rather than included in a batch error listing. Key points to evaluate include the following:

--Are easily understood error messages created for all transactions and data fields so that terminal operators can take corrective action?

--Does an automated suspense file control all rejected transactions to insure timely and accurate corrections?

--Are procedures for processing corrected transactions the same as those for processing original transactions with the addition of supervisory review and approval before reentry?

AUDIT PROCEDURES

Use the background material obtained in section III and:

1. Complete the following questionnaire 12 on data processing controls.
2. Complete the appropriate section of profile 3 on application controls.
3. On the basis of the level of potential risk determined on the application controls profile 3, consult the application controls matrix 3 at the end of this section for guidance on additional audit steps.

DATA PROCESSING CONTROLS

Data processing controls are used to insure the accuracy, completeness, and timeliness of data during processing by the computer. These controls apply to application programs and computer operations related to the application. Data processing is usually accomplished in batch or real time. The main areas of control include

--data processing integrity,

--data processing validation and editing, and

--data processing error handling.

Of particular importance are those controls over files and other systems which interface with the application being reviewed.

The auditor should determine the adequacy of controls over data processing, to make sure that data is accurately processed through the application and that no data is added, lost, or altered during processing.

BATCH--DATA PROCESSING INTEGRITY

	YES	NO
1. Do documented procedures exist to explain the methods for proper data processing of each application program?	___	___
2. Are duties separated to make sure that no one individual performs more than one of the following operations:		
--Originating data?	___	___
--Inputting data?	___	___
--Processing data?	___	___
--Distributing output?	___	___
3. Do operator instructions include:		
--System startup procedures?	___	___
--Backup assignments?	___	___
--Emergency procedures?	___	___
--System shutdown procedures?	___	___

QUESTIONNAIRE 12

	YES	NO
--Error message debugging instructions?	___	___
--System and job status reporting instructions?	___	___
4. Do computer program run books include:		
--Definitions of input sources, input data, and data formats?	___	___
--Descriptions of setup procedures?	___	___
--Descriptions of all halt conditions?	___	___
--Descriptions of restart procedures and checkpoints?	___	___
--Descriptions of data storage requirements?	___	___
--Printer carriage control tapes?	___	___
--Descriptions of expected output data and formats?	___	___
--Descriptions of output and file dispositions upon completion?	___	___
--Copies of normal console run sheets?	___	___
--Types of console message instructions?	___	___
--System flowcharts?	___	___
5. Do computer program run books exclude:		
--Program logic charts or block diagrams?	___	___
--Copies of program listings?	___	___
6. Are application programs prevented from accepting data from computer consoles?	___	___
7. Does the system have a history log which is printed on both a line printer and the console?	___	___
8. Does this log include:		
--Hardware failure messages?	___	___
--Software failure messages?	___	___
--Processing halts?	___	___

QUESTIONNAIRE 12

	YES	NO
--Abnormal terminations of jobs?	___	___
--Operator interventions?	___	___
--Error messages?	___	___
--Unusual occurrences?	___	___
9. Is the log routinely reviewed by supervisors to determine the causes of problems and the correctness of actions taken?	___	___
10. Does the data processing department have a schedule, by application, that shows when each application program is to be run and needs to be completed?	___	___
11. Does the data processing department have a control group responsible for controlling all data processing operations?	___	___
12. Does the data processing control group limit access to and use of job control cards so that unauthorized programs will not be executed?	___	___
13. Does the data processing control group independently control data processing by:		
--Assuring that application schedules are met?	___	___
--Balancing batch counts of data submitted for processing?	___	___
--Balancing record counts of data submitted for processing?	___	___
--Balancing predetermined control totals of data submitted for processing?	___	___
--Maintaining accurate logs of input/work/ output files used in computer processing?	___	___
--Assuring that input/work/output files used in computer processing are correct?	___	___
--Assuring that restarts are performed properly?	___	___
--Other? (Describe)	___	___
14. Is there some means of verifying master file contents (samples being periodically drawn from data files and reviewed for accuracy)?	___	___

QUESTIONNAIRE 12

	YES	NO
15. Does each input transaction have a unique identifier (transaction code) which directs the transaction to the proper application program for processing?	___	___
16. Do programs positively identify input data as to type (transaction code)?	___	___
17. Are standardized default options built into computer program logic?	___	___
18. Are computer-generated control totals (run-to-run totals) automatically reconciled between jobs to check for completeness of processing?	___	___
19. Where computerized data is entered into the computer application are there controls to verify that proper data is used?	___	___
20. Where computer files are entered into the computer application, are there controls to verify that the proper version (cycle) of the file is used?	___	___
21. Do all programs include routines for checking internal file header labels before processing?	___	___
22. Are controls in place to prevent operators from circumventing file checking routines?	___	___
23. Are internal trailer labels containing control totals (record counts, predetermined control totals, etc.) generated for all computer files and tested by the application programs to determine that all records have been processed?	___	___
24. Are file completion checks performed to make sure that application files have been completely processed, including both transaction and master files?	___	___
25. Do data processing controls make sure that:		
--Output counts from the system equal input counts to the system?	___	___
--Program interfaces require that the sending program output counts equal the receiving program input counts?	___	___

QUESTIONNAIRE 12

	YES	NO
--System interfaces require that:		
--The sending system's output counts equal the receiving system's input counts?	___	___
--Shared files meet the control requirements of both the sending and receiving systems?	___	___

BATCH--DATA PROCESSING VALIDATION AND EDITING

26.	Is data validation and editing performed as early as possible in the data flow to insure that the application rejects any incorrect transaction before master file updating?	___	___
27.	Is data validation and editing performed for all data fields even through an error may be detected in an earlier field of the transaction?	___	___
28.	Are the following checked for validity on all input transactions:		
	--Individual and supervisor authorization or approval codes?	___	___
	--Check digits on all identification keys?	___	___
	--Check digits at the end of a string of numeric data that is not subjected to balancing?	___	___
	--Codes?	___	___
	--Characters?	___	___
	--Fields?	___	___
	--Combinations of fields?	___	___
	--Transactions?	___	___
	--Calculations?	___	___
	--Missing data?	___	___
	--Extraneous data?	___	___
	--Amounts?	___	___

QUESTIONNAIRE 12

	YES	NO
--Units?	___	___
--Composition?	___	___
--Logic decisions?	___	___
--Limit or reasonableness checks?	___	___
--Signs?	___	___
--Record matches?	___	___
--Record mismatches?	___	___
--Sequence?	___	___
--Balancing of quantitative data?	___	___
--Crossfooting of quantitative data?	___	___
29. Is relationship editing performed between input transactions and master files to check for appropriateness and correctness before updating?	___	___
30. Are special routines used which automatically validate and edit input transaction dates against a table of cutoff dates?	___	___
31. Is full data validation and editing (questions 28-30) performed on all files interfacing with the application?	___	___
32. Do the programs that include a table of values have an associated control mechanism to assure accuracy of the table values?	___	___
33. Are all persons prevented from overriding or bypassing data validation and editing problems?	___	___
34. If not are the following true:		
--This override capability is restricted to supervisory personnel in a limited number of acceptable circumstances?	___	___
--All system overrides are automatically logged by the application so that these actions can be analyzed for appropriateness and correctness?	___	___

QUESTIONNAIRE 12

	YES	NO
35. Are record counts generated by the application used by the data processing control group to validate the completeness of data processed by the system?	___	___
36. Are predetermined control totals generated by the application used by the data processing control group to validate the completeness of data processed by the system?	___	___
37. Does a direct update to files cause:		
--A record to be created and added to a backup file, containing a before and after picture of the record being altered?	___	___
--The transaction to be recorded on the transaction history file together with date and time of entry and the originator's identification?	___	___

BATCH--DATA PROCESSING ERROR HANDLING

38. Do documented procedures exist that explain the process of identifying, correcting, and reprocessing data rejected by the application?	___	___
39. Are error messages displayed with clearly understood corrective actions for each type of error?	___	___
40. Are error messages produced for each transaction which contain data that does not meet edit requirements?	___	___
41. Are error messages produced for each data field which does not meet edit requirements?	___	___
42. Is all data that does not meet edit requirements rejected from further processing by the application?	___	___
43. Is all data rejected by the application automatically written on an automated suspense file?	___	___
44. Does the automated suspense file include:		
--Codes indicating error type?	___	___

QUESTIONNAIRE 12

	YES	NO
--Date and time transaction was entered?	___	___
--Identity of the user who originated the transaction?	___	___
45. Are record counts automatically created by suspense file processing to control these rejected transactions?	___	___
46. Are predetermined control totals automatically created by suspense file processing to control these rejected transactions?	___	___
47. Are rejected transactions transmitted to the users originating them so that corrective action can be taken?	___	___
48. Does the user department control group independently control data rejected by the application system using:		
--Turnaround transmittal documents?	___	___
--Batching techniques?	___	___
--Record counts?	___	___
--Predetermined control totals?	___	___
--Logging techniques?	___	___
--Other? (Describe)	___	___
49. Is the automated suspense file used to control followup, correction, and reentry of transactions rejected by the application?	___	___
50. Is the automated suspense file used to produce, for management review, analysis of:		
--Level of transaction errors?	___	___
--Status of uncorrected transactions?	___	___
51. Are these analyses used by management to make sure that corrective action is taken when error levels become too high?	___	___
52. Are these analyses used by management to make sure that corrective action is taken when uncorrected transactions remain on the suspense file too long?	___	___

	YES	NO
53. Are progressively higher levels of management reported to as these conditions worsen?	___	___
54. Are debit- and credit-type entries (as opposed to delete- or erase-type commands) used to correct rejected transactions on the automated suspense file?	___	___
55. Is the application designed so that it cannot accept a delete- or erase-type command?	___	___
56. Do valid correction transactions purge the automated suspense file of corresponding rejected transactions?	___	___
57. Are invalid correction transactions added to the automated suspense file, along with the corresponding rejected transaction?	___	___
58. Are record counts appropriately adjusted by correction transations?	___	___
59. Are predetermined control totals appropriately adjusted by correction transactions?	___	___
60. Are all corrections subject to supervisory review and approval before reentry?	___	___
61. Are the procedures for processing corrected transactions the same as for processing original transactions, with the addition of supervisory review and approval before reentry?	___	___
62. Does the ultimate responsibility for completeness and accuracy of all application processing remain with the user?	___	___
REAL-TIME--DATA PROCESSING INTEGRITY		
63. Do documented procedures exist that explain the methods for proper data processing of every application program?	___	___
64. Are duties separated to make sure that no one individual performs more than one of the following operations:		
--Originating data?	___	___
--Inputting data?	___	___

QUESTIONNAIRE 12

		YES	NO
	--Processing data?	___	___
	--Distributing output?	___	___
65.	Is there a logging type facility (audit trail) in the application to assist in reconstructing data files?	___	___
66.	Can messages and data be traced back to the user or point of origin?	___	___
67.	Does the application protect against concurrent file updates (i.e., does initial access of a record lock out that record so that additional access attempts cannot be made until the initial processing has been completed)?	___	___
68.	Are transactions date and time stamped for logging purposes?	___	___
69.	Are application programs prevented from accepting data from computer consoles?	___	___
70.	Does the system have a history log which is printed on both a line printer and the console?	___	___
71.	Does this log include:		
	--Hardware failure messages?	___	___
	--Software failure messages?	___	___
	--Processing halts?	___	___
	--Abnormal terminations of jobs?	___	___
	--Operator interventions?	___	___
	--Error messages?	___	___
	--Unusual occurrences?	___	___
	--Terminal failure messages?	___	___
	--Terminal startup?	___	___
	--Terminal shutdown?	___	___
	--All input communications messages?	___	___
	--All output communications messages?	___	___

		YES	NO
72.	Is the log routinely reviewed by supervisors to determine the causes of problems and the correctness of actions taken?	___	___
73.	Does the data processing department have a control group which is responsible for controlling all data processing operations?	___	___
74.	Does the data processing control group independently control data processing by:		
	--Monitoring terminal activity?	___	___
	--Investigating and correcting any terminal problems that cannot be resolved at the sources?	___	___
	--Investigating and correcting any terminal imbalances or failures?	___	___
	--Investigating any operator intervention actions?	___	___
	--Investigating any operator deviations from the rules?	___	___
	--Assuring that restarts are performed properly?	___	___
	--Balancing batch counts of data processed (as developed during off-line operations)?	___	___
	--Balancing record counts of data processed (as developed during off-line operations)?	___	___
	--Balancing predetermined control totals of data processed (as developed during off-line operations)?	___	___
	--Other? (Describe)	___	___
75.	Are periodic balances taken at fairly short intervals to make sure that data is being processed accurately?	___	___
76.	Is off-line file balancing performed on:		
	--Batch counts?	___	___
	--Record counts?	___	___
	--Predetermined control totals?	___	___

		YES	NO
	--Other? (Describe)	___	___
77.	Is there some means of verifying master file contents (e.g., samples being periodically drawn from data files and reviewed for accuracy)?	___	___
78.	Does each input transaction have a unique identifier (transaction code) which directs the transaction to the proper application program for processing?	___	___
79.	Do programs positively identify input data as to type (transaction code)?	___	___
80.	Are standardized default options built into computer program logic?	___	___
81.	Are computer-generated control totals (run-to-run totals) automatically reconciled between jobs to check for completeness of processing?	___	___
82.	Where computerized data is entered into the computer application, are there controls to verify that proper data is used?	___	___
83.	Where computerized files are entered into the computer application, are there controls to verify that the proper version (cycle) of the file is used?	___	___
84.	Do all programs include routines for checking internal file header labels before processing?	___	___
85.	Are controls in place to prevent operators from circumventing file checking routines?	___	___
86.	Are internal trailer labels containing control totals (record counts, predetermined control totals, etc.) generated for all computer files and tested by the application programs to determine that all records have been processed?	___	___
87.	Are file completion checks performed to make sure that application files have been completely processed, including both transaction and master files?	___	___

	YES	NO
88. Do data processing controls make sure that:		
--Output counts from the system equal input counts to the system?	___	___
--Program interfaces require that the sending program output counts equal the receiving program input counts?	___	___
--System interfaces require that:		
--The sending system's output counts equal the receiving system's input counts?	___	___
--Shared files meet the control requirements of both the sending and receiving systems?	___	___

REAL-TIME--DATA PROCESSING VALIDATION AND EDITING

89. Is data validation and editing performed as early as possible in the data flow to insure that the application rejects any incorrect transaction before master file updating?	___	___
90. Is data validation and editing performed for all data fields even through an error may be detected in an earlier field of the transaction?	___	___
91. Are the following checked for validity on all input transactions:		
--Individual and supervisor authorization or approval codes?	___	___
--Check digits on all identification keys?	___	___
--Check digits at the end of a string of numeric data that is not subjected to balancing?	___	___
--Codes?	___	___
--Characters?	___	___
--Fields?	___	___
--Combinations of fields?	___	___
--Transactions?	___	___

QUESTIONNAIRE 12

	YES	NO
--Calculations?	___	___
--Missing data?	___	___
--Extraneous data?	___	___
--Amounts?	___	___
--Units?	___	___
--Composition?	___	___
--Logic decisions?	___	___
--Limit or reasonableness checks?	___	___
--Signs?	___	___
--Record matches?	___	___
--Record mismatches?	___	___
--Sequence?	___	___
--Balancing of quantitative data?	___	___
--Crossfooting of quantitative data?	___	___
92. Is relationship editing performed between input transactions and master files to check for appropriateness and correctness prior to updating?	___	___
93. Are special routines used which automatically validate and edit input transaction dates against a table of cutoff dates?	___	___
94. Is full data validation and editing (questions 91-93) performed on all files interfacing with the application?	___	___
95. Do the programs that include a table of values have a control mechanism to assure accuracy of the table values?	___	___
96. Are all persons prevented from overriding or bypassing data validation and editing problems?	___	___
97. If not, are the following true:		

	YES	NO
--This override capability is restricted to supervisory personnel in a limited number of acceptable circumstances?	___	___
--All system overrides are automatically logged by the application so that these actions can be analyzed for appropriateness and correctness?	___	___
98. Are record counts generated by the application used by the data processing control group to validate the completeness of data processed by the system?	___	___
99. Are predetermined control totals generated by the application used by the data processing control group to validate the completeness of data processed by the system?	___	___
100. Does a direct update to files cause:		
--A record to be created and added to a backup file, containing a before and after picture of the record being altered?	___	___
--The transaction to be recorded on the transaction history file together with the date and time of entry and the originator's identification?	___	___

REAL-TIME--DATA PROCESSING ERROR HANDLING

101. Do documented procedures exist that explain the process of identifying, correcting, and reprocessing data rejected by the application?	___	___
102. Are error messages displayed with clearly understood corrective actions for each type of error?	___	___
103. Are error messages produced for each transaction which contains data that does not meet edit requirements?	___	___
104. Are error messages produced for each data field which does not meet edit requirements?	___	___
105. Is all data that does not meet edit requirements rejected from further processing by the application?	___	___

QUESTIONNAIRE 12

		YES	NO
106.	Is all data rejected by the application automatically written on an automated suspense file?	___	___
107.	Does the automated suspense file include:		
	--Codes indicating error type?	___	___
	--Date and time transaction was entered?	___	___
	--Identity of the user who originated the transaction?	___	___
108.	Are record counts automatically created by suspense file processing to control these rejected transactions?	___	___
109.	Are predetermined control totals automatically created by suspense file processing to control these rejected transactions?	___	___
110.	Are rejected transactions transmitted to the users originating them so that corrective action can be taken?	___	___
111.	Does the user department control group independently control data rejected by the application system using:		
	--Turnaround transmittal documents?	___	___
	--Batching techniques?	___	___
	--Record counts?	___	___
	--Predetermined control totals?	___	___
	--Logging techniques?	___	___
	--Other? (Describe)	___	___
112.	Is the automated suspense file used to control followup, correction, and reentry of transactions rejected by the application?	___	___
113.	Is the automated suspense file used to produce, for management review, analysis of:		
	--Level of transaction errors?	___	___
	--Status of uncorrected transactions?	___	___

		YES	NO
114.	Are these analyses used by management to make sure that corrective action is taken when error levels become too high?	___	___
115.	Are these analyses used by management to make sure that corrective action is taken when uncorrected transactions remain on the suspense file too long?	___	___
116.	Are progressively higher levels of management reported to as these conditions worsen?	___	___
117.	Are debit- and credit-type entries (as opposed to delete- or erase-type commands) used to correct rejected transactions on the automated suspense file?	___	___
118.	Is the application designed so that it cannot accept a delete- or an erase-type command?	___	___
119.	Do valid correction transactions purge the automated suspense file of corresponding rejected transactions?	___	___
120.	Are invalid correction transactions added to the automated suspense file along with the corresponding rejected transactions?	___	___
121.	Are record counts appropriately adjusted by correction transactions?	___	___
122.	Are predetermined control totals appropriately adjusted by correction transactions?	___	___
123.	Are all corrections subject to supervisory review and approval before reentry?	___	___
124.	Are the procedures for processing corrected transactions the same as for processing original transactions, with the addition of supervisory review and approval before reentry?	___	___
125.	Does the ultimate responsibility for completeness and accuracy of all application processing remain with the user?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

DATA OUTPUT CONTROLS

These are used to insure the integrity of computer outputs and to make sure that timely and proper distribution of outputs is made. Special care should be exercised over accountable documents, such as blank checks, bond stocks, etc. Also, retention cycles need to be established to permit reconstruction of data and files in the event of error. Data is usually output in either a batch or on-line mode. Each is discussed separately below. The main control areas are

--output balancing and reconciliation,

--output distribution,

--output error handling, and

--handling and retention of output records and accountable documents.

Similar to data input controls, the interface between the data processing department control group and the various user department control groups is critically important.

Batch--output balancing and reconciliation

The data processing department control group should be responsible for reviewing system outputs for completeness and accuracy before releasing them to user department control groups. Procedures should be documented in writing. The data processing department control group should

--monitor the flow of data through the application;

--review output products for general acceptability and completeness;

--reconcile record counts and control totals before releasing of any output reports; and

--maintain a log of all outputs produced, summarizing the number of reports generated, pages and lines printed, copies made, and recipients of each report.

These logs provide a record of report distribution and an audit trail. They should be periodically reviewed by supervisors for completeness, accuracy, and appropriateness.

For control purposes, each output product should contain

--name or title of the product;

--processing program name or number;

--date and time prepared;

--processing period covered;

--user name and location;

--control counts and totals developed during processing;

--end-of-job/file/report indication; and

--the security classification, if any.

User department control groups should also be required to balance and reconcile computer outputs. To do this, the control groups should

--review all outputs received from the data processing department for accuracy and completeness,

--reconcile all record counts and control totals with those manually prepared during data origination, and

--keep up to date with all changes made to the application and with transactions entered and processed by interfacing systems.

The user departments have ultimate responsibility for the accuracy of all outputs.

Batch--output distribution

Written procedures should describe the methods for proper handling and distribution of outputs. These procedures should require

--cover sheets for each report produced by the application which clearly identify the recipients' names and locations and

--logs of all reports leaving the data processing department which identify the job names and times and dates of production, product names and times and dates of distribution, recipients' names, quantities distributed, and security status.

Periodically, users should be independently canvassed to determine if the correct number of copies are being received on time. A priority system should be established so that critical outputs can be produced on time.

The data processing control group should be responsible for distributing all outputs. It should have a schedule, by application, showing when processing will be complete and when outputs need to be distributed. The group should maintain logs and checklists showing the exact disposition of every output. It should also use turnaround transmittal documents to verify that all outputs have been received by the authorized recipients.

Batch--output error handling

Controls need to be established over errors detected at this stage of processing. The data processing control group should immediately notify user department control groups of problems found in outputs. Procedures should be documented in writing. The data processing control group should

--maintain an output error control log which records the type of error detected, corrective action to be taken, date and time of resubmission, and date and time of distribution to users;

--maintain a history file of all output product errors; and

--keep users informed of output product errors and the progress of corrective actions.

The output error control log and error history file should be reviewed periodically by supervisors to insure proper and timely identification and correction of erroneous outputs and to identify causes of and trends in errors so that areas requiring additional guidance and training can be pinpointed.

User department control groups should also maintain output error control logs of all errors reported to them by the data processing department control group. These logs should be used to identify causes of and trends in errors to make sure they are corrected in a timely manner. Users should be promptly notified of errors in their output products.

Batch--handling and retention of output records and accountable documents

Retention periods for source documents and output reports should be established for reasonable periods so that records can be reconstructed when improper or erroneous processing occurs. These periods should consider the facilities' backup arrangements and audit requirements. Access to documents and reports should be restricted to authorized individuals. Appropriate facilities should be used to dispose of records at the end of their retention periods.

Users should be queried periodically to determine whether

--output products are needed in the same format as currently being received,

--they are needed as often as currently being received, and

--the same numbers of copies as are currently being received are needed.

Special controls need to be established over accountable documents, such as check stock, bond stock, and identification

card stock. Dual custody, or the practice of having two different people concurrently responsible, should be used while accountable documents are in storage, are in transit, are awaiting use by the application, are awaiting distribution, or are in transit back to storage. Access to accountable documents should be restricted to authorized personnel. Special care should be exercised to make sure that accountable documents scheduled for destruction are completely destroyed.

On-line--output balancing and reconciliation

Many controls over batch output balancing and reconciliation apply to on-line systems as well. These include the need for documented procedures, a data processing control group, and proper identification of output products. However, additional controls need to be established over outputs transmitted or printed via terminals. The data processing department control group, in addition to reviewing output products and scheduling and monitoring production, should balance and reconcile all record counts and control totals before transmitting outputs to a remote terminal.

A transaction log should be kept by the application to provide an audit trail of transactions processed. A similar log should also be kept at each output transmission device to provide an audit trail of outputs received. These two logs should be compared regularly to make sure that all transactions were processed and proper outputs transmitted.

Terminal devices should automatically disconnect when unused for a certain amount of time. However, they should automatically return to service to receive a new transmission.

All output devices should be located in a secure facility, and a priority system should be established so that critical outputs can be transmitted on time. Outputs waiting for transmission should be placed on a backup log before being put in the transmission queue. As outputs are transmitted and received, the terminal output device should send a reply that the outputs were received and that the backup log can be purged. The application should automatically verify that outputs are being transmitted and received by the right terminal and validate the message content for proper characters, format, etc., before displaying, writing, or printing on the terminal output device. The day's activities should be summarized and printed for each terminal device. These activity reports provide the audit trail for output products.

As with batch systems, user department control groups should independently balance and reconcile output products and keep informed of all transactions and records that are internally generated or that come from other systems.

On-line--output distribution

Controls over output distribution for on-line systems are essentially the same as those for batch systems, except that the user department control group is the focal point rather than the data processing department control group. Key control areas include

--documented procedures describing the methods of distribution;

--user department control group scheduling, monitoring, reviewing, and distributing of output products; and

--use of turnaround transmittal documents and distribution checklists to verify and record the receipt of output products by the authorized user.

On-line--output error handling

Controls over output error handling for on-line systems are essentially the same as those for batch systems, except that the user department control group is the focal point rather than the data processing department control group. Key control areas include

--documented procedures describing the methods for reporting and controlling output errors,

--user department control group responsibility for controlling the detection and correction of erroneous output products, and

--use of control logs to identify causes and trends of output errors and to insure timely correction of errors.

On-line--handling and retention of output records and accountable documents

Controls in this area are the same for both on-line and batch processing systems. Key control areas include

--establishing record and document retention periods which provide for adequate backup, record reconstruction, and audit;

--using appropriate waste disposal facilities for unneeded, aborted, and outdated records and documents;

--limiting access to records and documents to authorized individuals; and

--using dual custody over accountable documents.

AUDIT PROCEDURES

Use the background material obtained in section III and:

1. Complete the following questionnaire 13 on data output controls.

2. Complete the appropriate section of profile 3 on application controls.
3. On the basis of the level of potential risk determined on the application controls profile 3, consult the application controls matrix 3 at the end of this section for guidance on additional audit steps.

QUESTIONNAIRE 13

DATA OUTPUT CONTROLS

Data output controls are used to insure the integrity of output and the correct and timely distribution of outputs produced. Not only must outputs be accurate, but they must also be received by users in a timely and consistent manner. Outputs can be produced in two different ways: batch and on-line. The main areas of control include

--output balancing and reconciliation,

--output distribution,

--output error handling, and

--handling and retention of output records and accountable documents.

Of critical importance is the interface between the data processing department and the user department.

The auditor should evaluate the adequacy of controls over outputs to make sure that data processing results are reliable, output control totals are accurate, and reports are distributed in a timely manner to users.

	YES	NO
BATCH--OUTPUT BALANCING AND RECONCILIATION		
1. Do documented procedures exist that explain the methods for proper balancing and reconciliation of output products?	___	___
2. Does the data processing department have a control group which is responsible for reviewing all outputs produced by the application?	___	___
3. Does the data processing control group monitor the processing flow to make sure that application programs are being processed according to schedule?	___	___
4. Does the data processing department control group review output products for general acceptability and completeness?	___	___
5. Does the data processing department control group reconcile each output batch total with		

QUESTIONNAIRE 13

	YES	NO
input batch totals, before the release of any reports, to ensure that no data was added or lost during data processing?	___	___
6. Does the data processing department control group reconcile each output record count with input record counts, before the release of any reports, to insure that no data was added or lost during data processing?	___	___
7. Does the data processing department control group reconcile each output predetermined control total with input predetermined control totals, before the release of any reports, to insure that no data was added or lost during data processing?	___	___
8. Does the data processing department control group keep a log which summarizes the:		
--Number of application reports generated?		
--Number of pages per report?	___	___
--Number of lines per report?	___	___
--Number of copies of each report?	___	___
--Recipient(s) of each report?	___	___
9. Are system output logs kept to provide an audit trail for the outputs?	___	___
10. Are output logs reviewed by supervisors to determine the correctness of output production?	___	___
11. Is a transaction log kept by the application to provide an audit trail for the transactions being processed?	___	___
12. Is a transaction log kept at each output device to provide an audit trail for the transactions being processed?	___	___
13. Is the transaction log kept by the application compared regularly with the transaction log kept at each output device to make sure that all transactions have been properly processed to the final output steps?	___	___

QUESTIONNAIRE 13

	YES	NO
14. Can transactions be traced forward to the final outputs?	___	___
15. Can transactions be traced backward to the original source documents?	___	___
16. On each output product, does the application identify the:		
--Title or name of product?	___	___
--Processing program name or number?	___	___
--Date and time prepared?	___	___
--Processing period covered?	___	___
--User name and location?	___	___
--Counts developed during processing?	___	___
--End-of-job/file/report indication?	___	___
--Security classification, if any?	___	___
17. Does the user department have a control group which is responsible for reviewing all output received from the data processing department?	___	___
18. Is the user department control group given lists of all changes to the application master file data or programmed data?	___	___
19. Is the user department control group given lists of all internally generated transactions produced by the application?	___	___
20. Is the user department control group given lists of all interface transactions processed by the application?	___	___
21. Is the user department control group given a list of all transactions entered into the application?	___	___
22. Are all listings (questions 18-21) reviewed by the user department control group to insure completeness of data processed by the application?	___	___

QUESTIONNAIRE 13

	YES	NO
23. Is the user department control group furnished reports produced by the application which shows the:		
--Batch totals?	___	___
--Record counts?	___	___
--Predetermined control totals?	___	___
24. Does the user department control group verify all computer-generated batch totals with its manually developed batch totals?	___	___
25. Does the user department control group verify all computer generated record counts to their manually developed record counts?	___	___
26. Does the user department control group verify all computer-generated predetermined control totals with its manually developed predetermined control totals?	___	___
27. Does the user department control group verify the accuracy and completeness of all outputs?	___	___
28. Does the user department retain ultimate responsibility for the accuracy of all outputs?	___	___

BATCH--OUTPUT DISTRIBUTION

29. Do documented procedures exist that explain the methods for proper handling and distribution of output products?	___	___
30. Are duties separated to make sure that no one individual performs more than one of the following operations:		
--Originating data?	___	___
--Inputting data?	___	___
--Processing data?	___	___
--Distributing output?	___	___
31. Are users questioned periodically to determine their continued need for the product and the number of copies received?	___	___

QUESTIONNAIRE 13

	YES	NO
32. Does the cover sheet of every report clearly identify the recipient's name and location?	___	___
33. Does the data processing department have a control group which is responsible for distributing all output produced by the computer application?	___	___
34. Does the data processing department control group have a schedule, by application, that shows when output processing will be completed and when output products need to be distributed?	___	___
35. Has a priority system been established so that critical outputs can be produced on time?	___	___
36. Does the data processing department control group keep a log, by application, of all output products produced by the system?	___	___
37. Does this log identify the following for each output product:		
--Job name?	___	___
--Time and date of production?	___	___
--Product name?	___	___
--Time and date of distribution?	___	___
--Name(s) of recipient(s)?	___	___
--Quantity distributed to each recipient?	___	___
--Security status, if any?	___	___
38. Is each entry in the data processing department control group's log signed by supervisors to indicate that the reports were in fact produced and transmitted to recipients?	___	___
39. Does this log include notes on problems that arose with processing (reruns, data checks, etc.)?	___	___

	YES	NO
40. Does the data processing department control group maintain a formalized output distribution checklist to show the disposition of each output product?	___	___
41. Are turnaround transmittal documents used by the data processing department control group to verify that the output product has been received by the authorized recipient?	___	___
42. Is the output distribution checklist used to verify the acknowledgment of all turnaround transmittal documents from recipients of output?	___	___
43. Does the data processing department control group verify that only authorized numbers of copies of outputs are produced?	___	___

BATCH--OUTPUT ERROR HANDLING

44. Do documented procedures exist that explain data processing department methods for reporting, correcting, and reprocessing output products with errors?	___	___
45. Is the user department control group notified immediately by the data processing control group of problems in output products?	___	___
46. Does the data processing department control group keep a control log of output product errors?	___	___
47. Is this log used to:		
--Identify the problem?	___	___
--Note corrective action taken?	___	___
--Record date and time of resubmission?	___	___
--Record date and time of transmission to users?	___	___
48. Do supervisors use this log to make sure that timely resubmissions of jobs are accomplished and corrected reports are expeditiously transmitted to the users?	___	___
49. Does the data processing department control group develop an independent history file of output products with errors?	___	___

QUESTIONNAIRE 13

		YES	NO
50.	Is this file reviewed periodically by supervisors to identify causes of and trends in output product errors?	___	___
51.	Are users kept apprised of progress being made to correct problems that cause output product errors?	___	___
52.	Are the outputs from rerun jobs subjected to the same quality review as the original output products that were found to be in error?	___	___
53.	Do documented procedures exist that explain the methods for user department reporting and control of output product errors?	___	___
54.	Is the user notified immediately by the user department control group of problems in output products?	___	___
55.	Does the user department control group keep a control log of output product errors?	___	___
56.	Is this log used to:		
	--Identify the problem?	___	___
	--Identify data processing department personnel contacted?	___	___
	--Record date and time of data processing department contact?	___	___
	--Record data processing department corrective action taken?	___	___
	--Record date and time of receipt of corrected output product?	___	___
	--Identify causes and trends of output product errors?	___	___
	--Make sure that output product errors are corrected in a timely manner?	___	___

QUESTIONNAIRE 13

	YES	NO
BATCH--HANDLING AND RETENTION OF OUTPUT RECORDS AND ACCOUNTABLE DOCUMENTS		
57. Have record and document retention periods been established?	___	___
58. Are the periods reasonable for backup and audit purposes?	___	___
59. Are appropriate methods (i.e., degaussing, shredding, etc.) used to dispose of unneeded records and documents?	___	___
60. Is access to records and documents restricted to authorized individuals?	___	___
61. Are periodic reviews made to determine if output products are still needed by the user?	___	___
62. Is the dual custody technique used to control accountable documents (check stock, bond stock, identification card stock, etc.) during the following:		
--In storage?	___	___
--In transit?	___	___
--Waiting to be used by the application?	___	___
--Being used by the application?	___	___
--Waiting for distribution?	___	___
--Waiting for destruction?	___	___
--Waiting for transit back to storage?	___	___
63. Is access to accountable documents restricted to authorized personnel?	___	___
ON-LINE--OUTPUT BALANCING AND RECONCILIATION		
64. Do documented procedures exist that explain the methods for proper balancing and reconciliation of output products?	___	___
65. Does the data processing department have a control group responsible for making sure that output products are accurately processed by data processing and correctly transmitted to user terminal devices?	___	___

		YES	NO
66.	Does the data processing department control group have a schedule by application that shows when pre-output processing ends and when output processing begins?	___	___
67.	Does the data processing department control group monitor the processing flow to make sure that application programs are being processed according to schedule?	___	___
68.	Does the data processing department control group reconcile each output batch total with input batch totals, before the transmission of outputs, to insure that no data was added or lost during data processing?	___	___
69.	Does the data processing department control group reconcile each output record count with input record counts, before the transmission of outputs, to insure that no data was added or lost during data processing?	___	___
70.	Does the data processing department control group reconcile output predetermined control totals with input predetermined control totals, before the transmission of outputs, to insure that no data was added or lost during data processing?	___	___
71.	Is a log kept by the application to provide an audit trail for transactions being processed?	___	___
72.	Is a log kept at each output transmission device to provide an audit trail for outputs being transmitted to user terminal devices?	___	___
73.	Is the transaction log kept by the application compared regularly with the transmission log kept at each output transmission device to make sure that all outputs have been properly transmitted to the final users?	___	___
74.	On each output product, does the application system identify:		
	--Title or name of product?	___	___
	--Processing program name or number?	___	___

QUESTIONNAIRE 13

	YES	NO
--Date and time prepared?	___	___
--Processing period covered?	___	___
--User name and location?	___	___
--Counts developed during processing?	___	___
--End-of-job/file/report indication?	___	___
--Security classification, if any?	___	___
75. Do terminal devices automatically disconnect from the computer-based system if they are unused for a certain amount of time?	___	___
76. Do terminal devices need to be logged off at the end of the day so that they will be disconnected from the computer-based system?	___	___
77. Even though teminals are disconnected from the system, can output reports still be transmitted to terminal output devices?	___	___
78. Are output devices located in secure facilities at all times to protect against unauthorized access?	___	___
79. Has a priority system been established so that critical outputs can be transmitted on time?	___	___
80. Are all outputs waiting for transmission placed on a backup log before being put into the transmission queue?	___	___
81. As outputs are transmitted and received, does the terminal output device send a reply that they have been correctly received?	___	___
82. Is the backup log purged when the terminal output device reply has been received?	___	___
83. Does the computer-based system automatically check an output message before displaying, writing, or printing it to make sure that it has not reached the wrong terminal output device?	___	___
84. Is message content validated before displaying, writing, or printing on the terminal output device?	___	___

QUESTIONNAIRE 13

		YES	NO
85.	Can transactions be traced forward to the final output products?	___	___
86.	Can transactions be traced backward to the original source documents?	___	___
87.	Are all the day's activities summarized and printed for each terminal device?	___	___
88.	Are these activity reports used to provide an audit trail for the output products?	___	___
89.	Are these reports reviewed by supervisors to determine the correctness of output production?	___	___
90.	Does the user department have a control group responsible for reviewing all outputs produced by the computer application?	___	___
91.	Does the user department control group reconcile each output batch total with input batch totals, before the release of any reports, to insure that no data was added or lost during data processing?	___	___
92.	Does the user department control group reconcile each output record count with input record counts, before release of any reports, to insure that no data was added or lost during data processing?	___	___
93.	Does the user department control group reconcile output predetermined control totals with input predetermined control totals, before release of any reports, to insure that no data was added or lost during data processing?	___	___
94.	Is the user department control group given lists of all changes to application system master file data or programmed data?	___	___
95.	Is the user department control group given lists of all internally generated transactions produced by the application?	___	___
96.	Is the user department control group given lists of all interface transactions processed by the application?	___	___

QUESTIONNAIRE 13

		YES	NO
97.	Is this user department control group given a list of all transactions entered into the system?	___	___
98.	Are all listings (questions 94-97) reviewed by the user department control group to insure completeness of data processed by the system?	___	___
99.	Does the user department control group verify the accuracy and completeness of all outputs?	___	___
100.	Is the user department ultimately responsibile for the accuracy of all outputs?	___	___

ON-LINE--OUTPUT DISTRIBUTION

101.	Do documented procedures exist that explain the methods for proper handling and distribution of output products?	___	___
102.	Are duties separated to make sure that no one individual performs more than one of the following operations:		
	--Originating data?	___	___
	--Inputting data?	___	___
	--Processing data?	___	___
	--Distributing output?	___	___
103.	Are users questioned periodically to determine their continued need for the products and the number of copies received?	___	___
104.	Does the user department have a control group responsible for distributing all output products produced by the application?	___	___
105.	Does the user department control group have a schedule, by application, that shows when output processing will be completed and when output products need to be distributed?	___	___
106.	Does the user department control group monitor system outputs to make sure that application programs are being processed according to schedule?	___	___

QUESTIONNAIRE 13

		YES	NO
107.	Does the user department control group maintain a formalized output distribution checklist to show the disposition of each output product?	___	___
108.	Are turnaround transmittal documents used by the data processing department control group to verify that the output product has been received by the authorized recipient?	___	___
109.	Is the checklist used to verify the acknowledgment of all turnaround transmittal documents from recipients of outputs?	___	___

ON-LINE--OUTPUT ERROR HANDLING

110.	Do documented procedures exist that explain the methods for user department reporting and control of output errors?	___	___
111.	Is the user notified immediately by the user department control group of problems in outputs?	___	___
112.	Does the user department control group keep a control log of output product errors?	___	___
113.	Is this log used to:		
	--Identify the problem?	___	___
	--Identify data processing department personnel contacted?	___	___
	--Record date and time of data processing department contact?	___	___
	--Record data processing department corrective action taken?	___	___
	--Record date and time of receipt of corrected output product?	___	___
	--Identify causes and trends of output product errors?	___	___
	--Make sure that output product errors are corrected in a timely manner?	___	___

	YES	NO
114. Are the outputs from rerun jobs subject to the same quality review as the original output products that were found to be in error?	___	___

ON-LINE--HANDLING AND RETENTION OF OUTPUT RECORDS AND ACCOUNTABLE DOCUMENTS

115. Have record and document retention periods been established?	___	___
116. Are the periods reasonable for backup and audit purposes?	___	___
117. Are appropriate methods (i.e., degaussing, shredding, etc.) used to dispose of unneeded records and documents?	___	___
118. Is access to records and documents restricted to authorized individuals?	___	___
119. Are periodic reviews made to determine if output products are still needed by the user?	___	___
120. Is the dual custody technique used to control accountable documents (check stock, bond stock, identification card stock, etc.) during the following:		
--In storage?	___	___
--In transit?	___	___
--Waiting to be used by the application?	___	___
--Being used by the application?	___	___
--Waiting for distribution?	___	___
--Waiting for destruction?	___	___
--Waiting for transit back to storage?	___	___
121. Is access to accountable documents restricted to authorized personnel only?	___	___

NOTES: Questions should be self-explanatory. Responses will frequently be a simple "yes" or "no." All responses should be indexed to appropriate supporting documents or records of interviews. Explain any "no" answers and identify alternate control procedures.

APPLICATION CONTROLS PROFILE

On the basis of questionnaire responses and other information obtained relating to the following control characteristics, how much risk (low, medium or high) do you believe is involved in relying on the agency's application controls to assure accurate and reliable data processing? Refer to appendix II for more information on assessing risk.

Control characteristics	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level of potential risk?
DATA ORIGINATION CONTROLS					
Source document origination					
Source document authorization					
Source document data collection and input preparation					
Source document error handling					
Source document retention					
DATA INPUT CONTROLS					
Batch--data conversion and entry					
Batch--data validation and editing					
Batch--data input error handling					
On-line--data conversion and entry					

PROFILE 3

APPLICATION CONTROLS PROFILE

Control characteristics	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level poten ris
On-line--data validation and editing					
On-line--data input error handling					
DATA PROCESSING CONTROLS					
Batch--data processing integrity					
Batch--data processing validation and editing					
Batch--data processing error handling					
Real-time--data processing integrity					
Real-time--data processing validation and editing					
Real-time--data processing error handling					
DATA OUTPUT CONTROLS					
Batch--output balancing and reconciliation					

PROFILE 3

APPLICATION CONTROLS PROFILE

Control characteristics	Is the control in place?	Is the control effective?	Is some alternate control in place?	Is the alternate control effective?	Level of potential risk?
Batch--output distribution					
Batch--output error handling					
Batch--handling and retention of output records and accountable documents					
On-line--output balancing and reconciliation					
On-line--output distribution					
On-line--output error handling					
On-line--handling and retention of output records and accountable documents					

MATRIX 3

APPLICATION CONTROLS MATRIX

If the degree of risk determined on the previous profile warrants additional audit work (medium or high risk), the following matrix should help the auidtor select appropriate audit steps to complete the review.

	document the data flow	observe operations	obtain user satisfaction	process test data	perform computer program analysis	perform data retrieval analysis	analyze job accounting data	report deficiencies	suggest additional audit
Data Origination Controls									
Source Document Organization	●	●						●	
Source Document Authorization	●	●						●	
Source Document Collection and Input Preparation	●	●						●	
Source Document Error Handling	●	●						●	
Source Document Handling and Retention	●	●						●	
Data Input Controls									
Batch--Data Conversion and Entry	●	●		●	●	●	●	●	
Batch--Data Validation and Editing	●	●		●	●	●		●	
Batch--Data Input Error Handling	●	●	●	●	●	●		●	
On-Line--Data Conversion and Entry	●	●		●	●	●	●	●	
On-Line--Data Validation and Editing	●	●		●	●	●		●	
On-Line--Data Input Error Handling	●	●	●	●	●	●		●	

MATRIX 3

APPLICATION CONTROLS MATRIX

Data Processing Controls	document the data flow	observe operations	obtain user satisfaction	process test data	perform computer program analysis	perform data retrieval analysis	analyze job accounting data	report deficiencies	suggest additional audit
Batch--Data Processing Integrity	●	●		●	●	●		●	
Batch--Data Processing Validation and Editing	●	●		●	●	●		●	
Batch--Data Processing Error Handling	●	●	●	●	●	●		●	
Real Time--Data Processing Integrity	●	●		●	●	●	●	●	
Real Time--Data Processing Validation and Editing	●	●		●	●	●		●	
Real Time--Data Processing Error Handling	●	●	●	●	●	●		●	
Data Output Controls									
Batch--Output Balancing and Reconciliation	●	●		●				●	
Batch--Output Distribution	●	●		●			●	●	
Batch--Output Error Handling	●	●	●	●				●	
Batch--Handling and Retention of Output Records and Accountable Documents	●	●		●				●	
On-Line--Output Balancing and Reconciliation	●	●		●				●	
On-Line--Output Distribution	●	●		●			●	●	
On-Line--Output Error Handling	●	●	●	●				●	
On-Line--Handling and Retention of Output Records and Accountable Documents	●	●		●				●	

Detailed Analysis & Testing Phase

On the basis of the results of work done in the internal controls phase, the auditor should perform some level of detailed analysis and testing of the application to substantiate and verify the existence and effectiveness of internal controls. Usually, the auditor should

--prepare a data flow diagram,
--observe manual and automated processing of data,
--obtain user satisfaction with computer output, and
--verify a sample of master records with source documents.

If control weaknesses are disclosed, the auditor may use computer audit techniques to identify the amount and extent of errors that exist. The auditor could

--analyze the system with test data,
--analyze computer programs with specialized software packages,
--retrieve and analyze data with generalized audit software packages, or
--analyze job accounting data.

The auditor may use one or all these techniques on any given audit.

SECTION VII

DATA FLOW ANALYSIS

Data flow analysis (also known as transaction flow analysis or control flowcharting) is an audit technique where flowcharting symbols and narrative descriptions are used to visually display an overall picture of internal controls in a computer application. This technique has proven to be of great value in simplifying the identification of internal controls and their interrelationships in a system and in helping to assess their adequacy. This analysis can be performed at various levels of detail as warranted by the complexity of the application and the severity of control weaknesses disclosed. Data flow analysis also helps the auditor evaluate the adequacy and accuracy of application documentation and the effectiveness of computer processing. It is, however, time consuming and detailed work which must be anticipated when planning the audit.

PREPARING A DATA FLOW DIAGRAM

To prepare such a diagram, the auditor needs copies of application documentation. Most of this should have been collected in section III. As a minimum, the auditor should have

--narrative descriptions of all major application programs;

--examples of all manually prepared source documents, coding sheets, and data transcription instructions;

--record layouts for all major computer input and output files, master files, and work files;

--examples of all major output products; and

--lists or dictionaries of standard codes, constants, and tables.

Once documentation has been collected, the auditor should use it, along with information developed during the internal controls phase, to prepare a data flow diagram. The diagram should identify

--the point of origin for all source documents, including the organization, title, and individual;

--all control points where source documents are transferred from one person or office to another;

--transcriptions, coversions, or entry of data from source documents to machine-readable format;

--computer processing of application data;

--all major outputs created by the application; and

--recipients of all major outputs.

An example of a data flow diagram is shown in exhibit 1. For guidance on flowcharting techniques, refer to the Federal Information Processing Standards (FIPS) Publication No. 24, "Flowchart Symbols and Their Usage in Information Processing," prepared by the National Bureau of Standards, Department of Commerce.

EVALUATING CONTROLS OVER DATA

Once the data flow diagram has been prepared, the auditor should identify control points in the application and describe the types of control used (i.e., record counts, passwords, etc.). Exhibit 1 also illustrates this process. Effective controls generally mean that a control exists every time data moves within a department, between departments, and between processing steps and when data is added, deleted, or manipulated. The auditor should also identify points in the data flow where controls are

deficient or missing. A complete data flow diagram should show the overall network of controls over the application being reviewed.

EVALUATING QUALITY OF DOCUMENTATION

On the basis of answers to the documentation part of questionnaire 5 and the degree of difficulty experienced in constructing the data flow diagram, sufficient information should be available to evaluate the quality of the application documentation. The auditor should be able to determine whether documentation is complete, accurate, and up to date. Criteria for this evaluation are included in FIPS Publication No. 38, "Guidelines for Documentation of Computer Programs and Automated Data Systems," dated February 1976, and FIPS Publication No. 64, "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase," dated August 1979.

EVALUATING COMPUTER PROCESSING EFFECTIVENESS

In preparing a data flow diagram, the auditor may identify problem areas in the application processing cycle, including

--redundant processing of data or other forms of duplication,

--bottlenecks that delay processing, or

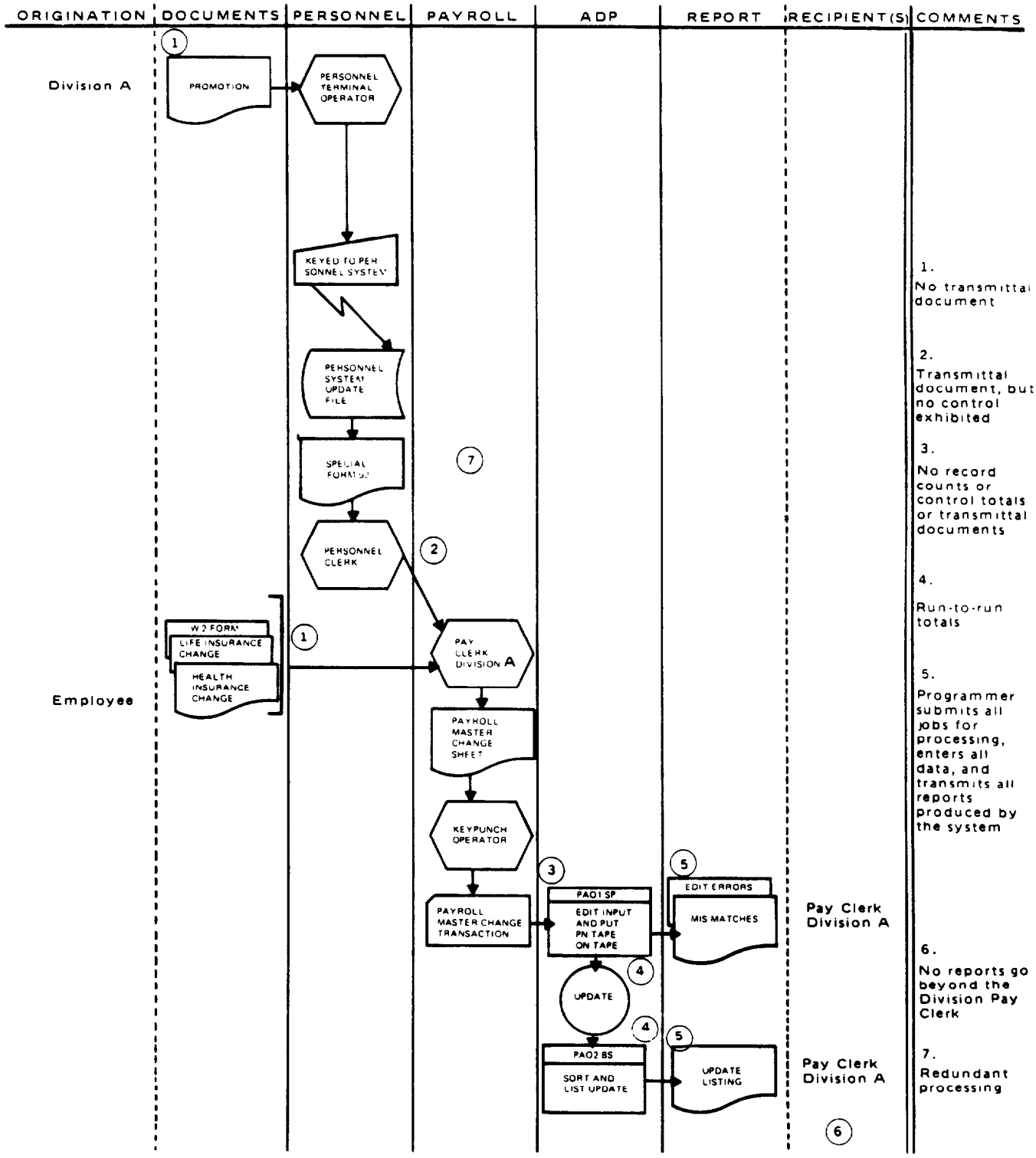
--points in the operation where insufficient time has been allocated to perform a task.

These areas may be discussed in the final report or may result in suggestions for additional audit work because of their impact on the accuracy and timeliness of the application being reviewed.

EXHIBIT 1

EXHIBIT 1

EXAMPLE OF A DATA FLOW DIAGRAM



SECTION VIII

OBSERVATION ANALYSIS

Periodically during the audit, the auditor should observe actual processing of the application. The objective is to confirm that control practices are being followed and that the application is being processed in accordance with documentation. These observations should be spread throughout the period under audit to help determine whether control lapses occur due to sickness, vacation, personnel turnover, etc. At least one visit should be unannounced. For discussion, observation of processing is divided into manual operations and automated operations.

OBSERVING MANUAL OPERATIONS

Manual operations include procedures that are performed before data is converted into a machine-readable format and after outputs have been created. This observation should confirm

--controls over origination and entry of data,

--the degree of separation of duties during manual processing,

--effectiveness of physical protection controls in manual processing departments, and

--controls over the receipt and distribution of outputs.

The previously developed data flow diagram should be used as a guide in observing manual operations.

OBSERVING AUTOMATED OPERATIONS

Automated operations include those procedures that begin with the conversion of data to machine-readable form and end when output products are created. Auditor observations should confirm

--controls over the conversion and entry of data;

--controls used during processing;

--the degree of separation of duties during automated processing;

--the effectiveness of physical protection controls over the computer center, data entry devices, etc.;

--the quality of housekeeping in the computer center; and

--controls over the creation of output products.

General criteria for evaluating typical protection controls over automated operations are included in FIPS Publication 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management," dated June 1975; FIPS Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," dated May 1975; and FIPS Publication 73, "Guidelines for Security of Computer Applications," dated June 1980. General criteria for evaluating the quality of ADP management is included in the General Services Administration's Federal Property Management Regulations, Title 41, Part 101-Subchapter F.

Control problems identified while observing manual and automated operations should be brought to the immediate attention of the agency for corrective action. These problems may be discussed in the final report or may result in suggestions for additional audit work depending on their impact on the accuracy and timeliness of the application(s) being reviewed.

SECTION IX

USER SATISFACTION ANALYSIS

Users of data or reports produced by a computer application can help the auditor identify errors in processing or other major problem areas. The auditor should, therefore, identify and interview all principal users to determine exactly how they use the data and what their opinions are concerning its accuracy, timeliness, and completeness.

IDENTIFYING PRINCIPAL USERS

For each major computer output, all users should be identified from a current computer product distribution list, which should be available from data processing department personnel. Exhibit 2, "Principal Users Overview," can be used as an aid in identifying users.

DETERMINING USER SATISFACTION

Typically, users have varying knowledge about product quality. To make sure user responses are reliable, the auditor should personally interview enough users to develop a general idea about computer output usefulness. Exhibit 3, "User Satisfaction Questionnaire," provides questions for determining user satisfaction.

When there are many principal users or several users at different locations, it may be impractical to personally interview each one. In these cases, the auditor may (1) select a sample of users based on number, location, or some other suitable criterion, (2) interview users by telephone, or (3) distribute the questionnaire for users to complete. In the last situation, the auditor

must maintain control over questionnaires and conduct some follow-up to assure accurate responses.

When conducting interviews, it is especially important to obtain evidence of incomplete or inaccurate data identified by a user. The auditor should determine

--the nature of the problem--amounts overstated or understated incorrect totals, incomplete data fields, and negative balances which should be positive;

--how frequently errors are observed--isolated instances or recurring problems;

--whether the user can help explain why errors are made--since errors affect users the most, they may have conducted studies to show the cause and magnitude of errors; and

--whether users keep manual records for use instead of computer reports or output--manually kept records in a computer environment can mean poor quality of computer output and unnecessary expenditures for duplicate record-keeping.

User comments can help substantiate earlier audit findings and help direct audit coverage to specific areas. Information obtained in this section is normally included in the final report on the application being reviewed.

EXHIBIT 2

PRINCIPAL USERS OVERVIEW

Computer product				User		
Name	Number	Type	Purpose	Name	Function	Comments

EXHIBIT 3

USER SATISFACTION QUESTIONNAIRE

This questionnaire is designed to obtain user evaluations of computer products. It includes questions on product format, sufficiency and accuracy of reported information, necessity for the product, and possibilities for product improvement. Since computer output is generated for users, responses to this questionnaire can be considered strong indicators of whether computer products are accurate and reliable.

Product identification

1. Title of product. _____
2. Data processing identification number. _____
3. Type of product. _____
4. Part of product to be evaluated. _____

_____

_____

5. Frequency of product. _____

User identification

6. Name. _____
7. Date. _____
8. Title. _____
9. Organization. _____
10. Phone number/address. _____
11. Extent of knowledge about product. _____

_____

_____

_____

_____

EXHIBIT 3

User evaluation of output product

12. For what purpose do you use the product?

	YES	NO
--Initiate transactions.	___	___
--Authorize changes to the system.	___	___
--Operate computer terminal.	___	___
--Maintain data controls.	___	___
--Design/program applications.	___	___
--Other. (Explain.)_____		
_____	___	___

13. In relation to the work of your office or department, the product is

Not important — Very important

1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10

14. The product's contents are

Very difficult to understand — Very easy to understand

1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10

15. Can the product be used as is without correction, further identification, or analysis? _____YES _____NO

16. In your judgment, is the product:

	YES	NO
--Accurate and reliable?	___	___
--Available when needed?	___	___
--Current and up to date?	___	___
--Useful?	___	___
--Understandable?	___	___

For each "no" answer, please explain below and provide examples.

_____

_____

_____

_____

_____

_____

EXHIBIT 3

17. In your opinion, should the product:

	YES	NO
--Provide more data?	___	___
--Provide less data?	___	___
--Be combined with other output products?	___	___
--Be considered obsolete?	___	___
--Be improved to make your job easier?	___	___

For each "yes" answer, please explain below.

_____

_____

_____

_____

18. If you maintain manual records to supplement computer-processed information, briefly explain why.

_____

_____

_____

19. Does the product duplicate any other information you receive? _____YES _____NO

If "yes", briefly explain._____

_____

_____

20. Can you readily obtain, from other sources, the information in the product? _____YES _____NO

If "yes", list the other source(s)._____

_____

_____

21. Do you supply the raw data (input) for this product? _____YES _____NO

22. Do you check this product for quality when you receive it? _____YES _____NO

If "no", please identify the person or group performing this function._____

_____

EXHIBIT 3

23. Is the product ever rerun by the data processing department? _____YES _____NO

If "yes":

--How frequently? _____
--Why were reruns necessary? _____
--How do you make sure that rerun material is correct? _____

24. If you have/had problems with this product, with whom would/did you discuss them? _____

_____

Is this person authorized to make changes to the product?
_____YES _____NO

25. Do you maintain correspondence with the data processing department or other user departments concerning the product? _____YES _____NO

If yes, attach copies of recent correspondence.

26. Could you effectively perform your duties:

	YES	NO
--Without this product?	___	___
--If this product were produced less often?	___	___

27. Did you or anyone within your department help design the product? _____YES _____NO

28. Does it save you any clerical effort?
_____YES _____NO

Explain. _____

_____

29. Can this product be improved to make your job easier?
_____YES _____NO

Explain. _____

_____

_____

_____

_____

EXHIBIT 3

30. How often do you refer to this product?

	YES	NO
--Daily.	___	___
--Weekly.	___	___
--Monthly.	___	___
--Annually.	___	___
--Never.	___	___
--Other. (Explain.)_____	___	___

_____

31. How long is the product kept after receipt?

	YES	NO
--1 day.	___	___
--1 week.	___	___
--1 year.	___	___
--Other. (Explain.)_____		

_____

Where is the product filed? _____

_____

SECTION X

TEST DATA ANALYSIS

Test data analysis involves using simulated transactions designed to test processing logic, computations, and controls actually programmed in the computer application. If test transactions are prepared in accordance with user procedures, test data analysis can also help the auditor evaluate these procedures. Test data analysis can be used to evaluate individual programs or an entire system. It can be extremely complex and time consuming depending on the number of transactions processed, the number of programs to be tested, and the complexity of the application. Test data analysis only points out the potential for erroneous processing; it does not evaluate actual production data. Test data analysis can direct the auditor to areas where erroneous processing has occurred, especially when used in conjunction with data retrieval and program analysis techniques discussed later.

DEVELOPING TEST DATA

Before trying to conduct test data analysis, the auditor must first have a detailed understanding of system functions, along with indications that there are potential problems with controls, computations, or other processing logic in the application. The auditor obtains such information by completing a data flow analysis, observing processing, and determining that programs were not adequately tested or do not contain adequate built-in controls and audit trails. Indications of control problems would come from negative responses to questionnaire 5. This knowledge is essential because it helps the auditor test a particular program or processing step rather than an entire system.

If the decision is made to use test data, the auditor should develop a detailed plan outlining the testing to be performed. It should include

--a list of transaction types and conditions to be tested;

--a list of various types of errors and error conditions to be tested;

--input procedures to be tested and the input media to be used;

--master files to be created and used;

--volume of test data; and

--a description of audit objectives, scope of testing, and impact on normal operations.

This test plan should be used for coordination with agency personnel so that they can arrange for test data processing and provide other required services, such as keypunching.

When creating test data, the audit objective should be to determine if the program or entire application (1) processes normal transactions accurately and in a timely manner, and (2) rejects or "flags" invalid transactions to make sure that they do not affect data accuracy and can be adequately controlled for correction and reentry into the system. Normal test transactions should exercise the program's ability to establish, change, and delete master records; perform calculations; and and test processing logic. Invalid test transactions should try to process

--alphabetic characters in numeric fields (and vice versa);

--invalid account or identification codes;

--incomplete, extraneous, and missing data in input fields;

--negative amounts in positive-only fields (and vice versa);

--illogical conditions in related data fields; and

--illegal or nonstandard limits or balances.

Invalid test data should also be designed to determine if edit checks exist and work properly.

Test data can be prepared in a number of ways.

The simplest way is to obtain and manually prepare all input forms needed to test a specific condition. This approach can be used to create both master records and transactions to test the various controls, computations, and processing logic. This approach can be modified by copying existing master records onto a test master and then preparing the desired test transactions. This modified approach precludes the need to create new master records for use in testing. Manually prepared test data has several advantages. For example, desired functions can be tested with known variables; test results can be easily predetermined since only one test transaction is processed against each master record; and test volumes can be kept to manageable levels. This approach does require, however, a considerable time investment and does introduce the likelihood of human error in preparing test data.

Another approach to the preparation of test data is to select actual "live" transactions to be used as test data. This approach is less time consuming, but it does have some disadvantages. First, even though there may be volumes of transactions to pick from, specific transactions to test certain computer or logic routines may not be available. This is especially true for invalid test transactions because most live transactions

should include only valid data. Second, the ability to predetermine test results may be difficult because live transactions may exercise more than one function per master record. While these transactions can be traced through the system to determine what happened, this work will increase evaluation time and may more than offset any time savings in test data preparation.

A third approach is to use test data generator software packages. Normally, test data generators create test data through use of control parameters. Such programs generally provide ranges of values to be generated on separate transactions for a given data element, thus providing ample data for testing automated controls, computations, and program logic. They also eliminate errors that normally accompany manual test data preparation. Test data generators, however, have certain disadvantages. They may

--require as much effort to devise a particular transaction type as manually prepared test data,

--significantly increase the amount of time needed to evaluate test data results due to the volume of transactions that can be generated, and

--produce test media which is incompatible with the program or system being tested (i.e., produces cards when system needs tape).

No matter which method of test data preparation is used, care must be taken to make sure that test data developed satisfies audit objectives in the test plan. Because manually prepared test data is more easily controlled by the auditor, this manual method is recommended.

PROCESSING TEST DATA

Test data is normally processed either in a parallel processing run or through an integrated test facility. Each is discussed separately below.

Processing test data in a parallel processing run is the simplest method. After test data has been prepared, a special "run" of the computer program or application should be scheduled. If the auditor plans to test processing procedures as well, data conversion and data entry must also be scheduled. Test data should be processed against the latest production version of computer programs. All test transactions and test files must be segregated from regular production processing so that test data is not accidently introduced into the live production system. To assure proper processing, the auditor should observe the entire test data processing operation--from conversion of source documents to the creation of output reports and files.

Parallel processing of test data works best when testing batch input and batch processing systems. On-line test data is more difficult to keep separate from live data. Either the on-line input system must be made operational during special hours, or special codes may have to be included on test data so that it can be separated from live data at a later date. Even if care is taken in handling on-line input, there is still a risk that test data may be mixed with live data. For real-time processing systems, the problem of keeping test data separate from live data becomes much more difficult. A special run of the entire application at nonregular processing time is almost a necessity

if parallel processing is to be performed. This procedure may not always be feasible.

Because of the above difficulties, the integrated test facility (ITF) concept was developed. An ITF permits the auditor to examine an application in its normal operating environment. This technique involves processing test transactions against a fictitious, or "dummy," entity integrated into the normal production system. Normal application processing produces reports that the auditor uses to verify the completeness and accuracy of individual programs or entire systems. All transaction types, combination of types, logic paths, computations, and controls within the application can be tested by this method at any time.

When using an ITF, the auditor must establish additional controls to make sure that test data is not posted to live production records. For example, all test data must be keyed to or identified with a fictitious entity by using a unique identification code. In addition, special procedures must be established to (1) make sure that test data is separated and not included in final output reports and accounting records and (2) prevent test data from being communicated to other applications within the agency. These additional procedures require the auditor to

--modify existing programs to separate test data from live production data,

--manually adjust output reports to reverse transactions or delete test data, or

--design the application so it can process but keep separate both test data and normal production data.

The best time to establish an ITF is during the initial design of an application. This procedure eliminates the cost of modifying programs after the fact and reduces the amount of manual intervention for reversal transactions. For more details on ITFs and a discussion of a unique technique developed by GAO for incorporating ITFs in operational systems, refer to the Summer 1977, GAO Review article "A Simultaneous Parallel Approach to Testing Computerized Systems."

An ITF provides a comprehensive method for auditors and system development personnel to evaluate controls, computations, and processing logic in an application. Once the ITF is operational, audit checks can be performed on a regular and unscheduled basis, which provide a strong deterrent to erroneous or fraudulent processing. The ITF requires minimum costs to maintain because test data volumes are normally small compared with actual production. When used successfully, the ITF provides objective evidence that policies, procedures, and specifications are being followed.

EVALUATING TEST DATA

Once test data has been processed, test results should be compared with predetermined results. Deviations which require analysis, correction, and reentry may be encountered. The auditor may have to run several cycles of the actual test until all test conditions have been satisfied. When differences occur between actual and predetermined results, indicating control weaknesses, the auditor should document these findings and determine whether manual or automated compensating controls exist. If compensating controls do not exist, the auditor should assess

the effect of the control weakness on the accuracy and reliability of computer produced data. Even if an alternate manual control compensates for a control weakness, the auditor should consider recommending replacement of the manual control with an automated control. Generally, automating a manual operation will increase processing speed, avoid some personnel costs, and reduce human errors.

Control weaknesses disclosed by test data processing help show the potential for errors or problems. The auditor can determine the extent or signficance of these potential errors by using data retrieval and analysis routines discussed later. In other words, the auditor should evaluate test data results to determine the type of records that should be retrieved for analysis. If the auditor determines that control deficiencies adversely affect data reliability, analysis of a particular program or data element processing may be necessary to pinpoint the location where additional controls or other corrective action is needed. Program analysis techniques discussed in the next section permit the auditor to do this.

SECTION XI

COMPUTER PROGRAM ANALYSIS

Computer program analysis involves the use of specialized software packages that analyze job control statements and COBOL source programs and generate reports that detail the flow of data through a computer application along with the logic, computations, and controls incorporated within an application. Program analysis is extremely complex and requires a working knowledge of both the vendor's job control statements and the COBOL programming language. In the hands of a skilled auditor, program analysis can help pinpoint problem areas where errors are likely be made.

SPECIALIZED SOFTWARE PACKAGES AVAILABLE

To aid in analyzing programs, GAO acquired DCD-II, Automatic COBOL Documentation System, a software package developed by CGA Software Products Group, Rockville, Maryland. A detailed explanation of the package is included in the GAO CAATS Manual. Its capabilities are briefly summarized in the remainder of this section.

DCD-II operates at two levels: the program level, and the system level. Each is discussed below.

Program level reports

DCD-II's program facility is a comprehensive and complete COBOL program documentation system. At this program level, three reports can be generated at the auditor's discretion:

--Source List Report.

--Layout Documentation Report.

--Expanded Cross-Reference Listing.

The Source List Report is produced every time that DCD-II is run unless the auditor specifically requests that it be omitted. The report includes reproduced source program elements or statements on the left and a narrative on the right defining data manipulation and program control statements. This information permits the auditor to quickly trace a data item through its entire processing path--from input through working storage to output--and to evaluate controls over the data element.

The Layout Documentation Report provides a graphic representation of all files, records, and working storage described in the COBOL data division section. The length, picture type, and relative locations of each data name are printed, and any initial values are printed just below the data name. This report provides a reference index in the order of appearance in the files and the individual areas used by the COBOL program. This descriptive information will help the auditor evaluate data files that have not otherwise been adequately documented.

The Expanded Cross-Reference Listing provides an alphabetic index of all data elements used in the COBOL program, including references to literals, unreferenced names, constants, indexes, special registers, figurative constants, and "copy's." It also documents the use of all paragraphs and sections within the COBOL program. For the auditor, the list provides a quick reference for locating a particular data element or procedure for analysis.

System level reports

DCD-II's system facility permits analysis of multiple COBOL programs within a given system. There are five system level reports covering different aspects of system documentation:

--File Analysis Report.

--Data Analysis Report.

--Copy Analysis Report.

--Linkage Analysis Report.

--Data Set Analysis Report.

The File Analysis Report consists of two parts, a record summary and a data element summary. The record summary indicates whether selected records were modified by the program, used to create another field or record, and/or checked by the processing program. The data element summary expands the record summary for selected records to describe each data name in the record. It then lists other information, like location, name of field, program name, etc. By reviewing a File Analysis Report, the auditor can determine which COBOL programs process a given record or data element and what type of processing was performed. This report helps the auditor isolate COBOL programs which should be reviewed at the program level.

The Data Analysis Report is analogous to the Expanded Cross-Reference Listing at the program level. It provides a detailed alphabetic cross-reference list of all data elements processed by a system of COBOL programs. It provides the same information as the Expanded Cross-Reference Listing, with the addition of the program name containing the data element. Again, it provides the auditor a quick reference for locating data elements or procedures for further analysis.

The Copy Analysis Report contains a program reference section and a member reference section. Each contains the same information but is sorted differently. The program reference

section lists all "copy" members referenced for each COBOL program constituting the system. The member reference section lists all programs which reference each "copy" member. This report is extremely important to the auditor because it identifies programs which are actually copied into and used by other programs.· This copy feature can be used to hide illegal or fraudulent coding.

The Linkage Analysis Report is similar to the Copy Analysis Report, except that it identifies linkages to external programs rather than to programs copied into the system. The Linkage Analysis Report records all "entries" and "calls" and their linkage parameters within the system. This report contains a program linkage section and a call/entry linkage section. Both contain the same information but are sorted differently. For each COBOL program, the program linkage section lists all called subprograms and calling parameters, as well as all entry point names and their linkage parameters. For each called subprogram or entry point name, the call/entry linkage section lists programs that called the subprogram, the entry point, and the capacity. Again, this report is extremely important to the auditor because it helps identify other computer programs used by the application.

The Data Set Analysis Report is created from the job control statements used to process a given system. It provides the data set name, the COBOL program which uses the data set, the procedure the COBOL program uses, the step number and name in the procedure where the data s is referenced, and the corresponding job control statement definition name. This report helps the

auditor trace a data set through the system and identify locations where specific programs process it.

PREPARING FOR PROGRAM ANALYSIS

After completing data flow analysis and observing computer processing, the auditor may have indications that certain computer programs or an entire system has not been adequately tested or documented. If, in the auditor's judgment, there is further need to document or substantiate the existence and function of certain controls, computations, or other processing logic, a program analysis may be in order. If so, the auditor should prepare a detailed plan of the analysis that is to be done. It should include

--a list of transaction types and conditions to be analyzed;

--a list of data elements to be evaluated;

--a list of computer programs, subsystems, or systems to be analyzed, including program name, location, and format;

--the level of analysis to be performed;

--the type(s) of DCD-II reports to be generated; and

--a description of audit objectives, scope of analysis, and impact on normal operations.

The plan should be used for coordination with agency personnel so they can arrange for processing and provide other needed assistance.

When performing program analysis, the auditor should make sure that the source program being evaluated is the same one being used in actual production. In most instances, the production program is in object code format. To make sure that this object program was derived from the source program being analyzed, the auditor could compile the source program and use a data retrieval

package to compare the newly derived object program with the one in production status. The auditor should resolve any differences before proceeding with program analysis.

PROCESSING PROGRAM ANALYSIS

Operating procedures for using the DCD-II software package are included in the GAO CAATS Manual. The auditor should follow these procedures closely and document the step-by-step process so that it can be repeated. The auditor does not have to arrange for a separate stand-alone run of the DCD-II software. In a normal multiprogramming environment, the auditor should be able to run the DCD-II package with other processing programs. The auditor should observe and control program analysis processing.

EVALUATING PROGRAM ANALYSIS

The auditor should analyze program analysis reports and identify and document any control discrepancies. If discrepancies exist, the auditor should try to determine whether manual or automated compensating controls exist. If not, the auditor should determine the effect of the control weakness on the reliability of output reports or other computer products. The extent to which these control deficiencies affect the accuracy and reliability of data can best be determined by using data retrieval and analysis routines discussed later. If manual compensating controls exist, the auditor should consider recommending their replacement with automated controls to reduce human error. All deficiencies should be reported for corrective action by agency management.

SECTION XII

DATA RETRIEVAL AND ANALYSIS

Computerized data retrieval and analysis is performed with generalized audit software packages. These packages include a series of computer programs that have the power and flexibility of programming languages, but can be easily coded on preprinted parameter forms and debugged usually in a fraction of the time it takes to do the same problem in common programming languages such as COBOL or BASIC. They permit an auditor to perform the same functions that can be done through the use of programming languages, such as reading data, manipulating data, sorting data, and printing reports.

GAO currently uses two data retrieval and analysis packages. They are DYL-260 and DYL-AUDIT. Both were developed by DYLAKOR Software Systems, Inc., Granada Hills, California. DYL-260 is an easy to use extended utility, data management system with flexible report writing capabilities. DYL-AUDIT is an audit package that provides a wide range of functions, such as sampling, aging analysis, frequency distribution reporting, and confirmation letter writing. Both packages are ideal for auditing computerized data in GAO's environment, where quick response and one-time analysis and reporting are normal.

TYPES OF AUDIT FUNCTIONS PERFORMED

Many audit functions can be performed through use of computerized data retrieval and analysis. Those functions most frequently used in GAO audits are discussed below.

Reading and evaluating data

DYL-260 can read just about any form of computer data (cards, tapes, disks, etc.), and just about any file organization (sequential, random, undefined, etc.). Millions of records can be read quickly and efficiently in a fraction of the time it would take to manually read the same number of records. On the basis of various auditor-selected criteria, records can be searched for errors and identified for detailed evaluation. These errors can then be traced back into the computer system to identify specific problems.

Selecting samples

DYL-260 and DYL-AUDIT can both be used to select statistically valid samples if the data is in computerized format or if the report being used came from a computerized data base. Several different types of sampling techniques have been developed in-house for use with DYL-260. These techniques are described in detail in GAO's CAATS Manual. DYLAKOR has also developed many sampling techniques for the DYL-AUDIT package. These techniques are described in detail in a separate DYL-AUDIT Reference Manual.

Performing calculations

Calculations can be performed quickly and efficiently using DYL-260. A full range of mathematical operations are available with the package. Any number of calculations can be performed in a matter of seconds. These calculations can be performed in any combination or sequence. They can be used to recalculate figures produced by computer applications.

Matching data

DYL-260 can be used to match data included in several different data bases. DYL-260 has an automatic update feature that matches two different data bases and identifies records that match or mismatch. DYL-260 also permits the auditor to write code that matches up to a total of eight different data bases. These techniques permit the auditor to compare or verify agency data with that from outside sources and to verify the accuracy of interfaces between different data bases to make sure that data was exchanged correctly. The auditor can also use this technique to match or compare object code in computer programs.

Summarizing data

DYL-260 can be easily used to summarize or aggregate data in a various of ways. Through use of control breaks, data can be totaled at different levels.

Aging data

DYL-AUDIT has an automatic aging analysis function. Up to 9 different aging analyses can be performed with 10 different date ranges or groups (i.e., 1 to 30 days, 31 to 60 days, etc.). Reports, either summary or detail, can be produced automatically by DYL-AUDIT.

Sorting data

DYL-260 has a sort function which sorts records in any sequence desired. This function can be imbedded in any DYL-260 application. This technique permits sorting to be included along with other processing and precludes the need for an intermediate sort application. Sorting permits the auditor to rearrange the sequence of data to meet audit needs.

Frequency distribution reporting

DYL-AUDIT has an automatic frequency distribution reporting function that permits the auditor to arrange numerical data in graduated categories, or groupings, called intervals. The auditor can specify up to 147 simple arithmetic or logarithmic intervals. DYL-AUDIT automatically accumulates totals for each interval and provides statistically important values, including mean and standard deviation, in either a table or a graphic format.

Writing reports or letters

DYL-260 has a full range of report-writing capabilities. An automatic feature is available that permits quick and easy report compositions. In addition, the auditor can also prepare detailed reports using DYL-260's extended report-writing capabilities. DYL-AUDIT contains a letter-writing function which produces form letters that can have variable information, such as names, addresses, dates, and amounts, inserted into the body of the letter. This letter-writing function is of particular value when preparing confirmation letters.

PREPARING A DATA RETRIEVAL AND ANALYSIS APPLICATION

When using DYL-260 or DYL-AUDIT, the auditor should prepare the application with care. Steps normally followed include the following:

--Identify the specific computerized data that is available for analysis (usually done as part of data flow analysis discussed previously).

--Determine which package (DYL-260 or DYL-AUDIT) best meets audit needs.

--Determine the specific audit function to be performed.

--Decide which computer system will be used (the one being audited or another).

--Arrange for the proper cycle or version of the computer files to be copied (request that data be copied in the format which is easiest to process on the computer system to be used).

--Request the agency to provide the following information, along with copied files:

  ---Record layouts and data element definitions.

  ---Partial hexadecimal and graphic printouts or dumps of the data, including the header and trailer labels (used to verify that the information copied is in the correct format).

  ---Production listings of the program(s) used to copy the files (used to verify that the proper files were copied).

  ---Record counts of both the input and output files (used to verify that no data was added or lost).

--Verify record layouts by comparing with hexadecimal and graphic dumps of the data.

--Prepare a flowchart of procedures to be followed.

--Prepare logic flowcharts for all data retrieval programs.

--Prepare, in detail, all report or other output layouts.

--Prepare a plan to test programs to be used.

--Obtain technical review of design and testing plans from supervisor.

--Code specification sheets for each data retrieval program.

--Key and verify the specification sheets.

--Execute previously prepared test plan.

--Review and document test results for reasonableness and accuracy.

--Obtain technical review of test results from supervisor.

PROCESSING A DATA RETRIEVAL AND ANALYSIS APPLICATION

Normally, the auditor does not have to arrange for a separate standalone run of DYL-260 or DYL-AUDIT software. In a normal multiprogramming environment, the auditor should be able to run both DYL-260 and DYL-AUDIT with other programs, provided adequate computer resources are available. Steps followed in processing an application include the following:

--Process data retrieval programs on computer (observe and control processing of the data retrieval application if possible).

--Review processing results for reasonableness and accuracy.

--Update documentation to reflect actual processing (flowcharts should be annotated with actual job names, data set names and volume serial numbers, input/output counts, and output product titles).

--Obtain technical review of documentation and output products and document supervisor acceptance.

EVALUATING DATA RETRIEVAL AND ANALYSIS RESULTS

On completion of data retrieval processing and technical review, the auditor should analyze in detail the results of each data retrieval application. Each potentially erroneous condition should be traced back to the point of origin so that cause and effect can be identified. The total number or amount of errors can be determined by reprocessing corrected data by using either data retrieval programs prepared by the auditor or agency programs processed under the auditor's control.

SECTION XIII

JOB ACCOUNTING DATA ANALYSIS

Most computer manufacturers provide a job accounting function with their mainframe operating systems. This function accumulates information for use in billing users and evaluating system usage. It also produces data which can be used by auditors to evaluate controls in the data processing department. The auditor can access these job accounting records with the DYL-260 data retrieval and analysis package. Special purpose applications have been developed to produce reports from job accounting records that help the auditor. They help

- --verify controls over access to the computer system,
- --verify controls over access to system and application software,
- --verify controls over access to data sets and output products,
- --identify problems in processing computer programs,
- --identify problems with computer tapes, and
- --compare user billing/chargeout costs with actual system workload statistics.

These special purpose data retrieval and analysis applications are included in the GAO CAATS Manual.

TYPES OF JOB ACCOUNTING REPORTS

Numerous reports can be produced from job accounting data. Those which are of particular value in performing internal controls reviews are discussed in detail in the remainder of this section.

Verifying controls over access to the computer system

Two types of reports help the auditor verify controls over access to the system. They are

--job initiation and

--terminal activity.

The job initiation report identifies all persons who use the system. It specifies the job name, user identification, programmer's name, and computer usage information. The auditor can use this report to determine who accessed the system and then compare this list of actual users with a list of authorized users to determine if there have been any unauthorized accesses. In addition, the auditor should evaluate the list of authorized users to make sure they need access to the system.

The terminal activity report identifies all persons who had access to the system through a terminal. It specifies all log on and log off operations and all invalid log on attempts. The auditor can use this report to determine who accessed the system and who tried and was denied access and to verify that terminal log on and log off procedures are consistent with agency documentation. The auditor should compare the list of valid log ons and invalid log on attempts with a list of authorized users to determine if there have been unauthorized access or attempted accesses. In addition, the auditor should evaluate a list of authorized users to make sure they need access.

Verifying controls over access to system and application software

A software initiation report lists the persons who used each system or application software, in either a test or a

production mode. It specifies job name, user identification, programmer's name, computer usage information, and program name. The auditor can use this report to determine who has accessed the various system and application software. The auditor should compare this list of actual users with a list of authorized users to determine if there have been unauthorized uses of software. In addition, the auditor should evaluate the list of authorized users to make sure they need access. Also, when software is being switched from test to production mode, the auditor can use this report together with other program change control procedures to make sure they are being effectively exercised.

Verifying controls over access to data sets and output products

Three separate reports deal with access to data sets or output products:

--tape data set activity report,

--mass storage access activity report, and

--output products report.

The tape data set activity report lists the persons who accessed each data set. It also specifies whether the data set was created, read, updated, extended, rewritten, scratched, or renamed. In addition, the report specifies the job name; user identification; and data set information, such as data set names, volume serial numbers, etc. The auditor can use this report to determine who accessed each data set and why. The auditor should compare this list of actual users with a list of authorized users to determine if there have been unauthorized

uses of data sets. In addition, the auditor should evaluate the list of authorized users to make sure they need access.

The mass storage access activity report lists each person who accessed each mass storage data set or catalog. It also specifies whether the data set was created, read, updated, extended, rewritten, scratched, or renamed and whether a catalog entry was created, altered, or deleted. In addition, the report specifies the job name; user identification; mass storage data set information, such as data set names, volume serial numbers, etc.; and pertinent catalog information, such as name of catalog, volume serial number of catalog, etc. The auditor can use this report to determine who accessed each mass storage data set or catalog and why. The auditor should compare this list of actual users with a list of authorized users to determine if there have been unauthorized uses. In addition, the auditor should evaluate the list of authorized users to make sure they need access.

The output products report lists all creators of output products. Specifically, it lists job name, user identification if terminal entry, number of logical records written by the output writer, number of data sets completely written by the output writer, form numbers, and number of copies to be distributed. The auditor can use the report to determine who created the various system outputs. The auditor should compare this list of outputs with a list of authorized products to determine if unauthorized products or unauthorized copies have been produced. In addition, the auditor should evaluate the list

of authorized products to make sure that the products and the number of copies are actually needed by users.

Identifying problems in processing computer programs

An abnormal termination report identifies each computer program that terminated without reaching successful completion. It specifies program name, step name, job name, user identification, computer usage information, input/output errors, and abnormal termination type and code. The auditor can use this report to identify problems caused by computer program errors. This information can also be used to help identify potential problems with system design, development and modification procedures, data processing operations procedures, and computer hardware.

Identifying problems with computer tapes

A tape error report specifies the volume serial number, tape drive address, data block size, tape density, number of temporary read and write errors, permanent read and write errors, noise blocks, and erase gaps. The auditor can use this report to identify processing problems caused by tape errors to help identify computer tape and tape drive malfunctioning.

Comparing user billing/chargeout costs with actual system workload statistics

A workload statistics report provides details on system utilization. It specifies job name, user identification if terminal entry, job priority, job start date and time, job termination date and time, job elapsed time, central processing unit elapsed time, number of tape drives used, number of mass storage devices used, core requested, core used, number of data

blocks read and written, number of cards read, number of cards punched, and number of lines spooled or printed. The auditor can compare this report with agency user billing/chargeout reports to make sure that correct information is used in developing costs. The auditor can use a data retrieval and analysis package to recompute costs to make sure that proper cost alogrithms are employed to bill users.

PROCESSING JOB ACCOUNTING DATA

Operating procedures for using DYL-260 special purpose job accounting applications are included in the GAO CAATS Manual. The auditor should follow each step precisely and make sure that the proper cycle or version of the job accounting files is copied for analysis.

EVALUATION OF JOB ACCOUNTING DATA ANALYSIS

The auditor should analyze in detail each job accounting report. Any control weaknesses, processing weaknesses, or erroneous billing procedures should be pinpointed. Causes and effects of discrepancies should be identified. Auditors should be alert to the possibility that one person could use another's identification code. This security violation may not be obvious when evaluating job accounting data. Therefore, procedures for issuing and protecting user identification codes should also be reviewed in conjunction with this job accounting data analysis.

Reporting Phase

On the basis of the results of prior phases, the auditor has several alternatives available. Assuming that problems were disclosed, the auditor can either

--document the descrepancy and report on it or
--recommend that additional audit work be done.

Since reviews of internal controls in computer applications are extensive and cover many different subjects, each issue can be reported on separately or collectively in one single report. Further, during a review of internal controls, other issues may be identified (i.e., low computer utilization, poor personnel practices, etc.) which warrant additional review.

SECTION XIV

REPORTING AND RECOMMENDATIONS FOR ADDITIONAL AUDIT WORK

Numerous issues can be fully developed into findings, conclusions, and recommendations as part of a review of the internal controls in a computer-based system. Some of the issues may be significant enough to be addressed separately in a single report. Other issues are best combined and addressed collectively in one report. The severity of the problem and the significance of the issue must be weighed in deciding how the issue should be reported.

There may be other issues identified during the review which will require additional audit work before a report can be prepared.

REPORTABLE ISSUES

Three major categories of internal controls have been discussed in this audit guide:

--Management.

--General.

--Application.

Each can very easily be addressed separately in a single report. In fact, reports can be issued on each control point within these categories. For example, under management controls, problems with internal audit can be reported on separately; under general controls, problems with the system development life cycle can be reported on separately; under application controls, problems with error handling can be reported on separately; and so on. Just as easily, however, each major category can be addressed as a major section of one single report.

In addition, some of the compliance tests can provide enough in the way of supportable findings, conclusions, and recommendations to warrant issuance of separate reports. For example, when performing

--user satisfaction analysis, the auditor may find major problems with a single output product which should be reported on separately;

--data retrieval and analysis, the auditor may disclose serious problems, such as the lack of an interface with another computer system, which should be reported separately; and

--job accounting data analysis, the auditor may determine that the user billing/chargeout procedures are incorrect, which cause erroneous bills to be sent to system users, and decide that a separate report is warranted.

Each situation must be evaluated separately.

RECOMMENDATIONS FOR ADDITIONAL AUDIT WORK

Certain issues discussed in this audit guide may require additional work to support findings, conclusions, and recommendations. Except for ADP planning as discussed under the management controls area, these issues fall mainly within the general controls area. They deal with such issues as

--personnel policies,

--malfunction reporting and preventive maintenance,

--user billing/chargeout procedures,

--disaster recovery,

--system software controls, and

--hardware controls.

If enough audit work has not been done during the internal controls review to support findings, conclusions, and recommendations about the above issues, the audit staff may recommend a separate review to focus on the issue(s) raised.

BIBLIOGRAPHY

American Federation of Information Processing Societies, Inc. Security System Review Manual. Arlington, VA.: AFIPS Press, 1974.

American Institute of Certified Public Accountants. Audits of Service-Center-Produced Records. New York: AICPA, 1974.

----------. Computer Assisted Audit Techniques. New York: AICPA, 1979.

----------. Controls Over Using and Changing Computer Programs. New York: AICPA, 1979.

----------. Guidelines for General Systems Specifications for a Computer System. New York: AICPA, 1976.

----------. Management, Control and Audit of Advanced EDP Systems. New York: AICPA, 1977.

----------. Report of the Special Committee on Equity Funding. New York: AICPA, 1975.

----------. Statements on Auditing Standards, No. 3, "The Effects of EDP on the Auditor's Study and Evaluation of Internal Controls." New York: AICPA, 1974.

----------. The Auditor's Study and Evaluation of Internal Control in EDP Systems. New York: AICPA, 1977.

American National Standard Institute Inc. American National Dictionary for Information Processing. Washington, D.C.: Computer and Business Equipment Manufacturers Association, 1977.

----------. American National Standards Flowchart Symbols and Their Usage in Information Processing, New York: American National Standards Institute, 1970.

Arkin, Herbert, Handbook on Sampling for Auditing and Accounting. New York: McGraw Hill, 1974.

Burch, John G. and Joseph L. Sardinas. Computer Control and Audit: A Total Systems Approach. Santa Barbara, CA.: John Wiley and Sons, 1978.

Burch, John G., Felix R. Strater Jr. and Gary Grudnitski, Information Systems: Theory and Practice. New York: John Wiley and Sons, 1979.

Canadian Institute of Chartered Accountants, Computer Audit Guidelines. Toronto: CICA, 1975.

----------. Computer Control Guidelines. Toronto: CICA, 1970.

Cougar, J. Daniel and Fred R. McFadden. Introduction to Computer Based Information Systems. New York: John Wiley and Sons, 1975.

Davis, Gordon B.. Auditing and EDP. New York: AICPA, 1968.

----------. Computer Data Processing. New York: McGraw Hill, 1973.

----------. Computers and Information Processing. New York: McGraw Hill, 1978.

----------. Introduction to Computers. New York: McGraw Hill, 1977.

EDP Auditors Foundation. Control Objectives. Altamonte Springs, Fla.: EDPAF, 1980.

Faim Technical Library. Auditing Computer Systems. Melville, NY: Faim Technical Library, 1980.

Fitzgerald, Jerry. Internal Controls for Computerized Systems. San Leandro, CA.: E. M. Underwood, 1978.

Intitute of Internal Auditors. How To Acquire and Use Generalized Audit Software. Altamonte Springs, Fla.: IIA, 1979.

----------. Systems Auditability and Control, Audit Practices. Altamonte Springs, Fla.: IIA, 1977.

----------. Systems Auditability and Control, Control Practices. Altamonte Springs, Fla.: IIA, 1977.

Jancura, Elise. Audit and Control of Computer Systems. New York: Petrocelli Books, 1976.

Lainhart, John and Barry Snyder. "A Simultaneous-Parallel Approach to Testing Computerized Systems." GAO Review. U.S. General Accounting Office, Summer 1977.

Mair, William, Donald Wood and Keagle Davis. Computer Control and Audit. Altamonte Springs, Fla.: IIA, 1976.

Martin, James. Future Developments in Telecommunications. Englewood Cliffs, N.J.: Prentice-Hall, 1971.

----------. Introduction to Teleprocessing. Englewood Cliffs, N.J.: Prentice-Hall, 1972.

----------. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, N.J.: Prentice-Hall, 1973.

----------. Systems Analysis for Data Transmission. Englewood Cliffs, N.J.: Prentice-Hall, 1972.

----------. Telecommunications and the Computer. Englewood Cliffs, N.J.: Prentice-Hall, 1972.

Roberts, Donald M.. Statistical Auditing. New York: AICPA, 1978.

U.S. Department of Commerce, National Bureau of Standards. Audit and Evaluation of Computer Security. Special Publication, 500-19, 1977.

----------. Audit and Evaluation of Computer Security II, Special Publication, 500-57, 1980.

----------. Computer Security Guidelines for Implementing the Privacy Security and Risk Management. FIPS Publication 41, 1975.

----------. Guidelines for Automated Data Processing Physical Security and Risk Management. FIPS Publication 31, 1974.

----------. Guidelines for Automatic Data Processing Risk Analysis. FIPS Publication 65, 1979.

----------. Guidelines for Documentation of Computer Programs and Automated Data Systems. FIPS Publication 38, 1976.

----------. Guidelines for Documentation of Computer Programs in Automated Data Systems for the Initiation Phase. FIPS Publication 64, 1979.

----------. Performance Assurance and Data Integrity Practices. Special Publication 500-24, 1978.

National EDP Auditing Committee of the IIA. Hatching the EDP Audit Function. Altamonte Springs, Fla.: IIA, 1975.

Perry, William E. and Thomas W. Porter. EDP Controls and Auditing. 2d ed., Belmont, Calif.: Wadsworth Publishing Co., 1977.

----------. Selecting EDP Audit Areas. Altamonte Springs, Fla.: EDPAF, 1980.

U.S. General Accounting Office, Guidelines for Accounting for Automatic Data Processing Costs. Federal Government Accounting Pamphlet Number 4, 1978.

U.S. General Accounting Office, Standards for Audits of Governmental Organizations, Programs, Activities, and Functions. Revised 1981.

ASSESSING RISK

Two primary criteria should be used to determine the degree of potential risk associated with computer-processed data: Is a control in place, and is it effective? The following tables show possible risk levels that could be assigned to system controls.

DETERMINING RISK LEVELS

Control characteristic	Is the control in place?	Is the control effective?	Is some alternate control in places?	Is the alternate control effective?	Level of potential risk
Security and access	Yes	Yes	No	-	Low
	No	-	Yes	Yes	Medium
	Yes	No	Yes	Yes	Medium
	Yes	No	No	-	High
	No	-	Yes	No	High
	No	-	No	-	High
	Yes	No	Yes	No	High

POSSIBLE EFFECT ON AUDIT WORK

Level of potential risk	Possible Effects
Low	Unlikely that more audit tests are required.
Medium	Likely that more audit tests are needed unless another information source can be used or the auditor is satisfied that the risk is acceptable. Recommendations for corrective action(s) may be possible.
High	Need for additional audit tests is a virtual certainty unless another information source can be used or the auditor is satisfied that the risk is acceptable. Recommendations for corrective action(s) should be made.

* U. S. GOVERNMENT PRINTING OFFICE : 1981 720-023/ 4845