

29701

COVER SUMMARY

AUDIT GUIDES TO REVIEW IMPLEMENTATION
OF THE FEDERAL MANAGERS' FINANCIAL
INTEGRITY ACT: THE SECOND YEAR



The Federal Managers' Financial Integrity Act imposes an important responsibility on all Government officials to strengthen internal controls. GAO's audit guides provide for a comprehensive assessment of agencies' progress in implementing the act and improving their internal control and accounting systems.

030475 / 125524

GAO/AFMD-84-77
AUGUST 21, 1984

29701

COVER SUMMARY

AUDIT GUIDES TO REVIEW IMPLEMENTATION
OF THE FEDERAL MANAGERS' FINANCIAL
INTEGRITY ACT: THE SECOND YEAR

The Federal Managers' Financial Integrity Act imposes an important responsibility on all Government officials to strengthen internal controls. GAO's audit guides provide for a comprehensive assessment of agencies' progress in implementing the act and improving their internal control and accounting systems.

030475 / 125524

GAO/AFMD-84-77
AUGUST 21, 1984

PREFACE

In passing the Federal Managers' Financial Integrity Act of 1982, Congress focused attention on the need to strengthen internal controls. The 1982 act requires agencies to periodically evaluate internal control systems and the heads of executive agencies to report annually on their systems' status. The act presents an opportunity for a cooperative effort among OMB, GAO, and the agencies to improve internal controls throughout the Government.

GAO's audit guidelines are prepared for its internal use and, as a general practice, are not made available for external distribution. In this instance, limited distribution of appropriate sections of the guidelines is being made to OMB and the Inspectors General, to apprise them of the key areas on which GAO will focus and which it believes need to be stressed to achieve compliance with the Federal Managers' Financial Integrity Act. Any wider distribution of the guides should be made only upon approval by GAO (Director, Accounting and Financial Management Division).

We would appreciate any comments or suggestions OMB or the Inspectors General may have concerning the audit guides. Any inquiries concerning the audit guides should be directed to Mr. Jeffrey C. Steinhoff, Deputy Associate Director (telephone 275-9484).

CONTENTS

	<u>Page</u>
Introduction	1
PART A - FIA Section 2 Guidelines	2
Objectives	3
Section I - Agency Progress in Implementing the FIA	5
Section II - ADP Work Program for Second Year FIA	18
Section III - Progress and Problems in Improving Internal Control Systems	41
Section IV - Assessment of the Reasonableness of the Agency's Second Annual Assurance Letter	49
PART B - Guidelines for Performing FIA Section 4 Audit Work	51
Objectives	51
Section I - Agencies' Progress	54
Section II - Evaluating Corrective Actions Planned and Completed	69
Section III - Agencies' Annual Statement	73
APPENDIX I - Requirements to be Considered	76
Attachments A and B - Summary of ADP Internal Controls	77

INTRODUCTION

The audit guidelines consist of two parts: Part A addresses the work related to Section 2 of the act and Part B addresses the work related to Section 4 of the act.

The GAO program divisions have overall responsibility for the reports on their agencies. Program divisions will perform work relating to the agencies' evaluation of internal controls (Part A of the guidelines).

The Information Management and Technology Division (IMTEC) has responsibility to support the program divisions with audit work and technical consultation in the ADP area. The general, IMTEC will perform all work relating to ADP general controls and some application controls. The program divisions will perform, with IMTEC's technical consultation, all work relating to non-technical ADP application controls using IMTEC furnished guidelines. (See Part A, Section II, page 19.) Close cooperation and coordination is mandatory to ensure the ADP work is effectively and efficiently accomplished.

Accounting systems work will be accomplished by AFMD staff using guidelines developed by them (Part B of the guidelines). Consequently, program division team leaders will incorporate the accounting systems work into their agency reports.

PART A

FIA SECTION 2 GUIDELINES

The Section 2 guidelines were developed under the assumption that audit work would be undertaken by most of the same staffs and at the same departments and agencies we reported on during our first year review of the Federal Managers' Financial Integrity Act (FIA). As a result, we assumed staffs have an understanding of FIA and we did not provide indepth background data or extensive explanations of audit steps. Staff members not participating in the first year review of FIA will need to review the first year agency report and supporting summaries. A number of additional background steps will need to be conducted in agencies we did not review during the first year. The audit team for these agencies should refer to the first year guidelines as needed.

As a result of experience gained during the first year, we have revised our basic audit approach and reporting requirements. These guidelines do not identify all audit steps needed to complete our work--instead the guidelines include the minimum requirement necessary to provide a basic understanding of each agency's FIA process and progress in improving its evaluation of its systems of internal controls. These guidelines will also provide basic data on the agencies' progress toward correcting its internal control weaknesses. Each audit staff should supplement these guidelines with additional audit steps for data needed in preparing their agency report where necessary.

OBJECTIVES

The major objectives of our review are to:

- update and evaluate progress made by the agencies in implementing their processes for evaluating systems of internal control;
- determine whether, through corrective actions, the agencies are improving their systems of internal control; and
- assess the reasonableness of the agencies' second annual assurance letters.

Audit steps in Sections A-I and A-II require audit teams to update the work at agencies, document any changes which have occurred, and review the implementation of the FIA process. This information will be used to assess the reasonableness of the assurance letter. The guidelines require audit teams to closely coordinate with GAO program division personnel (Associate Director, Group Director, and experienced staffs at audit sites) to ensure we utilize GAO's historical and indepth knowledge of the agencies.

In section A-III, we will be reviewing corrective action plans for material weaknesses identified in the annual assurance letters. We will also analyze corrective actions for internal control weaknesses identified in VAs and ICRs. We will collect any available FIA cost and benefit data that the agencies have compiled.

In section A-IV of the guidelines, we will assess the reasonableness of the agencies' second annual assurance letters. While our work may not be extensive enough to verify that the agency's letter reflects the actual condition of all of its internal

controls, we should have sufficient information to support or challenge certain statements in the agency's assurance letter.

Teams should recognize that these four sections of the audit guide are not mutually exclusive. As such, there will be many occasions when work from one section would logically be performed concurrently with work from another section. This is particularly true of sections A-I and A-II. Teams should carefully read all work steps and determine where work can be done simultaneously to prevent duplicate interviewing of agency officials and other review work.

Teams should also coordinate closely with their agency IG very early in the job. Several work steps involve discussions with IG personnel. It may also be possible to supplement our selection of VAs and ICRs with work performed by the IG if they performed comparable reviews. Teams should explore this possibility before selecting VAs and ICRs.

SECTION A-I
AGENCY PROGRESS IN
IMPLEMENTING THE FIA

The objective of this section is to evaluate each agency's process for evaluating its systems of internal control. In this section, we will update our data base on the agency's procedures and (1) determine whether the segmentation process covered all of the agency's programs, functions, and activities; (2) review some vulnerability assessments and internal control reviews; (3) determine whether the tracking and follow-up system is operating; and (4) evaluate the adequacy of the internal reporting system to ensure that internal control weaknesses are being reported to the proper organization or offices.

The work steps for ADP Have been broken out as a separate section (section A-II). However, some steps parallel the work steps in this section and should be done at the same time.

Before starting work in the second year, teams should fully coordinate with the agency IG. We should obtain and discuss any FIA reports issued by the IG, obtain their views on the agency's implementation, and discuss our work so that duplication of effort can be reduced or eliminated. We will be selecting a limited number of VAs and ICRs to review. If the IG is also reviewing VAs and ICRs, we should be sure not to duplicate their work and arrange to use their results to supplement ours if appropriate.

A. Our first year effort in reviewing agency implementation of FIA revealed many weaknesses and omissions in their procedures. Our objective is to evaluate those procedures in terms of the changes and improvements which have occurred. We need to document what the current procedures are, how they have changed or improved since our previous review effort, and what improvements are still needed to assure the agency complies with OMB guidance and establishes an effective means of implementing the FIA.

1. Organizing to Implement the FIA

- a. Determine agency's current organization to implement FIA. (Note all changes from the first year.)
 - (1) Assignment of overall responsibility
 - (2) Inspector General's role
 - (3) Performance appraisals
 - (4) Resources/staffing
 - (5) Training
 - (6) Quality assurance
 - (7) How has top management shown its commitment?
- b. How were organizational problems identified by GAO or others in the first year resolved?
- c. Does the agency's current organization for FIA comply with OMB guidelines? If not, describe.

2. Segmenting

- a. Determine the agency's current segmenting process.
- b. How were segmenting problems identified by GAO or others in the first year resolved?
- c. Obtain the current inventory of assessable units. How many are there?

3. Vulnerability Assessments

- a. Have problems with the written guidelines for VAs identified in the first year been resolved? Are there any new problems?
- b. Does the current agency vulnerability assessment process comply with OMB guidelines? If not, describe.
- c. If agency performed VAs in 1984, obtain a list.
 - (1) Were all identified units assessed?
 - (2) Were any omitted? If so, describe.
 - (3) How many were ranked low, moderate or high?
- d. Is the agency meeting its milestones for performing VAs? If not, why?

4. Alternatives to ICRs (for 1983 and 1984 VAs)

- a. OMB guidelines allow an agency to select from several alternatives after conducting its VAs. (See page IV-13 of OMB guidelines).

- (1) If the agency chose alternatives to ICRs, describe the criteria and procedures developed for choosing an alternative.

5. Internal Control Reviews

- a. Have problems with the agency ICR guidelines identified in the first year been resolved? Are there any new problems?
- b. Does the current ICR process comply with OMB guidelines? If not, describe.
- c. How did the agency select which assessable units would have an ICR? Does their selection methodology make sense?
- d. Has the agency followed its plan for performing ICRs?
 - (1) How many were completed in 1983?
 - (2) How many do they plan to complete in 1984?
 - (3) Is the agency on schedule? Why not?

6. Tracking and Follow-up System

- a. Obtain guidelines for agency's tracking and follow-up system for:
 - (1) scheduling performance of VAs and ICRs;
 - (2) recording and reporting results of VAs and ICRs;

(3) scheduling and tracking corrective actions on weaknesses identified in VAs and ICRs; and

(4) summarizing and reporting the overall results of VAs, ICRS, and corrective actions.

b. Have the tracking and follow-up procedural problems identified in the first year been resolved?

c. Many agencies did not implement a tracking system in their first year effort. Have they now implemented a tracking and follow-up system?

d. Does the agency's system comply with OMB guidelines? If not, describe.

e. Does the system include a means to evaluate the effectiveness of the corrective action?

7. Annual assurance letter

a. Determine the process that the agency plans to use to generate the 1984 assurance letter.

b. Have problems identified in the first year been resolved?

B. Did the segmentation process/inventory of assessable units cover the entire agency? List any omissions and quantify (dollars in budget, number of personnel, etc.). Does the size of the assessable units seem reasonable for your agency?

C. Review vulnerability assessments done during 1984. In this section, we will only review VAs done with updated agency guidance which incorporates changes as a result of GAO, OMB, and IG work.

1. Select a number of vulnerability assessments and evaluate them as discussed below. The number should be sized according to your team's time and resource constraints. Since we are most interested in identifying low or moderate areas that should have been rated high, teams should stratify their selection to include 20 percent high, 40 percent medium and 40 percent low. In addition, since ADP controls are important and need to be considered in conducting the VAs, teams should ensure that a majority of the VAs selected for review are in functions or programs that also have some ADP involvement.

The selection should be based on known problem areas. For example, instead of selecting from the agency's list of assessable units without regard to why they were vulnerable, the selection should be based on discussions with GAO and IG staff that are doing on-going work in the agency so that we can match problem areas with assessable units where possible. Selecting areas with current findings will provide the auditor with specific weaknesses and/or problem areas to take

to the person responsible for the vulnerability assessment and determine how these were considered.

We recognize that this selection approach may not be workable in your agency. In that case, you should devise a selection method that fits the intent of these guidelines and your agency.

2. Review available documents and interview personnel that conducted the VA. The entire VA process should be reviewed. The following should be specifically addressed. (For VAs involving ADP application controls, also perform steps in section A-II, p.22.)

- a. Were agency and OMB guidelines followed? Discuss differences.
- b. Did the person conducting the VA use data from audit reports and other known reports?
- c. Is there any evidence (prior audit reports, findings from current audits, and agency studies) that was not considered? Could the evidence change the conclusion?
- d. How did the agency consider the GAO internal control standards when performing the vulnerability assessments?
- e. Were the vulnerability assessments adequately documented? In our

first-year report to the Congress we discussed how much documentation is enough and stated "one useful rule of thumb is that the amount and depth of documentation should be sufficient that managers and supervisors reviewing an evaluation would have a reasonable basis for determining how the conclusion was reached".

- f. Did the person performing the vulnerability assessment feel that he/she had adequate training? Why or why not? Does the quality of the vulnerability assessment documentation support that individual's opinion that he/she received adequate training?
 - g. Ask GAO program audit group personnel (associate and group directors and experienced staff) and agency IG personnel whether they feel, based on their institutional knowledge, and current audit work, that the VA conclusion was reasonable.
 - h. Is the VA's conclusion reasonable and supported by the evidence?
3. Many agency IGs are reviewing the validity of VAs. Use their audit results if applicable.

4. Reach a conclusion on the overall reasonableness of the VAs examined.
- D. If an agency has taken an action other than an ICR:
1. Why did the agency choose an alternative to an ICR?
 2. Did the agency follow its established procedures for choosing an alternative?
 3. Is the alternative chosen reasonable, given the results of the VA?
- E. Review a limited number of internal control reviews done in 1984. In this section, we will only review ICRs done with updated agency guidance which incorporates changes as a result of GAO, OMB, and IG recommendations made during the first year.
1. Select a number of ICRs conducted in 1984. The selection should be sized according to the team's time and resource constraints. The following factors should be considered in making the selection:
 - a. ICRs from varying locations should be included.
 - b. ICRs that identified significant problem areas that may be in the agency's annual assurance letter should be included.
 - c. ICRs that involve known problem areas identified by GAO or IG personnel should be included. Findings from current on-going work should be used to select

ICRs for review. The intent is to see if the ICR is identifying current problems.

- d. ICRs that are in functions or programs that have some ADP involvement should be included.

(These four factors are not mutually exclusive. Many ICRs will have some, if not all, of the attributes.)

- e. About 30 percent of the ICRs selected should be in areas that do not have known problems.

- 2. Review available documents and interview the personnel that conducted the ICR. The entire ICR process should be evaluated. The following should be specifically addressed. (For ICRs involving ADP application controls, also perform steps in section A-II, p.25.)

- a. Were agency and OMB guidelines followed? Discuss differences.
- b. Were the results of the VA used in the ICR? If not, why not?
- c. Was the ICR supported by reasonable testing of control techniques?
- d. How did the agency consider the GAO internal control standards when conducting the ICR?
- e. Did the ICR identify the problems found in current audit work (where applicable)?

- f. Was the ICR adequately documented? (Use the same criteria used in C. 2. e. above).
 - g. Does the person conducting the ICR feel he/she had adequate training? Why or why not? Does the quality of the documentation support an opinion of adequate training?
 - h. Discuss the ICR results with GAO program groups and IG personnel. Obtain their opinions on whether all known problems or weaknesses were identified (prior audits and current work).
 - i. Is the ICR result reasonable and supported by available evidence?
- 3. Many IGs are reviewing ICRs done in their agency. Use their results to supplement your analysis of ICRs if appropriate.
- 4. Reach a conclusion on the overall reasonableness of the ICRs examined.
- F. How did the agency's responsible FIA program official assure himself/herself that VAs and ICRs were adequately accomplished (quality assurance)? This step should be performed at each organizational level within the agency.
- G. This step concentrates on the agency's tracking and follow-up procedures. Additional work steps concerning implementation of corrective actions are in section A-III.

1. Are the internal control weaknesses identified in first and second year VAs and ICRs being put into the agency's tracking and follow-up system? This includes making sure all weaknesses are properly entered into the system from

--annual reports,

--feeder reports,

--ICRs, and

--VAs.

Because the agencies' follow-up and tracking systems are different, (centralized vs decentralized, and automated vs manual), each audit team should determine how best to ensure that the agency is entering all weaknesses identified from VA's and ICR's into the system.

Select at least 50 percent from first year. To the extent possible, our work should also include selected field locations if they enter weaknesses into a tracking and follow-up system.

2. Determine whether the agency is on schedule for correcting the weaknesses identified in step G.1. above. If the agency is not on schedule, why not?
3. How do the agency FIA officials assure themselves that all internal control weaknesses are put into a tracking and follow-up system and are systematically followed up?
4. Does the agency's internal reporting system, as it is actually operating, meet the following objectives?

- a. Weaknesses should be reported to a level that can assure corrective actions are developed and implemented.
- b. Weaknesses should be reported to a level that has agency-wide or function-wide oversight so that systemic problems are identified and resolved.
- c. The reporting system should support the agency's annual assurance letter.

Agencies' internal control reporting systems vary to such a degree that we cannot specify the work steps necessary to accomplish this section. We suggest, however, that as a minimum teams interview agency officials responsible for collecting FIA data and review agency FIA feeder reports to determine whether the objectives are being met.

- 5. Reach a conclusion on the overall adequacy of the agency's tracking and follow-up system.
- H. Some agencies annual assurance letter may be based on assurances from appropriate officials and other information provided as well as the OMB evaluation process. Under these circumstances, the team should determine what the "other information" is and why it was used in addition to the OMB evaluation process.

SECTION A-II
ADP WORK PROGRAM FOR
SECOND YEAR FIA

The second year ADP audit effort will also entail assessing the progress agencies are making toward increasing the consideration of ADP controls during the evaluation process. GAO will not do any original work, i.e., assess agency's internal controls, but we should determine whether the program or functional managers adequately assessed controls during their evaluations. In conjunction with the divisional audit team, an IMTEC auditor should gather sufficient data to determine the extent to which agencies considered ADP general and application controls during the process.

While ADP general controls usually are pervasive, i.e., affect all ADP applications, ADP application controls are unique to specific tasks, e.g., payroll, inventory, supply etc. Since a heavy concentration of general controls is in the data processing organization, data processing management is ultimately responsible for their existence and effectiveness. On the other hand, the program or functional manager is responsible for ensuring that application controls are properly working within the automated systems supporting his program or function. Both types of controls consist of manual (non-technical) and automated control techniques designed to provide reasonable assurance that predefined control objectives are met.

Specifically, IMTEC will be responsible for assessing the agencies' evaluation of ADP general controls, while the divisional audit teams will be responsible for assessing the non-technical application controls from the program or functional manager (user)

perspective. IMTEC will also be responsible for assessing the more technical application controls and providing overall technical consultation to the divisional audit team.

Criteria for what would constitute valid ADP general and application control objectives and techniques can be found in:

- Information System Review - Audit Guide - "Summary of ADP Internal Controls"--General Control Evaluation (Attachment A) and Application Control Evaluation (Attachment B), (GAO/IMTEC)
- Evaluating Internal Controls in Computer-Based Systems (GAO Black Book), and
- Guide for Studying and Evaluating Internal Controls in the Federal Government, (Arthur Anderson & Co.).

A. CURRENT STATUS OF THE AGENCY'S PROCESS

TO COMPLY WITH FIA

Objective: Update the agency's FIA process relating to the degree of consideration given to ADP controls. We should document the current process identifying any significant changes and improvements. The audit steps in this section are designed to update last year's efforts by documenting the agency's current process.

The following audit steps should be supplemented according to the situation at the individual agency:

1. Organizing to implement FIA

Objective: Determine whether the agency's organization to comply with the Act provides for considering ADP controls.

Tasks:

a. Describe how the agency's current organization to implement FIA provides for considering ADP controls.

- (1) ADP management involvement in the FIA implementation process.
- (2) Coordination of the work required under OMB Circular A-71 and A-123 in order to avoid duplication posed by each circular on the other.
- (3) Assignment of responsibility for reviewing ADP general and application controls.
- (4) Role of the ADP audit personnel from the IG office or other audit group.
- (5) Training given to program and functional managers on assessing ADP controls.
- (6) Quality assurance measures taken by the agency related to ADP controls.

2. Segmenting

Objective: Determine whether the segmentation of the agency includes all ADP activities.

Tasks:

- a. Describe the agency's treatment of ADP activities in its current segmenting process.
- b. Identify the first year segmenting problems and determine the agency status on resolving them.
- c. Obtain from the divisional team the agency's inventory of assessable units.
- d. Based on a review of the inventory and discussion with ADP management, identify assessable units addressing ADP management and operational components. In addition, identify other assessable units supported by automated applications.
- e. Document ADP activities omitted and provide potential effects (sensitive data, dollars, etc.).

3. Vulnerability Assessments

Objective: Determine if the agency's guidelines for performing vulnerability assessments provide for the consideration of ADP control objectives and techniques.

Tasks:

- a. Review the agency's current vulnerability assessment guidelines to determine if they provide for considering ADP control objectives and techniques.
- b. Have problems with the guidelines identified in the first year been resolved? Are there any new problems?

4. Internal Control Reviews

Objective: Determine if agency's guidelines provide for the consideration of ADP controls during internal control review or substituted alternatives; e.g., management studies and reviews, etc.

Tasks:

- a. Review the agency's current guidelines for performing internal control reviews to determine if they provide for identifying, documenting, and evaluating control objectives and control techniques.
- b. Have problems with the guidelines identified in the first year been resolved? Are there any new problems?

B. ASSESSMENT OF THE AGENCY'S

CONSIDERATION OF ADP CONTROLS

Objective: Determine whether the agency considered general and application control objectives and techniques during the agency's implementation of the process. We should determine whether the scope of the agency's vulnerability assessments and internal control reviews, where applicable, provided for the consideration of ADP control objectives and techniques. We should review supporting documentation and interview responsible managers to determine the criteria and methodology they used to assess ADP controls. IMTEC and the divisional audit team have joint responsibility for completing this section.

1. Review Vulnerability Assessments--Adequate consideration of ADP controls

Objective: Determine whether managers, when conducting vulnerability assessments, adequately (a) reviewed policies/procedures (e.g., SOP(s) and users manual) pertaining to control objectives and techniques, (b) identified control objectives and key control techniques and determined the reasonableness of control techniques to meet

objectives, (c) identified any independent reviews of the program or function by audit, quality assurance review, or other studies, and (d) documented known control problems.

IMTEC will be responsible for reviewing the vulnerability assessment and discussing with the managers the consideration given to the ADP general control objectives and techniques. IMTEC will follow, where applicable, the tasks in Section I-C in addition to the tasks in this section. Divisional audit teams will be primarily responsible for evaluating the consideration given by the program and functional managers (users) to application control objectives and techniques. However, IMTEC will be responsible for evaluating the consideration given to the more technical application control techniques (e.g., edits, validating, etc.). Close coordination between the audit team and IMTEC is required to ensure an adequate assessment of the managers consideration of ADP controls.

Tasks:

- a. Assist divisional audit team in selecting vulnerability assessments for review to ensure that programs supported by ADP applications are included. Also, with the audit team approval, select some vulnerability assessments of ADP functional areas to assess the manager's consideration of ADP general control objectives and techniques.
- b. Vulnerability Assessment (General Controls). IMTEC auditor should review available documents and interview personnel that conducted the vulnerability assessments:

1. Determine whether the manager, when conducting vulnerability assessments, identified proper control objectives and key control techniques for the following ADP general controls. Refer to Section II-B-3a, Summary of ADP Internal Controls - General Control Evaluation, page 27.

c. Vulnerability Assessment (Application Controls).

Divisional auditor, in conjunction with IMTEC auditor, should review available documents and interview personnel that conducted the vulnerability assessments:

1. Determine whether the manager when conducting vulnerability assessments identified proper control objectives and key control techniques for the following ADP application controls. Refer to Section II-B-3b, Summary of ADP Internal Controls - Application Control Evaluation, page 33.

d. Determine whether the manager evaluated how effectively the policies/procedures pertaining to each objective and technique are documented and communicated to personnel.

e. Did the manager determine whether the program or function area was subject to a recent independent review (e.g., audit, quality assurance function, or study)? How significant and recurring are any weaknesses?

f. Did the manager consider known control problems and their significance?

2. Review Internal Control Reviews or Their Substitutes--
Adequate consideration of ADP controls.

Objective: Determine whether managers, when conducting internal control reviews, adequately (1) identified and documented control objectives and techniques, (2) evaluated whether the control techniques meet the control objectives, (3) conducted compliance tests of key control techniques being utilized to meet control objectives, and, (4) summarized the results and identified corrective actions necessary.

IMTEC will be responsible for evaluating the consideration of general control objectives and techniques identified by data processing management during their internal control reviews. IMTEC will follow the guidelines in Section I-E-2 in addition to tasks in this section. Divisional audit teams will be primarily responsible for evaluating the consideration given by program managers (users) to application control objectives and techniques. However, IMTEC will be responsible for evaluating the consideration of the more technical application control techniques (e.g., edits, validating, etc.). Close coordination between the audit team and IMTEC is required to ensure an adequate assessment of managers consideration of ADP controls.

Tasks:

- a. Assist divisional audit team in selecting a number of internal control reviews (ICRs) in order to assure that some programs and functions which are supported by

application systems (application controls) are included. Also, in coordination with the audit team, select a number of ICRS addressing ADP management and operational areas.

b. Internal Control Review (General Controls) - IMTEC auditor should review available documents and interview personnel that conducted the internal control reviews:

1. Determine whether control objectives and proper control technique(s) were identified, documented, and evaluated by the agency's functional and program managers for ADP general control areas. Refer to Section II-B-3a, Summary of ADP Internal Controls - General Control Evaluation.

c. Internal Control Review (Application Controls) - Divisional auditor, in conjunction with IMTEC auditor, should review available documents and interview personnel that conducted the internal control reviews:

1. Determine whether control objectives and proper control technique(s) were identified, documented, and evaluated by the agency's functional and program managers for ADP application control areas. Refer to Section II-B-3b for ADP Application Control Objectives.

d. Was the ICR supported by reasonable testing of control techniques?

e. Was the ICR summarized and reasonable corrective actions initiated or planned?

3. Summary of ADP General and Application Controls

Objective: GAO's internal control standards require the identification of control objectives that should be achieved in each area of an agency's activities. We have identified the control objectives that should be achieved in an agency's ADP activities and documented them in the "Summary of ADP Internal Controls"--General Controls Evaluation (Attachment A), and Application Control Evaluation (Attachment B). These control objectives provide specific guidelines against which the auditor can compare the agency's evaluation of general and application control objectives and techniques. The auditor should assess the agency's evaluation of each control technique to determine whether it is achieving a specific control objective.

a. Summary of ADP Internal Controls - ADP General Control Evaluation. (Responsibility: IMTEC)

1. Internal Audit:

Control Objective(s)

(a) Inspector General Audit of ADP - The Office of Inspector General should substantiate and evaluate ADP activities and controls. For examples of applicable control techniques, refer to Attachment A, p. III-55.

2. Organization and Management of the ADP

Department:

Control Objectives(s)

(a) Definition and Communication of Responsibilities - The ADP department's

organizational structure, policies, and procedures should be clearly defined and communicated to provide reasonable assurance that ADP personnel perform correctly the duties they have been assigned. For examples of applicable control techniques refer to Attachment A, p. III-57.

(b) Separation of Responsibility - Key duties and responsibilities within the ADP department should be adequately separated to reduce the risk of errors, waste, or wrongful acts. For examples of applicable control techniques, refer to Attachment A, p. III-59.

(c) Supervision - ADP personnel should be properly supervised to ensure that delegated duties are performed in accordance with appropriate policies and procedures. For examples of applicable control techniques, refer to Attachment A, p. III-61.

(d) Competent Personnel - ADP personnel should maintain and demonstrate personal and professional integrity and a level of skill necessary to accomplish the assigned duties. For examples of applicable control techniques, refer to Attachment A, p. III-63.

3. System Design, Development, and Maintenance

Control Objective(s)

(a) System Acceptance - A formal system acceptance process should have been followed to provide reasonable assurance that the system was properly designed, developed, and tested before implementation. For examples of applicable control techniques, refer to Attachment A, p. III-65.

(b) System Maintenance - All application program system changes should be authorized and approved by appropriate user and ADP management personnel. For examples of applicable control techniques, refer to Attachment A, p. III-67.

(c) Testing and Conversion - New and modified systems should be properly tested and implemented/converted. For examples of applicable control techniques, refer to Attachment A, p. III-69.

(d) Documentation - New systems and program/system changes should be completely documented. For examples of applicable control techniques, refer to Attachment A, p. III-71.

4. Systems Hardware

Control Objective(s)

(a) Integrated Hardware - Integrated hardware controls should be used to maximize the potential for detecting errors during processing. For examples of applicable control techniques, refer to Attachment A, p. III-73.

5. Systems Software

Control Objective(s)

(a) Selection and Installation of Systems Software - Systematic procedures should be followed to identify, select, and install system software. For examples of applicable control techniques, refer to Attachment A, p. III-75.

(b) Systems Software Maintenance - System software changes should be properly documented, tested, and approved before implementation. For examples of applicable control techniques, refer to Attachment A, p. III-77.

(c) Systems Software Security - Access to system software and related documentation should be restricted to authorized personnel. For examples of applicable

control techniques, refer to Attachment A, p. III-75.

(b) Systems Software Maintenance - System software changes should be properly documented, tested, and approved before implementation. For examples of applicable control techniques, refer to Attachment A, p. III-77.

(c) Systems Software Security - Access to system software and related documentation should be restricted to authorized personnel. For examples of applicable control techniques, refer to Attachment A, p. III-79.

6. Data Center Operations

Control Objectives(s)

(a) Operations Procedures - Formal operations procedures and techniques should be used to provide reasonable assurance that the computer is operated efficiently and effectively. For examples of applicable control techniques, refer to Attachment A, p. III-81.

(b) Supervision and Review of Operations - Supervision and review of operations should provide reasonable assurance that the computer is used only for authorized

purposes and that operators are following prescribed procedures. For examples of applicable control techniques, refer to Attachment A, p. III-83.

(c) Input/Output Control and Scheduling - All input, error corrections, and output should be properly controlled and scheduled to ensure accurate and complete processing of data and proper distribution of report. For examples of applicable control techniques, refer to Attachment A, p. III-85.

7. Data Center Protection

Control Objective(s)

(a) Responsibility for Physical Security and Access Control - Responsibility for physical security and access control should be assigned to competent personnel at appropriate levels within the organization. For examples of applicable control techniques, refer to Attachment A, p. III-87.

(b) Access to Computer Room Equipment, and Critical Documents and Forms - Access to computer room, equipment, and critical documents and forms should be restricted to authorized personnel. For examples of applicable control techniques, refer to Attachment A, p. III-89.

(c) Access to Programs - Access to application program files and related documentation should be restricted to authorized personnel. For examples of applicable control techniques, refer to Attachment A, p. III-91.

(d) Access to Data - Access to data files should be restricted to authorized personnel. For examples of applicable control techniques, refer to Attachment A, p. III-93.

(e) Environment Protection - Facilities and files should be protected against accidental or malicious destruction by fire, water, or other hazards. For examples of applicable control techniques, refer to Attachment A, p. III-95.

(f) Background and Disaster Recovery - Formal procedures should exist for the backup of critical data files and programs and for the recovery of information system services in the event of an unanticipated disaster or interruption. For examples of applicable control techniques, refer to Attachment A, p. III-97.

b. Summary of ADP Internal Controls - Application Control Evaluation

1. Data Origination, Data Input, Data Processing, and Data Output (Responsibility: Audit Team - Data Organization, Data Input and Data Output; IMTEC - Data Processing)

Control objectives (s)

- (a) Separation of duties - Key duties and responsibilities performed within an application should be adequately separated. For examples of applicable control techniques, refer to Attachment B, p. III-99.

2. Data Origination (Responsibility: Audit Team)

Control objective(s)

- (a) Source Document Origination - Source documents should be properly prepared, and only by authorized personnel. For examples of applicable control techniques, refer to Attachment B, p. III-101.

- (b) Source Document Authorization - Source documents should be authorized by persons acting within the scope of their authority. For examples of applicable control techniques, refer to Attachment B, p. III-103.

- (c) Source Document Data Collection and Input Preparation - All authorized source documents should be complete and accurate, properly accounted for, and transmitted in a timely manner for input to the computer system. For

examples of applicable control techniques, refer to Attachment B, p. III-105.

(d) Source Document Error Handling - Error handling procedures during data origination should reasonably assure that errors and irregularities are detected, reported, and corrected. For examples of applicable control techniques, refer to Attachment B, p. III-107.

(e) Source Document Retention - Source documents should be retained to facilitate the retrieval or reconstruction of data. For examples of applicable control techniques, refer to Attachment B, p. III-109.

3. Data Input (Responsibility: Audit Team and IMTEC, if necessary)

Control objective(s)

(a) Batch--Data Conversion and Entry - Procedures should be established for the conversion and entry of data that ensure a separation of duties as well as routine verification of work performed in the data input process. For examples of applicable control techniques, refer to Attachment B, p. III-111.

(b) Batch--Data Validation and Editing - Input data should be validated and edited to provide reasonable assurance that erroneous data are detected before processing. For examples of applicable

control techniques, refer to Attachment B, p. III-113.

(c) Batch--Data Input Error Handling - Errors should be investigated and resubmitted for processing promptly and accurately. For examples of applicable control techniques, refer to Attachment B, p. III-115.

(d) On-Line--Data Conversion and Entry - Procedures related to the conversion and entry of data through terminals should be established to deter unauthorized use. For examples of applicable control techniques, refer to Attachment B, p. III-117.

(e) On-Line--Data Validation and Editing - Input data should be validated and edited to provide reasonable assurance that erroneous data are detected before processing. For examples of applicable control techniques, refer to Attachment B, p. III-119.

(f) On-Line--Data Input Error Handling - Errors should be investigated and resubmitted for processing promptly and accurately. For examples of applicable control techniques, refer to Attachment B, p. III-121.

4. Data Processing (Responsibility: IMTEC)
Control objective(s)

(a) Batch--Data Processing Integrity Procedures - Formal procedures should be established for data processing to ensure that data are processed completely, accurately, and on time. For examples of applicable control techniques, refer to Attachment B, p. III-123.

(b) Batch--Data Processing Integrity Provisions - Provisions to ensure complete and accurate processing of data should be included in application programs. For examples of applicable control techniques, refer to Attachment B, p.

(III-125.

c) Batch--Data Processing Validation and Editing - Data should be validated and edited during processing to provide reasonable assurance that erroneous data are detected and reported for investigation. For examples of applicable control techniques, refer to Attachment B, p. III-127.

(d) Batch--Data Processing Error Handling - Errors identified during data processing should be investigated, corrected, and resubmitted for processing. For examples of applicable control techniques, refer to Attachment B, p. III-129.

(e) Real-Time--Data Processing Integrity Procedures - Formal procedures should be established for data processing to ensure that data are processed completely, accurately, and on time. For examples

of applicable control techniques, refer to Attachment B, p. III-131.

(f) Real-Time--Data Processing Integrity Provisions

- Provisions to ensure complete and accurate processing of data should be included in application programs. For examples of applicable control techniques, refer to Attachment B, p. III-133.

g) Real-Time--Data Processing Validation and Editing - Data should be validated and edited during processing to provide reasonable assurance that erroneous data are detected and reported for investigation. For examples of applicable control techniques, refer to Attachment B, p. III-135.

h) Real-Time --Data Processing Error Handling - Errors identified during data processing should be promptly investigated, corrected, and resubmitted for processing. For examples of applicable control techniques, refer to Attachment B, p. III-137.

5. Data Output (Responsibility: Audit Team and IMTEC, if necessary)

Control objective(s)

(a) Batch--Output Balancing and Reconciliation -

Output should be balanced to record counts and control totals, and audit trails. For examples of applicable control techniques, refer to Attachment B, p. III-139.

- (b) Batch--Output Distribution - Output should be promptly distributed to authorized users. For examples of applicable control techniques, refer to Attachment B, p. III-142.
- (c) Batch--Output Error Handling - Procedures should exist to report and control errors contained in output. For examples of applicable control techniques, refer to Attachment B, p. III-144.
- (d) Batch--Output Handling and Retention - Output handling and retention procedures should provide reasonable assurance that output is properly secured and retained for the appropriate time period. For examples of applicable control techniques, refer to Attachment B, p. III-146.
- (e) On-line--Output Balancing and Reconciliation - Output should be balanced to record counts and control totals, and audit trails should be available to facilitate tracing and reconciliation. For examples of applicable control techniques, refer to Attachment B, p. III-148.
- (f) On-line--Output Distribution - Output should be promptly distributed to authorized users. For examples of applicable control techniques, refer to Attachment B, p. III-151.
- (g) On-line--Output Error Handling - Procedures should exist to report and control errors contained in output. For examples of applicable control techniques, refer to Attachment B, p. III-153.

(h) On-line--Output Handling and Retention - Output handling and retention procedures should provide reasonable assurance that output is properly secured and retained for the appropriate time period. For examples of applicable control techniques, refer to Attachment B, p. III-155.

C. ADP RELATED IMPROVEMENTS RESULTING FROM THE FIA PROCESS

Objective: Describe ADP related improvements resulting from the FIA process. (IMTEC will perform this objective using steps in Section A-III, Progress and Problems in Internal Control Systems.)

Tasks:

- a. Based on interview and observation, determine improvements resulting from the FIA process.

SECTION A-III
PROGRESS AND PROBLEMS IN IMPROVING
INTERNAL CONTROL SYSTEMS

Our objective in this section is to examine the agency's corrective actions to determine if they are reasonable, address the problems, are effective, and being implemented in a timely manner. We will discuss the corrective actions with agency, GAO and IG officials and, on a limited basis, test to see that the actions are correcting the identified weaknesses and improving internal controls. In addition, we will obtain any available related data on costs and benefits of the FIA process collected by the agency.

A. Corrective actions for material weaknesses in the agency's 1983 annual report to the Congress.

1. Select four of the most significant material weaknesses/areas reported (whether corrected or not) in the 1983 letter. Factors to consider are:

- Recent audit (GAO and IG) work in the area.
- Dollars in the area relative to the agency budget.
- Recent congressional or public interest.
- Longstanding problems that have been historically difficult to solve.
- Importance of the area to the agency mission or programs.

2. Is there a comprehensive corrective action plan for each material weakness/area reported?
 - a. Are the specific problems or weaknesses identified and explained?
 - b. Are the individual corrective actions specifically identified and explained?
 - c. Were alternative actions developed and considered?
 - d. Have milestones been established?
 - e. Has responsibility for implementing the plan been specifically assigned?
 - f. Has the plan been approved by top agency management?
 - g. Does the plan call for additional resources? Have they been requested and/or assigned?
 - h. Are the corrective actions supported by a cost/benefit analysis? If so, document the expected costs and benefits to the agency.
 - i. How old is the plan? Has implementation been previously attempted? What were/are the problems blocking the implementation?
 - j. Does the plan contain a method for evaluating the effectiveness of each corrective action?

3. Determine the status of the agency's corrective action plan for the four selected areas (may have been done in section A-I.G.2 p. 18).
 - a. Are the milestones being met? If not, why not?
 - b. Has the agency measured the effectiveness of corrective actions that have been implemented (such as testing)?
 - c. If measured, what are the results?
 - d. If actions have not been effective, what has the agency done to solve the problem?
4. Discuss the problem areas and corrective action plan with cognizant GAO and IG audit personnel. Obtain their views on whether--the problem statements adequately reflect the actual problems,
--the corrective actions will solve the problems,
--the milestones are realistic and achievable, and
--the overall corrective action plan is realistic and achievable.

If any of the above are negative, obtain their views on what the real issues are.
5. We should discuss the plan with agency managers involved in the problem areas. This should include, depending on the circumstances, the person (or group) who studied

the problem and/or wrote the corrective action plan; the person (or group) responsible for implementing the plan; and the manager of the organization involved. Obtain their views on whether

--the problem or statement adequately

reflects what the real problems are,

--the corrective actions will solve the problems,

--the milestones are realistic and achievable,

--the overall corrective action plan is realistic and achievable, and

--the plan will achieve its projected benefits.

6. Based on the above analysis, form an opinion on the overall worth (validity) of the plan. Comment specifically on each of the points in 4 and 5 above. Depending on the strength of your opinion and the support you have for it, you have several options:

--If you conclude that the plan definitely will not accomplish its objective, discuss your conclusion in your agency report. You should also advise the GAO program audit group(s) of the situation so they can consider an indepth audit of the area.

--If you suspect that the plan will not accomplish its objectives, discuss it with the GAO audit group and ask them to consider it for an indepth audit. In the report you should say that GAO has some concerns about the plan and will monitor its implementation.

--If you have no major concerns about the plan, you should consider saying in your agency report that GAO sees nothing in the agency plan that would prevent successful implementation, but because the problem is (complex, longstanding, dependent on future congressional support, etc. [choose one or more]) we will continue to monitor its implementation.

Teams should recognize that the major problems reviewed in this section are probably too complex and difficult to solve for us to endorse a corrective action plan in a GAO report.

B. Corrective actions in feeder reports and individual VAs/ICRs.

1. Using the sample of VAs and ICRs selected and reviewed in section A-I.G.1 (p. 16) of these guidelines complete the following steps.

(You should also include weaknesses from feeder reports.)

- a. Evaluate the corrective action plan for each VA or ICR selected. Since the depth of the corrective action plan will vary according to the complexity of the problem, there are no standard review steps for a plan. For some major weaknesses, each of the steps in A-III.A. above should be repeated. For others, a simple reading and judgment of reasonableness will be sufficient. The following questions should be answered:
 - Does the plan adequately address the problem?
 - Does the plan arrive at a reasonable solution?
- b. Evaluate the effectiveness of selected corrective actions that have been implemented.

- (1) Obtain evidence of and verify implementation. Does it address and solve the problem? If feasible, limited testing should be done.

(2) How did the agency assure itself that the corrective action solved the problem?

2. Express an opinion on the overall effectiveness of the corrective action plans and corrective actions examined under this subsection (A-III. B.)

C. Benefits accruing to agencies from FIA include actual and planned improvements to internal controls as well as indirect benefits such as a greater awareness by management of the need for good internal controls.

1. Ask FIA officials and the managers of the programs, functions, or activities where FIA work took place, their opinion on the actual and potential benefits of FIA. The discussions should also include the effect that FIA is having on problem areas that were known prior to implementation of FIA. Officials and managers should be interviewed at agency headquarters and field locations where we perform the audit work. Interviews in this section should be conducted at the same time as other audit work in this program as appropriate.

- a. Identify specific benefits such as
 - (1) improved systems of internal controls,
 - (2) increased awareness of the importance of internal controls by managers at all levels, and
 - (3) others (give examples).
2. Some agencies are collecting data on the costs of implementing the FIA. If this is the case in your agency, obtain the information.

SECTION A-IV
ASSESSMENT OF THE REASONABLENESS OF THE
AGENCY'S SECOND ANNUAL ASSURANCE LETTER

Following the work performed in the first three sections of this guide, our objective is to assess the reasonableness of the agency's annual assurance letter. We will object to an agency's statement of assurance if we observe something of significance to contradict the statement. This work program, however, is not designed to give audit teams the ability or information to endorse the agency's statement of assurance. An endorsement would require extensive auditing or statistically significant sample testing of an agency's internal controls.

During the course of this review effort, we have evaluated several VAs and ICRs, as well as the agency's compliance with OMB guidelines. The results of these evaluations and our institutional knowledge should affect our assessment of the reasonableness of the agency's assurance letter.

A. In assessing the reasonableness the auditor should consider whether:

1. The agency's internal control process complied with the OMB's guidelines. We will challenge the agency's assertion that it followed the guidelines if there is a deviation which, in our opinion, materially affects the agency's ability to state that it followed the guidelines.

2. The agency did not include all programs, activities, and functions in its internal control evaluation process. If it has omitted significant activities we will take exception to the agency's statement that it complied with OMB's guidelines.
3. The agency's weaknesses (reported and unreported), when taken in the aggregate, are of such magnitude or importance that the agency cannot assert that, "taken as a whole", it has reasonable assurance.
4. The agency did not report all known (to the agency) material weaknesses. In this case, we will point out the omissions.

PART B

GUIDELINES FOR PERFORMING FIA
SECTION 4 AUDIT WORK

The act requires the agencies to submit an annual statement, by December 31, to the President and the Congress on whether their accounting system conforms to the accounting principles, standards and related requirements prescribed by the Comptroller General¹.

OBJECTIVES

The objectives of our review are to (1) update and evaluate the agencies' progress in evaluating their accounting systems, (2) determine the adequacy of agencies' plans and completed actions for correcting identified accounting system deficiencies including determinations of actions and plans for implementing revised Title 2, and (3) assess the reasonableness of agencies' annual statements of accounting systems' conformance with the CG's principles and standards.

In September 1983, the Comptroller General suggested several actions that agencies should take until formal OMB guidelines are available. These suggestions included establishing an inventory of accounting systems, identifying system deviations from GAO's P&S previously reported, identifying system enhancement projects, ranking systems according to the materiality of potential deviations from GAO's P&S, and initiating reviews of major systems. In taking these actions, we believe that agencies should give careful

¹The term GAO's P&S used throughout the audit program refers to the Comptroller General's Accounting Principles and Standards (Titles 2, 4, 5, 6, and 7) and related requirements such as Treasury Fiscal Requirements Manual, OMB Circulars, etc. Also, agency accounting systems must include internal controls that comply with the Comptroller General's internal control standards. See appendix I for a list of requirements to be considered.

consideration to organizing the process, identifying and following up on corrective actions deemed necessary for correcting system deviations, and establishing a reporting process for consolidating results for the agency's report.

These guidelines provide a framework for determining whether agencies' statements on conformance with GAO's Principles and Standards are accurate. Upon completion of this work, auditors should prepare a summary which will conclude (1) whether the agency's inventory of accounting systems is accurate and complete, (2) whether the statement considers all material system deficiencies identified by the agency, by GAO or by others, and (3) whether the agency adequately evaluated and tested its systems to determine whether they comply with GAO's P&S. The summary should clearly state our scope and methodology.

As a result of experience gained during the first year we have revised our basic audit approach and reporting requirements. These guidelines do not identify all audit steps needed to complete our work--instead the guidelines include the minimum requirement necessary to provide a basic understanding of each agency's Section 4 process for and progress in evaluating its accounting systems. These guidelines will also provide for an assessment of the agencies' progress toward correcting identified accounting system weaknesses. In instances where an agency's process for evaluating its systems is inadequate or our staff has reason to question the results of the evaluation, the audit staff may supplement these guidelines with additional audit steps to test the system and possibly take exception to the agency's report to the Congress.

One goal of our second year effort is to develop information that will enable us to compare and contrast agencies' efforts to implement section 4 of the Act. In addition to identifying problems associated with accounting system deficiencies and internal control weaknesses we want to obtain examples where agencies have been successful in developing and implementing good practices related to evaluating accounting systems (e.g. development of a comprehensive training program).

/

SECTION B-1

AGENCIES' PROGRESS

Our objective is to update and evaluate the agencies' progress in evaluating their accounting systems.

The purpose of this section is to develop information on the agencies' organization and implementation of its evaluation process for determining accounting systems' conformance with GAO's P&S.

General Tasks

1. Develop an inventory of system deviations using any of the following which provide current information:
 - GAO reports,
 - IG reports,
 - consultant/contractor studies and reports, and
 - congressional hearings.
2. Supplement this information through discussions with knowledgeable GAO staff and agency IG¹ officials.
3. Review prior year workpapers and reports relating to the FIA effort. For example:
 - GAO's FIA report to the agency,
 - GAO's overall FIA report to the Congress,
 - the agency's 1983 FIA report,
 - any IG and OMB reports on the FIA process, and
 - consultant and other reports relating to Section 4.

¹The term IG refers to the Inspector General or the equivalent; for example, internal audit.

4. Coordinate with GAO Section 2 and IMTEC teams to reduce duplication of efforts, for example, joint meetings with the IG.
5. Coordinate with OMB on their plans for year two to reduce duplication.
6. Coordinate with the IG to determine their plans for Section 4 FIA work.
 - a. Determine the role given to the IG in the overall compliance evaluation effort. For instance, was the IG:
 - providing technical assistance to those performing the compliance evaluations.
 - including reviews of internal controls in all audits.
 - commenting on the agency's final report for Section 4.
 - monitoring and providing comments on the compliance evaluation effort to make certain it was properly performed and in accordance with the agency and OMB guidelines.
 - selectively reviewing the compliance evaluations to assess quality, timeliness, and consistency.
 - b. Determine what objectives and tasks of this audit program have been or will be accomplished by the IG, which we could use in conjunction with or in lieu of our work. To accomplish this:
 - review the IG workpapers, work programs, reports, guidelines, etc.
 - evaluate whether the IG work may be used in conjunction with or in lieu of our work.

Tasks For Evaluating Agencies' Organization and Guidelines

In this section we will be concerned with evaluating the agencies' organization and guidelines for evaluating its accounting systems. Much of this work may have been accomplished during our first years' effort. Therefore, the auditor should merely update the process where warranted.

1. Describe the organizational structure designated for determining if the agency's accounting system is in conformance with GAO's P&S.
 - a. Determine whether the structure was set forth in written directives and obtain copies of the directives, instructions, and other guidance published by the agency.
 - b. Determine whether organizations having responsibility for designing and operating accounting systems have received the guidance and were aware of the effort.
 - c. Determine whether overall responsibility for the effort was assigned to a senior agency official such as the Assistant Secretary for Financial Management or Comptroller. If assigned to a lower-level official, determine if the official has sufficient authority to direct and coordinate the effort, and resolve conflicts.
 - d. Determine whether the directives established specific responsibility for conducting and monitoring the compliance evaluations, assuring that uniform quality is maintained for all evaluations, summarizing and consolidating the results of the compliance evaluations for the agency head's

report, and describing what action has or shall be taken to correct identified deficiencies.

e. Determine whether the agency's current organization provides for considering ADP controls.

2. Determine whether the agency has developed guidelines for conducting evaluations of its accounting systems.

a. If not, ask agency officials how they plan to meet the FIA Section 4 reporting requirements.

b. If so, compare the agency's guidelines to the OMB guidelines.

--Document specific instances where agency guidelines fall short of the intent of OMB guidelines.

--Document specific instances where agency guidelines exceeded requirements of the OMB guidelines.

--In instances where agency's guidelines specify a process other than the OMB guidelines, determine the adequacy of the process guidelines.

3. Document instances where the agency's guidelines were not a good tool for conducting evaluations. Regardless of whether the OMB guidelines are issued or not, the agency guidelines should address:

--developing a comprehensive accounting system inventory,

--identifying and providing training for conducting the evaluations,

--identifying the IG's role in the evaluation effort,

--ranking and scheduling agency accounting systems for evaluation,

--establishing system control objectives,

- identifying control techniques based on statutes and GAO's P&S,
- testing critical techniques in operation,
- identifying and determining reportable system deviations,
- implementing a process for determining the validity of data included in the agency's financial reports,
- documenting the process used to evaluate the accounting systems,
- using the evaluation results to report conformance/nonconformance with the GAO's P&S,
- implementing a tracking and follow-up system to monitor the status of actions recommended as a result of system evaluations,
- coordinating results of accounting system compliance evaluations with accounting and financial management deficiencies disclosed in internal control reviews, and
- assuring that uniform quality is maintained for all evaluations.

4. Determine the adequacy of documentation requirements for compliance evaluations. Include what written guidelines were issued concerning the preparation and maintenance of adequate documentation on the compliance evaluation results. If written guidelines are available, do they require a description of:
 - the documentation of the evaluation results,
 - the accounting system/subsystem evaluated,
 - the methodology and basis used in the compliance evaluation,
 - the organizational components involved and their roles in the performance of the compliance evaluation,

- what principles and standards were included within the scope of the evaluation,
- what principles and standards were not being met,
- the extent and results of transaction testing,
- what action was taken or is planned to correct the identified deviations,
- the organizational unit/person to which the compliance evaluation results will be reported,
- the role of the IG in reviewing the documentation for completeness and accuracy, and
- provisions for the documentation of conclusions reached in the compliance evaluations.

5. Determine whether the agency has established a reasonable schedule such as a 5-year plan, with target dates for performing evaluations of its systems conformance with the GAO's P&S.

a. Obtain a copy of the agency's schedule for performing evaluations.

b. Compare the scheduled dates with the actual dates of performance and document significant slippages in the schedule.

6. Determine if an internal reporting and summarization process has been established to communicate the results of the compliance evaluations. Comment on the following:

--has the agency established policies and procedures for the internal reporting and summarization process?

--how will the compliance evaluation be reported from those performing the evaluation and how will the results be consolidated at any "intermediate" organizational levels?

--will the reporting format be conducive for entering the results into the agency's follow-up system?

--to what organizational level will the results be reported?

7. Determine the agency's overall progress in developing and implementing procedures for evaluating its accounting systems for compliance.
 - a. Determine whether the agency has initiated or completed any accounting system evaluations.
 - b. If no evaluations were completed, determine the agency's plans for meeting the act's requirements.
8. Based on (1) the extent of the agency IG's planned efforts, and (2) the agency's progress in implementing Section 4 of the act, make an initial determination of the level of effort required by GAO to meet the objectives in these guidelines.

Tasks For Evaluating
Implementation Of The Process

In performing the tasks under this section, we will evaluate (1) the completeness of the agency's accounting system inventory, and (2) the adequacy of the agency's performance of compliance evaluations and the consolidating and reporting of the evaluation results. Relative to the inventory, this work may have been accomplished during our first year effort and need only be updated as appropriate.

1. Obtain a copy of the current accounting systems inventory from the agency. If unavailable,
 - a. Determine the status of the agency's plan for developing an inventory.
 - b. Determine if the plan appears reasonable, including target dates for finalizing the inventory and procedures for updating the inventory.
2. If the inventory is available, describe what the agency did to make certain that all its accounting operations were included in the inventory and determine if the agency included provisions for ensuring the inventory is updated as systems are replaced or modified.
3. Ask the agency to provide an overview describing each system/subsystem and their relationship to each other and to other financial management systems within the agency as well as the centralized accounting/reporting system of the central agencies.
 - a. Determine if the overview describes all the systems/subsystems on the agency's inventory.

- b. Determine if the overview describes the operation of each system/subsystem in terms of whether it is
 - operating on a standardized or nonstandardized basis,
 - manual or automated,
 - operating on a centralized or decentralized basis.
 - c. Determine if the overview describes
 - information captured and recorded by each system,
 - records and reports created and used by each system,
 - information transferred between systems,
 - control procedures used in each system,
 - flowcharts describing system inputs, key processing steps, system controls and outputs, and
 - procedures manuals for computer and manual operations.
 - d. Determine if the overview describes the relationships of the accounting system/subsystems to each other and to the agency's program, budget, and organizational structure. If the agency does not have an integrated accounting and budgeting structure, ask agency officials to describe how they compare their accounting results to the budget structure.
4. If the agency has an inventory, validate it using readily available information. For example,
- Treasury listing of Agency Location Codes.
 - listing of agency ADP accounting applications.
 - unique site identifiers in the agency's accounting handbook.
 - breakdown of the financial plan (budget).
 - prior agency accounting system inventories.

NOTE: It may not be necessary in all instances to compile all of the information above to validate the inventory. It is extremely important that the auditor use professional judgement in determining the accomplishment of this task and be able to justify the scope and methodology used.

5. Give an overall opinion on whether the agency's accounting systems inventory is complete and accurate based on our work. Discuss all disagreements with agency officials and determine if the differences are material.
6. Evaluate the adequacy of the actual performance of evaluations.
 - a. Determine how the agency ranked its systems for conducting evaluations and determine whether their method seems logical. Comment on whether the agency considered the results of past audits, inspections, studies, vulnerability assessments, and internal control reviews when ranking systems. Also, comment on whether the agency considered the size of the system, its purpose, the dollars accounted for, and the importance of the system to the operation and management of the agency.
 - b. Ask the agency to document the resources dedicated for each effort in terms of numbers of personnel, staff days, and dollars. If the requested breakout is unavailable, obtain the best available information. Determine whether a sufficient level of staff resources was committed to the effort in light of the agency size and organizational and management structure.
 - c. If the information is readily available, compare the level of effort devoted to the evaluations by organizational activity and accounting system/subsystem.

- d. Determine if the agency assigned personnel with the appropriate technical expertise to conduct the compliance evaluations of each accounting system. Categorize agency personnel as follows:
- agency comptroller/financial management personnel,
 - units/users,
 - IG staff,
 - ADP personnel,
 - other internal organizations,
 - contractors/consultants, and/or,
 - others (specify).
- e. Prepare a schedule categorizing the mechanism used by the agency for evaluating each accounting system using the following:
- checklist approach,
 - functional reviews,
 - internal reviews,
 - IG or GAO audit report,
 - prior GAO design approval,
 - OMB methodology, and
 - others (specify).
- f. Describe the methods used in performing compliance evaluations such as:
- reviewing documented policies and procedures,
 - discussions with the system/subsystem users,
 - observing system operations,
 - testing system operations,
 - knowledge of the using activities/individuals, etc.,
 - and/or,

--other (specify).

g. Determine if the agency's procedures for maintaining quality assurance over the evaluation process were followed and if they were adequate.

h. Through review of selected compliance evaluations, as well as discussions with agency personnel, comment on whether the agency adequately addressed the appropriate principles and standards in its reviews and if the reviews were adequately performed and documented. The number of compliance evaluations reviewed will depend on such factors as the number of evaluations performed, the procedures adopted by the agency to assure uniform quality of the evaluations, the GAO staff and time available, etc. In conducting reviews of agency compliance evaluations, consider whether the agency:

--reviewed the adequacy of the accounting system control objectives for assuring compliance with GAO's P&S,

--reviewed the adequacy of control techniques for achieving the control objectives,

--tested critical control techniques to determine whether they operate adequately,

--determined the status of and adequately considered prior GAO and internal audits, inspections, studies, and FIA vulnerability assessments and internal control review findings which disclosed accounting system deficiencies,

--evaluated and tested the adequacy of corrective actions taken as a result of prior audits, studies, inspections, vulnerability assessments and internal control reviews,

--evaluated the system structure,
--evaluated the system processes,
--evaluated the controls over and adequacy of system
 outputs,
--evaluated controls over system inputs,
--validated information in financial reports,
--adequately documented the accounting system compliance
 evaluations,
--adequately reported the results of compliance evaluations
 to agency officials responsible for the annual report
 under Section 4 of the FIA and for planning necessary
 corrective actions based on evaluation results, and
--provided adequate quality assurance over the evaluation
 process to assure that the evaluations were performed
 adequately, consistently, and in conformance with
 prescribed procedures.

- i. Identify what GAO P&S were identified by the agency as not being met in each accounting system/subsystem. Prepare a schedule of deviations identified in the compliance evaluations.
- j. Determine if the agency has appropriately coordinated and combined, where feasible, its efforts for performing compliance evaluations and internal control reviews. If not, discuss with agency officials the reasons and document the responses.
- k. Give an overall opinion on whether the agency conducted adequate compliance evaluations and had adequate quality assurance over its evaluation process. Document positive

aspects or procedures that the agency had in conducting compliance evaluations and determining quality assurance of the compliance evaluations' results.

7. Determine if the reporting and consolidation process provided the agency head with sufficient, factual information on whether the agency accounting system is in conformance with GAO's P&S.
 - a. Review the reports on compliance evaluations selected in task 6(h) and determine if results were communicated to the person/organization charged with the consolidation responsibility. If results were not communicated, consider expanding the scope of this work.
 - b. Determine if the departmental level consolidation effort accurately reflected the results of the compliance evaluations and if the results were accurately communicated to the agency head. For example,
 - were any intermediate consolidations accurate and not "watered down?"
 - were the results reported to the appropriate person/organizational level?
 - was action taken to verify the accuracy and completeness of the summarization and consolidation process at the departmental level such as a review by the IG?
 - had the reviewer accumulated all existing information on known deviations identified in GAO, agency, consultant and contractor reports and was such information used during the review process?
 - what questions were identified during the review process and how were they resolved?

- c. Determine whether all existing significant information pertaining to deviations from GAO's P&S, such as GAO, IG, and consultant reports, were communicated to the agency head.
- 8. Reach and document your conclusions on whether the agency's summarization and consolidation process was done properly, and whether it will provide the agency head with sufficient factual information upon which to conclude whether the agency's accounting system complies with GAO's P&S.

SECTION B-II

EVALUATING CORRECTIVE
ACTIONS PLANNED
AND COMPLETED

Our objective is to determine the adequacy of agencies' plans and completed actions for correcting identified accounting system deficiencies including determinations of actions and plans for implementing revised Title 2.¹

We want to evaluate the adequacy of agencies' corrective actions planned and completed and the capability of their follow-up systems to monitor actions taken and projected. Included are tasks to determine what the agencies are doing to incorporate revised Title 2 into their accounting systems.

1. Determine and describe what actions, if any, were taken or are being planned based on the compliance evaluations and on recommendations, suggestions, and observations in GAO's year 1 report. Does the agency plan to:

--develop and conduct training sessions on the need for importance of operating the system/subsystem in accordance with GAO's P&S.

--modify/redesign/clarify the system/subsystem to correct any deviations from GAO's P&S,

--take other actions (specify), or

--take no actions.

¹Title 2 is currently being revised and we expect to issue the revision this summer. Agencies should begin working toward implementing the revised title 2; however, full implementation will not be required for purposes of our evaluation of the agencies FIA reviews to meet the conformity requirement of the act for the agency annual report required December 31, 1984.

2. Using the evaluations selected for review, determine how the agency evaluated the alternatives available for corrective actions, for example: cost benefit analysis, resource and operational constraints.
 - a. Discuss these plans with responsible agency officials.
 - b. Determine whether realistic milestones and target dates (short and long range) have been established.
 - c. In instances where identified deficiencies are targeted for long range corrective actions, determine what interim measures the agency plans on using to correct selected problem areas within the deficiency.
 - d. Determine whether the required funding and resources have been identified.
 - e. Based on judgement, comment on whether the actions planned will adequately correct the deficiencies identified.
3. Determine how agency officials plan to assure themselves that corrective actions taken are effective.
4. Prepare a schedule of the status of corrective actions for (1) deficiencies identified in the first year reports and the year 2 reviews by the agency and (2) deficiencies identified by GAO which were not in the agency's report. If actions have not been initiated or have been initiated but are not yet fully implemented, determine and document the reasons why.
5. Determine what non-conformances the agency plans to include in its 1984 report and the planned actions to correct the deficiencies.

6. Evaluate the planned actions by considering the following (use data from task 2 above):
 - Does the planned action address the non-conformance identified?
 - Does the planned action seem reasonable for solving the problem?
 - Has a deadline/milestone been established for implementation of the corrective action?
 - Has anyone been designated responsible for implementing the corrective action?
 - If the corrective action involves external resources, have arrangements been made to obtain those resources? (e.g., has a contract been let or have funds been set aside?)
 - Prepare a schedule of new accounting systems and accounting system enhancements/redesigns planned or currently being developed. If available, show the cost of each and explain what system problems each will correct.
7. Evaluate the adequacy of the agency's follow-up system for ensuring the identification and correction of both accounting system internal control weaknesses and instances of accounting system non-conformance.
 - a. Determine if the system was developed specifically for A-123 and FIA requirements or has been "piggy-backed" onto an existing audit follow-up system.
 - b. Ascertain if the system has the capability to monitor whether corrective actions are actually taken in accordance with projected correction dates and whether the actions were effective.

--Using the compliance evaluations selected in task 6(h) under "Tasks for Evaluating Implementation of the Process," (see page 64), compare the corrective actions identified and dates for correction with information contained in the follow-up system. If information is not included in the system, consider expanding the scope of this work.

--Document results of the comparison and reasons for differences.

--If the agency does not have a formal follow-up system, determine if the agency has adequate procedures to ensure that identified deficiencies are corrected.

8. Discuss with agency officials and obtain their views on the draft GAO P&S (October 1983).
 - a. Determine whether the agency has begun to implement the proposed GAO P&S, for example, studies to determine what changes are needed in the agency's accounting system, contract requirements that systems under development must meet the proposed GAO P&S, and/or budget request for additional funds to modify systems.
 - b. Document plans, progress and problems.

SECTION B-III

AGENCIES' ANNUAL STATEMENT

Our objective is to assess the reasonableness of agencies' annual statements of accounting systems' conformance with the CG's Principles and Standards. We want to (1) summarize the information developed throughout the guidelines and (2) express an opinion on the agencies' basis for reporting under Section 4 of the act.

Tasks For Summarizing
Status of Systems

Using information developed throughout these guidelines, prepare an overall summary on the status of the agency's accounting systems. The summary should include:

- the status of the agency's inventory of its accounting systems subject to reporting under the act
- a discussion of GAO's principles and standards not met by the agency and considered in their 1984 FIA report
- a discussion of GAO's principles and standards not met by the agency which were not considered in their 1984 FIA report
- a discussion of other major system inadequacies identified through our interviews with agency officials
- a discussion of the comprehensiveness of the agency's plans for correcting its accounting system problems and its schedule for completing corrective actions including new systems and system enhancement projects. In instances where identified deficiencies are targeted for long range corrective actions, discuss what interim measures the agency plans on

using to correct selected problem areas within the deficiency

--a discussion of the agency's plans for completing evaluations of all its accounting systems

Tasks For Overall
Evaluation of Basis
For Reporting

If the agency will discuss their plans for reporting with us prior to issuing their final report, it may be necessary to perform the tasks in this section twice: first, when evaluating the agency's plans for its report; and second, when evaluating the agency's actual report, if different from its plans.

1. Express an opinion on:

- the appropriateness of the agency's organization and structure for implementing Section 4 of the act.
- the adequacy of the agency's inventory of accounting systems.
- the adequacy of the agency's evaluation of systems' conformance with GAO's P&S.
- the adequacy and comprehensiveness of the agency's efforts to correct instances of non-conformances with GAO's P&S.
- the adequacy of the agency's consideration of identified instances of non-conformances with the GAO's P&S when reporting to the President and the Congress.

2. List any deviations from GAO's P&S which the agency identified or we identified from past GAO/IG reports, etc. that were not considered in the agency's final report. (Use the inventory of

system deviations previously developed and other pertinent information obtained throughout this review.) Document the agency's reasons for excluding these deviations and decide what further work should be performed.

3. Determine whether the agency head's report responds fully to the requirements of the act and if the language of its report accurately describes the agency's compliance with GAO's P&S.
 - a. Comment on whether the agency report:
 - addresses all of the agency's accounting systems,
 - fully discloses all of the identified accounting system deviations from GAO's P&S, and
 - fully discloses the agency's process for evaluating and reporting on its systems, including which systems have been evaluated and which systems have not.
 - b. Comment on whether the agency process for evaluating its systems provided an adequate basis for determining and reporting on its systems' compliance with GAO's P&S and whether the results of the evaluations support the statements in its FIA report.
 - c. Comment on whether the agency's report provides an accurate description of the condition of the agency's accounting systems and their compliance with GAO's P&S.
 - d. Comment on whether the agency's corrective action plans are viable and comprehensive.

Requirements to be Considered

Congress:

Title 31, Money and Finance, of the U.S. Code

Authorizing legislation

Appropriation Acts

Congressional committees' reports

President:

Reorganization plans (Reform 88)

General Accounting Office:

General Accounting Office Policy and Procedures Manual for
Guidance of Federal Agencies

Federal government accounting series pamphlets

Decisions of the Comptroller General

Comptroller General's letters to heads of departments and
agencies.

Standards for Internal Controls in the Federal Government

Office of Management and Budget:

Circulars

Bulletins

Notices

Office of Personnel Management:

Federal Personnel Manual

Department of the Treasury:

Treasury Financial Manual

Treasury Financial Manual Bulletins

Department Circulars

General Services Administration:

Federal Travel Regulations

Federal Property Management Regulations

SUMMARY OF ADP INTERNAL CONTROLS

General Control Evaluation

Agency _____

System _____

Prepared by _____ Date _____

Reviewed by _____ Date _____

NOTE: Check all techniques that apply under each sub-area of activity. If additional control techniques are in use but are not listed, record them in the space provided at the end of each list of control techniques.

I. INTERNAL AUDIT

A. Inspector General Audit of ADP

- 1. Control Standard: Prompt Resolution of Audit Findings
- 2. Control Objective: The Office of Inspector General should substantiate and evaluate ADP activities and controls.
- 3. Control Techniques:

- The Inspector General has a qualified ADP audit team.
- Inspector General personnel review general controls in computer-based systems.
- Inspector General personnel perform rotational audits of application system and controls.
- Inspector General personnel review systems development activities and proposed systems controls.
- Inspector General personnel review significant modifications to applications and systems software.
- Inspector General personnel use computer-assisted audit techniques to test computer programs and verify transaction processing.
-
-
-
-

SUMMARY OF ADP INTERNAL CONTROLS^{1/}

The "Summary of ADP Internal Controls" is the instrument used to evaluate the adequacy of ADP controls. The Summary is organized in two parts. The first part is designed to analyze general controls. (Attachment A p. III-55) The second is designed to analyze application controls. (Attachment B p. III-99)

General controls affect all ADP applications. These controls are normally applicable to all processing being carried out within the ADP installation. General controls are divided into the following areas of ADP activity.

- Internal audit.
- Organization and management of the ADP department.
- System design, development, and maintenance.
- Hardware.
- System software.
- Data center operations.
- Data center protection.

Application controls are those controls that relate specifically to the system. They provide reasonable assurance that the recording, processing, and reporting of data are properly performed. Application controls are divided into the following areas of ADP activity:

- Data origination.
- Data Input.
- Data processing.
- Data Output.

1/ Source: Information System Review - Audit Guide - "Summary of ADP Internal Controls"--General Control Evaluation (Attachment A) and Application Control Evaluation (Attachment B), GAO/IMTEC.

II. ORGANIZATION AND MANAGEMENT OF THE ADP DEPARTMENT

A. Definition of Transactions and Events

1. Control Standard: Execution of Transactions and Events
2. Control Objective: The ADP Department's organizational structure, policies, and procedures should be clearly defined and communicated to provide reasonable assurance that ADP personnel perform correctly the duties they have been assigned.
3. Control Techniques:

- [] An executive ADP management committee establishes agency-wide ADP policies and approves short- and long-range system and computer equipment plans.
- [] An annual ADP operating budget is prepared and reviewed by the executive ADP management committee to ensure it is both comprehensive and appropriate.
- [] An agency organization chart is published and kept up to date showing the relationships between the ADP department and the rest of the organization.
- [] An ADP department organization chart is published and kept up to date.
- [] Formal job descriptions accurately reflect the duties performed and are kept up to date.
- [] Up-to-date policy manuals exist and are used by personnel.
- [] Up-to-date procedures manuals exist and are used by personnel.
- []
- []
- []
- []

B. Separation of Responsibilities

1. Control Standard: Separation of Duties
2. Control Objective: Key duties and responsibilities within the ADP department should be adequately separated to reduce the risk of errors, waste, or wrongful acts.
3. Control Techniques:

- [] The ADP department is independent of other agency functions.
- [] ADP personnel are prohibited from performing duties within other departments.
- [] The functions of system analysis, application programming, acceptance testing, production scheduling, equipment operation, data entry, data base management, systems programming, and data origination are performed by different groups and/or individuals and this separation is enforced.
- [] ADP personnel are prohibited from originating, changing, or correcting input or master file data (except for key-punch errors).
- [] Periodic job/shift rotations are required.
- [] ADP personnel are required to take regularly scheduled vacations.
- []
- []
- []
- []

C. Supervision

1. Control Standard: Supervision
2. Control Objective: ADP personnel should be properly supervised to ensure that delegated duties are performed in accordance with appropriate policies and procedures.
3. Control Techniques:

- [] There is a direct line of responsibility between every subordinate and supervisor.
- [] Subordinates' work is periodically reviewed by supervisors.
- [] No subordinate has more than one supervisor within a group or between groups.
- []
- []
- []
- []

D. Competent Personnel

1. Control Standard: Competent Personnel
2. Control Objective: ADP personnel should maintain and demonstrate personal and professional integrity and a level of skill necessary to accomplish the assigned duties.
3. Control Techniques:

- [] Personnel policies stress hiring individuals who are adequately qualified to perform their functional responsibilities.
- [] Personnel policies encourage training and development of competent personnel in their functional areas.
- [] A code of conduct governing personnel actions is published and enforced.
- [] Personnel are properly screened for security purposes in accordance with FPM Letter 732-7.
- [] Personnel are periodically appraised and counseled on their performance.
- []
- []
- []
- []

III. SYSTEM DESIGN, DEVELOPMENT, AND MAINTENANCE

A. System Acceptance

1. Control Standard: Execution of Transactions and Events
2. Control Objective: A formal system acceptance process should have been followed to provide reasonable assurance that the system was properly designed, developed, and tested before implementation.
3. Control Techniques:

- [] The system was subject to a formal system acceptance process.
- [] Sufficient time was allowed and sufficient staff members (both in numbers and qualifications) allocated for system acceptance purposes.
- [] System acceptance was performed by individuals independent of the analysis, design, and development of the system.
- [] The system acceptance process evaluated whether both manual and automated processes were performing in accordance with system specifications and processing standards.
- [] System acceptance was performed using data similar to, but independent of, program testing data.
- [] Once system acceptance was completed, but before the system was placed in operation, a written certification that the entire system performed in accordance with all specifications was required.
- []
- []
- []
- []

B. System Maintenance

1. Control Standard: Execution of Transactions and Events
2. Control Objective: All application program system changes should be authorized and approved by appropriate user and ADP management personnel.
3. Control Techniques:

- [] User management authorization and written approval are required for all application program/system changes.
- [] ADP management authorization and written approval are required for all application program/system changes.
- [] Program changes are thoroughly supervised and reviewed by programming supervisors.
- [] Users initiating changes are furnished with documentation that shows changes actually made.
- [] Users make the final decision on whether a change meets their needs.
- [] An executable load module library is used for production processing.
- [] Program library software is used to restrict access to computer programs and to report all program changes to user and ADP management.
- [] Computer operators are denied access to application systems documentation.
- [] Programmers are denied access to operations, production program files, and production JCL.
- [] Any program/system changes are subjected to system acceptance before being placed in operation.
- []
- []
- []
- []

C. Testing and Conversion

1. Control Standard: Execution of Transactions and Events
2. Control Objective: New and modified systems should be properly tested and implemented/converted.
3. Control Techniques:

- [] Each program, subsystem, and the system as a whole, are sequentially and comprehensively tested before implementation.
- [] Sufficient time and staff members (in both numbers and qualifications) are allocated for testing purposes.
- [] Testing is performed only on test files.
- [] Users are involved in preparing test data.
- [] Test results are approved by users and ADP management before implementation.
- [] Conversion procedures ensure proper cutoffs and conversion of data files.
- [] Testing is performed to evaluate the integrity of, all interfacing systems.
- [] New and modified systems are run parallel to old ones or as pilot systems to help ensure their accuracy.
- []
- []
- []
- []

D. Documentation

1. Control Standard: Documentation
2. Control Objective: New systems and program/system changes should be completely documented.
3. Control Techniques:

- [] Use of generally accepted design, programming, and documentation standards, as contained in FIPS 38 and 64, is required.
- [] Documentation is periodically reviewed to ensure it is current and complete and adheres to established standards.
- [] Approved change request forms are required to originate program system changes and are sequentially numbered and accounted for.
- [] Program library software is used to document and report all changes to user and ADP management.
- [] Written evidence exists of who performed all system analysis and programming work.
- []
- []
- []
- []

IV. SYSTEM HARDWARE

A. Integrated Hardware

1. Control Standard: Execution of Transactions and Events
2. Control Objective: Integrated hardware controls should be used to maximize the potential for detecting errors during processing.
3. Control Techniques:
 - [] Parity bit or other bit checks are used to detect parity errors.
 - [] Duplicate read-write operations are used to ensure the validity of data transfer.
 - [] Data transmission equipment contains built-in controls (validity and echo checking, etc.) that are adequate for checking transmission accuracy.
 - [] Program errors are detected by overflow, addressing, storage protection, and similar checks.
 - []
 - []
 - []
 - []

V. SYSTEM SOFTWARE

A. Selection and Installation of System Software

1. Control Standard: Execution of Transactions and Events
2. Control Objective: Systematic procedures should be followed to identify, select, and install system software.
3. Control Techniques:

- [] Formal procedures for identifying, selecting, and testing system software exist, are up to date, and are followed.
- [] System software was obtained from a reputable manufacturer and has been proven reliable.
- [] System software is comprehensively tested before being released for use.
- [] Documentation of system software is complete and kept current.
- []
- []
- []

B. System Software Maintenance

1. Control Standard: Execution of Transactions and Events
2. Control Objective: System software changes should be properly documented, tested, and approved before implementation.
3. Control Techniques:

- [] Formal policy and procedures pertaining to documentation and testing of system software maintenance exist, are up to date and are followed.
- [] Authorization and written approval of all changes are required by ADP management before changes are made.
- [] System software changes are subject to comprehensive testing before implementation.
- [] Library software documents all system software changes and provides an audit trail.
- [] All changes are thoroughly supervised and reviewed.
- [] Access to data files and application programs is denied to system programmers making system software changes.
- []
- []
- []
- []

C. System Software Security

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Access to system software and related documentation should be restricted to authorized personnel.
3. Control Techniques:

- [] System programmers are prohibited from operating the computer.
- [] Periodic security background investigations are performed on system programmers, in accordance with FPM 732-7.
- [] System software documentation is physically secure and access is restricted to authorized system programmers.
- [] System programs that allow normal system or application controls to be bypassed (i.e., Super-Zap, Ditto, direct file changes, etc.) are either prohibited or protected by the use of passwords and are used only in extreme circumstances and only in the presence of ADP supervisory personnel.
- []
- []
- []
- []

VI. DATA CENTER OPERATIONS

A. Operations Procedures

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Formal operations procedures and techniques should be used to provide reasonable assurance that the computer is operated efficiently and effectively.
3. Control Techniques:

- [] Detailed, written operator instructions are up to date and followed for each application, including set-up, file disposition, error response, and restart and recovery.
- [] Program and system design minimize operator processing actions.
- [] Computer files are uniquely identified to ensure easy reference of storage media.
- [] Current production programs are identified and distinguished from superseded and test versions.
- [] Formal preventive maintenance procedures have been established and are followed.
- [] Formal malfunction reporting procedures have been established and are followed.
- [] A plan exists that provides for the continuous monitoring and review of equipment performance and requirements.
- []
- []
- []
- []

B. Supervision and Review of Operations

1. Control Standard: Supervision
2. Control Objective: Supervision and review of operations should provide reasonable assurance that the computer is used only for authorized purposes and that operators are following prescribed procedures.
3. Control Techniques:

- [] Active supervision and review are provided on each shift.
- [] All operator activities are recorded on the console or operations log.
- [] Supervisors review console or operations log and job accounting reports and investigate abnormalities.
- []
- []
- []
- []

C. Input/Output Control and Scheduling

1. Control Standard: Execution of Transactions and Events
2. Control Objective: All input, error corrections, and output should be properly controlled and scheduled to ensure accurate and complete processing of data and proper distribution of report.
- 3: Control Techniques:

- [] Formal input/output control procedures have been established and are up to date.
- [] Formal scheduling procedures have been established and are up to date.
- [] A formal control group has been established within the data center.
- [] The control group logs all input and reconciles record counts and predetermined control totals submitted by users to record counts and control totals generated during processing.
- [] All errors disclosed during processing are controlled by an automated suspense file, and "clean-up" is monitored by the control group to ensure that the errors are promptly corrected.
- [] The control group is responsible for all negotiable instruments.
- [] Distribution of computer output is under strict control of the control group.
- [] The control group is responsible for scheduling computer runs, including production, nonproduction, aborted and erroneously processed.
- [] The computer system schedules work submitted through remote job entry.
- []
- []
- []
- []

VII. DATA CENTER PROTECTION

A. Responsibility for Physical Security and Access Control

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Responsibility for physical security and access control should be assigned to competent personnel at appropriate levels within the organization.
3. Control Techniques:

- [] Responsibility has been assigned for computer security for the agency overall and for each headquarters and field organization.
- [] Overall agencywide responsibility has been formally assigned for conducting periodic risk analyses of computer security.
- [] Risk analyses of computer security are periodically conducted in accordance with OMB Circular A-71, Transmittal Memorandum No. 1.
- [] General and application controls over computer-based systems are reviewed at the appropriate levels in meeting the requirements of the Federal Managers' Financial Integrity Act and OMB Circular A-123.
- []
- []
- []
- []

B. Access to Computer Room, Equipment, and Critical Documents and Forms

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Access to computer room, equipment, and critical documents and forms should be restricted to authorized personnel.
3. Control Techniques:

- [] There are clearly defined and approved policies and procedures stating that access to computer operations is limited to computer operators and operations supervisors. Others with need of limited access (e.g., hardware manufacturer representatives, systems programmers, etc.) are accompanied and closely watched by operations supervisors and prohibited from actually operating the computer.
- [] Physical barriers (locked doors, solid walls, etc.) restrict access to computer rooms.
- [] Access to computer rooms is restricted through the use of badges, special access keys, or other automated security devices.
- [] Terminals are located in areas that reduce risk of unauthorized viewing of data.
- [] Terminals connected to sensitive data have specifically scheduled hours of operation.
- [] Terminal activity reports are periodically reviewed for password violations, system abuses, unauthorized uses, or other unusual events.
- [] Access to source documents and critical forms (e.g., negotiable instruments, identification cards, etc.) during their storage and transportation is restricted to authorized personnel.
- [] Critical forms are prenumbered and accounted for periodically.
- [] Two or more people are present when critical forms are received, processed by the computer, or destroyed.
- [] Computer operations personnel are trained to use security controls and procedures.
- [] Security plans are tested periodically.
- []

C. Access to Programs

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Access to application program files and related documentation should be restricted to authorized personnel.
3. Control Techniques:

- [] Formal program library procedures exist, are up to date, and are followed.
- [] Program library software is used to restrict access to computer programs.
- [] Programmers are denied access to operations, production program files, and production JCL.
- [] Application systems documentation is physically secure and access is restricted to authorized programmers.
- [] Computer operators are denied access to application systems documentation.
- []
- []
- []
- []

D. Access to Data

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Access to data files should be restricted to authorized personnel.
3. Control Techniques:

- [] Data files are under strict control of a librarian at all times.
- [] Access to the library is limited at all times to the responsible librarian.
- [] File management system software restricts access to automated data files to authorized personnel.
- [] Passwords and identification codes are used to restrict access to and use of on-line data files.
- [] On-line functions that users are authorized to perform are restricted to specific dedicated terminals.
- [] Data file activity is logged and reviewed each day for possible access violations.
- [] Data base administrator controls passwords to data base.
- [] Users of data base have access only to data that is applicable to their systems.
- []
- []
- []
- []

E. Environmental Protection

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Facilities and files should be protected against accidental or malicious destruction by fire, water, or other hazards.
3. Control Techniques:

- [] Emergency procedures have been documented, are up to date, and employees are familiar with them.
- [] The computer center is separated from adjacent areas by fire-resistant partitions, walls, etc.
- [] The computer center is located apart from areas or activities that may be conducive to fire, flood, or explosion.
- [] Heat and smoke detectors and fire extinguishers are located in strategic areas.
- [] The computer center is protected by an automatic fire suppression system.
- [] The computer center is equipped with gauges that automatically activate signals if humidity or temperature go outside the normal range.
- []
- []
- []
- []

F. Backup and Disaster Recovery

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Formal procedures should exist for the backup of critical data files and programs and for the recovery of information system services in the event of an unanticipated disaster or interruption.
3. Control Techniques:

- [] Formal policy and procedures exist, are up to date, and are followed regarding the duplication of data and programs.
- [] Critical data files are duplicated on an appropriate schedule and stored off-site.
- [] Critical application programs and documentation are duplicated on an appropriate schedule and stored offsite.
- [] System software programs and documentation are duplicated on an appropriate schedule and stored off-site.
- [] Off-site application and system software programs are updated or replaced whenever significant changes are made to the programs.
- [] Access to off-site data files and programs is restricted to authorized personnel.
- [] The backup plan provides for necessary special forms and supplies.
- [] Formal backup arrangements exist with a compatible computer center.
- [] Backup procedures are periodically tested at the backup computer center.
- [] Critical environmental needs (e.g., air conditioning, power, etc.) are adequately backed up.
- []
- []
- []
- []

SUMMARY OF ADP INTERNAL CONTROLS

Application Control Evaluation

Agency _____

System _____

Prepared by _____ Date _____

Reviewed by _____ Date _____

NOTE: Check all techniques that apply under each subarea of activity. If additional control techniques are in use but are not listed, record them in the space provided at the end of each list of control techniques.

I. DATA ORIGINATION, DATA INPUT, DATA PROCESSING, AND DATA OUTPUT

A. Separation of Responsibilities

- 1. Control Standard: Separation of Duties
- 2. Control Objective: Key duties and responsibilities performed within an application should be adequately separated to reduce the risk of errors, waste, or wrongful acts.
- 3. Control Techniques:

[] The duties of data origination, data input, data processing, and data output are performed by different individuals.

[] Persons responsible for transaction origination or input are not responsible for originating or inputting data to master files.

[]

[]

[]

[]

II. DATA ORIGINATION

A. Source Document Origination

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Source documents should be properly prepared, and only by authorized personnel.
3. Control Techniques:
 - [] Documented procedures that explain the methods for proper source document origination, authorization, data collection, input preparation, error handling, and retention exist, are up to date, and are followed.
 - [] Source documents are designed to minimize errors and omissions.
 - [] Access to source documents and blank input forms is restricted to authorized personnel only.
 - []
 - []
 - []
 - []

B. Source Document Authorization

1. Control Standard: Execution of Transactions and Events Standard
2. Control Objective: Source documents should be authorized by persons acting within the scope of their authority.
3. Control Techniques:

- [] Authorizing signatures are used for all types of transactions.
- [] Documentation of approval is required for all critical transactions (system overrides, control bypassing, manual adjustments).
- [] Duties are separated to make sure that one individual does not prepare more than one type of transaction (e.g., establishing new records as well as changing or updating master records).
- []
- []
- []
- []

C. Source Document Data Collection and Input Preparation

1. Control Standard: Documentation
2. Control Objective: All authorized source documents should be complete and accurate, properly accounted for, and transmitted in a timely manner for input to the computer system.
3. Control Techniques:

- [] A user department control group is responsible for collecting source documents.
- [] The control group verifies that source documents are complete, accurate, and properly authorized.
- [] The user department control group controls source documents submitted to the data processing department for conversion or entry. This is done by using turnaround transmitted documents, batching techniques, record counts, predetermined control totals, or logging techniques.
- [] If the user department is responsible for its own data entry, a separate group within the department performs the input function.
- []
- []
- []
- []

D. Source Document Error Handling

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Error handling procedures during data origination should reasonably assure that errors and irregularities are detected, reported, and corrected.
3. Control Techniques:

- [] The user department control group identifies errors to facilitate the correction of erroneous information.
- [] Error logs are used to ensure timely followup and correction of unresolved errors.
- [] Source document originators are immediately notified by the control group of all errors.
- []
- []
- []
- []

E. Source Document Retention

1. Control Standard: Documentation.
2. Control Objective: Source documents should be retained to facilitate the retrieval or reconstruction of data.
3. Control Techniques:

- [] Source documents are retained so that data lost or destroyed during subsequent processing can be recreated.
- [] Source documents are stored so they can be easily and quickly retrieved.
- [] The retention period for each type of source document is preprinted on the document.
- []
- []
- []
- []

III. DATA INPUT

A. Batch -- Data Conversion and Entry

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Procedures should be established for the conversion and entry of data that ensure a separation of duties as well as routine verification of work performed in the data input process.
3. Control Techniques:

- [] Documented procedures for data conversion and entry exist, are up to date, and are followed.
- [] A data processing control group is responsible for data conversion and entry of all source documents received from user departments.
- [] The data processing control group accounts for all batches of source documents received from the user department to make sure that no batches are added or lost.
- [] The data processing control group reviews all input for user department approval.
- [] The data processing control group keeps a log showing the receipt of user department source documents and their actual disposition.
- [] The data processing control group uses turnaround transmittal documents, batching techniques, record counts, predetermined control totals, or logging techniques to control data submitted for conversion and data entry.
- [] Source documents are canceled after they have been entered.
- []
- []
- []
- []

B. Batch -- Data Validation and Editing

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Input data should be validated and edited to provide reasonable assurance that erroneous data are detected before processing.
3. Control Techniques:
 - [] Data validation and editing are performed as early as possible in the data flow to ensure that incorrect data are rejected before entry into the system.
 - [] All--or at least all significant--fields are key-verified.
 - [] Preprogrammed keying formats are used to ensure that data are recorded in the proper field, format, etc.
 - [] Key fields include check digits that are verified for validity.
 - [] Computer validation includes limit and reasonableness tests.
 - [] Overriding or bypassing data validation and editing problems is restricted to supervisors and is permitted in only a limited number of circumstances.
 - [] Every system override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.
 - []
 - []
 - []
 - []

C. Batch -- Data Input Error Handling

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Errors should be investigated and resubmitted for processing promptly and accurately.
3. Control Techniques:
 - [] Documented procedures for identifying, correcting, and reprocessing rejected data exist, are up to date, and are followed.
 - [] Error messages are displayed with clearly understood corrective actions for each type of error.
 - [] Rejected data are automatically written on an automated suspense file and held until corrected.
 - [] The automated suspense file is used to produce, on a regular basis and for management review, an analysis of the level of transaction errors and the status of uncorrected transactions.
 - [] Rejected transactions not caused by data conversion or entry errors are corrected by the user originating the transaction.
 - [] All corrections are reviewed and approved by supervisors before reentry.
 - []
 - []
 - []
 - []

D. On-Line -- Data Conversion and Entry

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Procedures related to the conversion and entry of data through terminals should be established to deter unauthorized use.
3. Control Techniques:

- [] Documented procedures for data conversion and entry exist, are up to date, and are followed.
- [] Terminals are located and locked in physically secure rooms.
- [] Supervisors are required to sign on each terminal device before anyone may sign on to begin work for the day.
- [] Data entry is made only from terminal devices with certain preassigned authority levels.
- [] Terminals are connected to the system only for certain periods of the day.
- [] Dial-up facilities perform call-back procedures to limit access to known, authorized terminals.
- [] Terminals generate a unique identifier code for computer verification.
- [] On-line access logs are maintained by the system and reviewed regularly for unauthorized access attempts.
- [] Passwords are used to prevent unauthorized use of terminals.
- [] Passwords and authorized codes are nonprinting or nondisplaying or are keyed onto obliterated spaces.
- [] A data access matrix is used to restrict unauthorized access to sensitive or classified data.
- [] All passwords are changed periodically; they are also changed when an individual changes jobs or separates and when there is a purported or real security violation.
- [] Transactions are logged as entered.
- [] Where appropriate, approved on-line input is batched and balanced against record counts and control totals entered by the operator.
- []

E. On-line--Data Validation and Editing

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Input data should be validated and edited to provide reasonable assurance that erroneous data are detected before processing.
3. Control Techniques:
 - [] Preprogrammed keying formats are used to ensure that data are recorded in the proper field, format, etc.
 - [] Prompting is used to reduce the number of operator errors.
 - [] Intelligent terminals are used to allow front-end validation, editing, and control.
 - [] Key fields include check digits that are verified for validity.
 - [] Computer validation includes limit and reasonableness tests.
 - [] Overriding or bypassing data validation and editing problems is restricted to supervisors and then only in a limited number of acceptable circumstances.
 - [] Every system override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.
 - []
 - []
 - []
 - []

F. On-line--Data Input Error Handling

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Errors should be investigated and resubmitted for processing promptly and accurately.
3. Control Techniques:

- [] Documented procedures for identifying, correcting, and reprocessing rejected data exist, are up to date, and are followed.
- [] Errors are displayed or printed immediately upon detection for immediate terminal operator correction.
- [] Error messages are displayed with clearly understood corrective actions for each type of error.
- [] Rejected data are automatically written on an automated suspense file and held until corrected.
- [] The automated suspense file is used to produce, on a regular basis and for management review, an analysis of the level of transaction errors and the status of uncorrected transactions.
- [] Rejected transactions not caused by data entry errors are corrected by the user originating the transaction.
- [] All corrections are reviewed and approved by supervisors before reentry.
- []
- []
- []
- []

IV. DATA PROCESSING

A. Batch--Data Processing Integrity Procedures

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Formal procedures should be established for data processing to ensure that data are processed completely, accurately, and on time.
3. Control Techniques: -

- [] Documented procedures for processing each application program exist, are up to date, and are followed, including operator instructions and computer program run books.
- [] A history log (including hardware and software failure messages, abnormal terminations of jobs, operator interventions, etc.) is printed on both a line printer and console and is routinely reviewed by supervisors.
- [] The ADP department has a schedule, by application, that shows when each application program is to be run and when it must be completed.
- [] A data processing control group (1) ensures that application schedules are met, (2) balances batch counts, record counts, and predetermined control totals, (3) maintains accurate logs of input/work/output files used in computer processing, and (4) ensures that restarts are performed properly.
- []
- []
- []
- []

B. Batch--Data Processing Integrity Provisions in Application Programs

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Provisions to ensure complete and accurate processing of data should be included in application programs.
3. Control Techniques:

- [] Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.
- [] Programs include routines to verify that the proper version of the computer file is used during processing.
- [] Programs include routines for checking internal file header labels before processing.
- [] Computer operators are prevented from overriding label or device errors.
- [] Internal trailer labels containing control totals (record counts, predetermined control totals) are generated for all computer files and tested by the application programs to determine that all records have been processed.
- [] System/program interfaces require that the sending system/program output counts equal the receiving system/program counts.
- []
- []
- []
- []

C. Batch--Data Processing Validation and Editing

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Data should be validated and edited during processing to provide reasonable assurance that erroneous data are detected and reported for investigation.
3. Control Techniques:

- [] The application rejects incorrect data before the master file is updated.
- [] Data validation and editing are performed on all fields even though an error may have been detected in an earlier field.
- [] Relationship editing is performed between input transactions and master files to check for appropriateness and correctness before updating.
- [] Transactions are verified using a table of values or master files of approved vendors, employees, etc., before they are processed.
- [] Programs perform limit and reasonableness checks on results of critical calculations.
- [] A "was-is" report, which shows master file contents before and after each change, is prepared and reviewed by the user.
- [] Record counts and predetermined control totals generated by the application are used by the data processing control group to validate the completeness of data processed by the system.
- []
- []
- []
- []

D. Batch--Data Processing Error Handling

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Errors identified during data processing should be promptly investigated, corrected, and resubmitted for processing.
3. Control Techniques:

- [] Documented procedures for identifying, correcting, and reprocessing rejected data exist, are up to date, and are followed.
- [] Error messages are displayed with clearly understood corrective actions for each type of error.
- [] Rejected data are automatically written on an automated suspense file and held until corrected.
- [] The automated suspense file is used to produce, on a regular basis and for management review, analyses of level-of-transaction errors and the status of uncorrected transactions.
- [] Rejected transactions are corrected by the users originating them.
- [] All corrections are reviewed and approved by supervisors before the corrections are reentered.
- []
- []
- []
- []

E. Real-Time--Data Processing Integrity Procedures

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Formal procedures should be established for data processing to ensure that data are processed completely, accurately, and on time.
3. Control Techniques:

- [] Documented procedures for processing each application program exist, are up to date, and are followed.
- [] A history log (including hardware and software failure messages, abnormal termination of jobs, operator interventions, etc.) is printed on both a line printer and console and is routinely reviewed by supervisors.
- [] A data processing control group monitors terminal activity; investigates and corrects terminal problems; investigates operator intervention actions; balances batch counts, record counts, and predetermined control totals of data processed (as developed during off-line operations); and ensures that restarts are performed properly.
- [] Transactions entered on-line are dated and time stamped and logged on computer files to provide an audit trail.
- [] Messages and data can be traced to the user or the point of origin.
- [] Application programs are prevented from accepting data from computer consoles.
- []
- []
- []
- []

F. Real-Time--Data Processing Integrity Provisions in Application Programs

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Provisions to ensure complete and accurate processing of data should be included in application programs.
3. Control Techniques:

- [] Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.
- [] Programs include routines to verify that the proper version of the computer file is used during processing.
- [] Programs include routines for checking internal file header labels before processing.
- [] Computer operators are prevented from overriding label or device errors.
- [] Internal trailer labels containing control totals (record counts, predetermined control totals) are generated for all computer files and tested by the application programs to determine that all records have been processed.
- [] System/program interfaces require that the sending system/program output counts equal the receiving system/program counts.
- [] The application protects against concurrent file updates (i.e., when a record is initially accessed, it cannot be further accessed until initial processing is complete).
- []
- []
- []
- []

G. Real-Time--Data Processing Validation and Editing

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Data should be validated and edited during processing to provide reasonable assurance that erroneous data are detected and reported for investigation.
3. Control Techniques:

- [] The application rejects incorrect data before the master file is updated.
- [] Data validation and editing are performed on all fields even though an error may have been detected in an earlier field.
- [] Relationship editing is performed between input transactions and master files to check for appropriateness and correctness of the information before updating the master file.
- [] Before being processed, transactions are verified using a table of values or the master files of approved vendors, employees, etc.
- [] Programs perform limit and reasonableness checks on results of critical calculations.
- [] A "was-is" report showing master file contents before and after each change is prepared and reviewed by the user.
- [] The data processing control group uses record counts and predetermined control totals generated by the application to validate the completeness of data processed by the system.
- []
- []
- []
- []

H. Real-Time--Data Processing Error Handling

1. Control Standard: Recording of Transactions and Events
2. Control Objective: Errors identified during data processing should be promptly investigated, corrected, and resubmitted for processing.
3. Control Techniques:

- [] Documented procedures for identifying, correcting, and reprocessing rejected data exist, are up to date, and are followed.
- [] Error messages are displayed with clearly understandable corrective actions for each type of error.
- [] Rejected data are automatically written on an automated suspense file and held until corrected.
- [] The automated suspense file is used to produce, on a regular basis and for management review, analyses of level-of-transaction errors and the status of uncorrected transactions.
- [] Rejected transactions are corrected by the users originating them.
- [] All corrections are reviewed and approved by supervisors before the corrections are reentered.
- []
- []
- []
- []

V. DATA OUTPUT

A. Batch--Output Balancing and Reconciliation

1. Control Standard: Documentation
2. Control Objective: Output should be balanced to record counts and control totals, and audit trails should be available to facilitate tracing and reconciliation.
3. Control Techniques:

- [] Documented procedures that explain how to properly balance and reconcile output products exist, are up to date, and are followed.
- [] Report identification and end-of-report messages are used.
- [] The data processing control group reviews output products for general acceptability and completeness.
- [] To ensure that no data were added or lost during processing, the data processing control group reconciles output batch totals, record counts, and predetermined control totals with input batch totals, record counts, and predetermined control totals before any output is transmitted.
- [] The data processing control group keeps a log that summarizes the output produced and recipients of the output (including the number of application reports generated, number of copies of each report, and recipient(s) of each report).
- [] The user department control group verifies the accuracy and completeness of all outputs.
- [] The user department control group verifies all computer-generated batch totals, record counts, and predetermined control totals with their manual counts.
- [] The user department control group is given lists of all changes to application system master file data.
- [] The user department control group is given lists of all internally generated transactions produced by the application.

- [] The user department control group is given lists of all interface transactions processed by the application.
- [] The user department control group is given lists of all transactions entered into the system.
- [] Transactions can be traced from the original source documents to the final output and back.
- []
- []
- []
- []

B. Batch--Output Distribution

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Output should be promptly distributed to authorized users.
3. Control Techniques:

- [] Documented procedures explaining how output products should be handled and distributed exist, are up to date, and are followed.
- [] The data processing control group is responsible for distributing all output produced by the application.
- [] The data processing control group has a schedule, by application, that shows when output processing will be completed and when output products need to be distributed.
- [] The data processing control group maintains a formalized output distribution checklist to show the distribution of each output product.
- [] The data processing control group verifies that only authorized numbers of copies of outputs are produced.
- []
- []
- []
- []

C. Batch--Output Error Handling

1. Control Standard: Documentation
2. Control Objective: Procedures should exist to report and control errors contained in output.
3. Control Techniques:

- [] Documented procedures that explain the methods for reporting, correcting, and reprocessing output products with errors exist, are up to date, and are followed.
- [] The user is notified immediately by the data processing or user department control group of problems in output.
- [] The data processing control group keeps a control log of output product errors and the corrective actions taken.
- [] The user department control group keeps a control log of output product errors and the corrective actions taken.
- [] Output from rerun jobs is subjected to the same quality review as the erroneous original output.
- []
- []
- []
- []

D. Batch--Output Handling and Retention

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Output handling and retention procedures should provide reasonable assurance that output is properly secured and retained for the appropriate time period.
3. Control Techniques:

- [] Record and document retention periods have been established, are up to date, and are followed.
- [] The retention periods are reasonable for backup and audit purposes.
- [] Appropriate methods (e.g., degaussing, shredding, etc.) are used to dispose of unneeded records and documents.
- [] Access to records and documents is restricted to authorized individuals.
- [] Periodic reviews are made to determine if output transmitted to users is still needed by them.
- [] Dual custody techniques are used to control the transmission, distribution, destruction, and return of accountable documents (checks, bonds, identification cards, etc.).
- []
- []
- []
- []

E. On-Line--Output Balancing and Reconciliation

1. Control Standard: Documentation
2. Control Objective: Output should be balanced to record counts and control totals, and audit trails should be available to facilitate tracing and reconciliation.
3. Control Techniques:

- [] Documented procedures that explain the methods for proper balancing and reconciliation of output products exist, are up to date, and are followed.
- [] Report identification and end-of-report messages are used.
- [] The data processing control group reviews output products for general acceptability and completeness.
- [] Before any output is transmitted, the data processing control group reconciles output batch totals, record counts, and predetermined control totals with input batch totals, record counts, and predetermined control totals. This is done to ensure that no data were added or lost during processing.
- [] The data processing control group keeps a log that summarizes output produced and recipients of the output (including number of application reports generated, number of copies of each report, and recipient(s) of each report).
- [] The user department control group verifies the accuracy and completeness of all outputs.
- [] The user department control group verifies all computer-generated batch totals, record counts, and predetermined control totals with their manually developed totals.
- [] The user department control group is given lists of all changes to application system master file data.
- [] The user department control group is given lists of all internally generated transactions produced by the application.

- [] The user department control group is given lists of all interface transactions processed by the application.
- [] The user department control group is given lists of all transactions entered into the system.
- [] Transactions can be traced from the original source documents to the final output and back.
- [] A log is kept at each output transmission device to provide an audit trail for outputs being transmitted to user terminal devices.
- [] Terminal devices automatically disconnect from the computer system if they are unused for a certain period of time.
- [] The day's activities are summarized and printed for each terminal device and reviewed by supervisors to determine the correctness of output production.
- [] The computer system automatically checks the output message before displaying, writing, or printing it to make sure that it has not reached the wrong terminal output device.
- []
- []
- []
- []

F. On-line--Output Distribution

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Output should be promptly distributed to authorized users.
3. Control Techniques:

- [] Documented procedures explaining how to properly handle and distribute output products exist, are up to date, and are followed.
- [] The user department control group is responsible for distributing all output produced by the application.
- [] The user department control group has a schedule, by application, that shows when output processing will be completed and when output products need to be distributed.
- [] The user department control group maintains a formalized checklist to show the distribution of each output product.
- [] The user department control group verifies that only authorized numbers of copies of outputs are produced.
- []
- []
- []
- []

G. On-Line--Output Error Handling

1. Control Standard: Documentation
2. Control Objective: Procedures should exist to report and control errors contained in output.
3. Control Techniques:

- [] Documented procedures that explain how to report, correct, and reprocess output products with errors, exist, are up to date, and are followed.
- [] The user is notified immediately by the user department control group of any problems in output.
- [] The user department control group keeps a control log of output product errors and corrective actions taken.
- [] Output from rerun.jobs is subjected to the same quality review as the erroneous original output.
- []
- []
- []
- []

E. On-Line--Output Handling and Retention

1. Control Standard: Access to and Accountability for Resources
2. Control Objective: Output handling and retention procedures should provide reasonable assurance that output is properly secured and retained for the appropriate time period.
3. Control Techniques:

- [] Record and document retention periods have been established, are up to date, and are followed.
- [] The retention periods are reasonable for backup and audit purposes.
- [] Appropriate methods (e.g., degaussing, shredding, etc.) are used to dispose of unneeded records and documents.
- [] Access to records and documents is restricted to authorized individuals.
- [] Periodic reviews are made to determine if output transmitted to users is still needed by them.
- [] Dual custody techniques are used to control the transmission, distribution, destruction, and return of accountable documents (checks, bonds, identification cards, etc.).
- []
- []
- []
- []