Chapter I - Considering the Effects of EDP on the Audit

Introduction

This manual describes the office's approach to considering the effects of electronic data processing (EDP) on our audits. References to audits or auditors throughout this manual include both financial and performance audits or auditors. The approach consists of: (1) planning the audit, (2) gaining an understanding of the internal control structure, (3) planning to test EDP controls, (4) testing application controls, (5) testing general controls, and (6) communicating the findings and recommendations. The approach takes into consideration computer technology trends, auditing standards and applicable statutes, and audit efficiency.

Computer technology is moving toward more automation every day. Automation increases the speed and reliability of doing business, and decreases the costs. Modern automated systems are evolving from back office accounting systems into information processing systems that integrate all the activities of the agency, financial and non-financial. These systems eliminate paper-based transaction records, including traditional audit trails. When this happens, auditors must develop new audit techniques.

Auditing standards and applicable statutes require us to consider the effects of EDP on our audits. AICPA and GAO Yellow Book standards require us to gain an understanding of the internal control structure on every audit, although they do not require us to test controls. These standards relate management's financial statement assertions to control procedures, and explain how to reduce substantive tests by relying on the controls. To the extent that EDP controls assure us that management assertions are materially correct, we can decrease our substantive tests of transaction details by testing the EDP controls.

The Single Audit Act, and the related auditing literature, indicate that auditors must test control procedures when auditing major federal financial assistance programs. The controls to be tested are those designed to ensure compliance with general and specific federal requirements, including eligibility, allowable costs and federal financial reporting. Therefore, EDP controls should be tested when they help ensure compliance with federal requirements.

Both computer technology and auditing standards are pushing us in the direction of more EDP auditing rather than less. Auditors may have some difficulty adjusting their audit techniques to move in this direction. This manual presents an approach to considering the effects of EDP on the audit that is both efficient and consistent with changes in computer technology and requirements of auditing standards and statutes.

Considering the effects of EDP on the audit begins during audit planning. The auditor should identify the application systems that could affect the audit objectives. The auditor must then determine whether each system identified is significant enough to require documenting an understanding of the EDP controls. Section 1, Planning the Audit, discusses these tasks.
If any of the applications are significant, the auditor should gain an understanding of the controls that are relevant to the audit objectives. This includes both application controls and general controls. Section 2, Gaining an Understanding presents procedures for gaining and documenting this understanding.

Some application systems are simple and straightforward, and we can easily audit around them. However, we cannot easily audit around systems that process very large volumes of data, perform complex computations, do not produce a simple paper-based audit trail, or interface with other systems. When the size or complexity of the application makes auditing around it impossible, we must test EDP controls.

When auditing through an application system, the auditor should make sure that the EDP controls necessary to support management's assertions are functioning effectively. As a general rule, the auditor can focus attention on a handful of critical controls to achieve this objective. The financial/performance and EDP auditors should jointly determine the EDP audit areas for review according to the overall audit objectives. They should then agree on how to coordinate their work. Section 3, Planning to Test Controls, explains this.

Some EDP controls that the auditor must test to achieve the audit objectives are specific to the various application systems. Section 4, Testing Application Controls discusses these application controls, such as data completeness procedures and data accuracy edits.

Other EDP controls affect multiple application systems. Section 5, Testing General Controls discusses these general controls, such as information security and program maintenance procedures.

Reviewing these application and general controls gives us the most important information we need to understand the effects of EDP on the agency. While reviewing these controls, we may identify reportable conditions for inclusion as Items for Discussion. Sometimes, we may find efficiency problems that also should be reported. Section 6, Communicating Findings and Recommendations, discusses the communication of these matters.

The following sections document the approach to be taken by the auditor and the EDP auditor in reviewing the effects of EDP on our audits. Many of the suggested procedures are included in the current General and Internal Control segments of the audit program. Additional audit steps should be added to our current audit programs based on specific audit considerations and auditor judgment.
Section 1. Planning the Audit

According to AICPA standards, the auditor should consider the methods the entity uses to process accounting information in planning the audit. The auditor should consider the extent of automation in each significant accounting application, the complexity of computer operations, the computer processing organizational structure, the availability of data, and the use of computer assisted audit techniques. Also, the auditor should consider whether specialized skills are needed to consider the effect of computer processing on the audit, to understand the internal control structure, or to design and perform audit procedures.

To comply with these standards, the auditor must consider the systems used by the agency. First, the auditor must identify all the application systems that could affect the audit. Applications which may affect audit objectives include general ledger, payroll, accounts receivable, purchasing, and eligibility for federal programs. The auditor should identify the systems through inquiries, examination of system inventories, and consultation with the EDP staff.

Early in the planning process, the auditor should check with the EDP staff for background information, then obtain or update the following information for each application system: (a) system name, (b) business function, (c) financial statement accounts/compliance requirements affected by the system, and (d) computer hardware that runs the system. For each system identified, the auditor should document:

1. The significance of the system to agency operations relative to our audit objectives.
2. The known or alleged system problems that increase the risk of errors or noncompliance.

The auditor must then determine whether each system identified is significant enough to require documenting an understanding of the EDP controls. This decision should consider factors such as planning materiality, known problems, and significant legal compliance requirements.

When the auditor decides to document the understanding of EDP controls over an application system, both the application and general controls should be considered.

The next section discusses the method of gaining and documenting this understanding.
Section 2. **Gaining an Understanding**

For each application system that is significant to the audit, the auditor must document the understanding of the application controls. These are the control procedures that are specific to each application system. When documenting application controls, the auditor also should document the understanding of the general controls. These are the control procedures that support all the agency's application systems. Together these controls make the system function securely and reliably. To document the EDP controls, do the following:

First, for each application system, document the essential application controls: (a) the primary completeness control, (b) the edits that ensure that transaction postings are in the correct accounts and amounts, (c) maintenance of the data tables used in processing, (d) user access controls, and (e) data backup procedures.

Additionally, if any of the application systems run on personal computers or local area networks, document whether access controls protect the programs and data, and whether backup procedures are appropriate.

Second, for each agency, document whether it has performed a computer security risk assessment, developed an information security plan, and appointed a security officer. Also, document what security software the agency uses to protect its applications and data.

Third, for each systems development group, document the systems development methodology and documentation standards.

Fourth, for each computer center, document whether it restricts physical access to the computer, and has fire and water protection. Also, document whether the computer center has standards for systems software maintenance, standard operating procedures, regular data backup procedures, and a disaster recovery plan.

When documenting these controls, ask when the controls were placed into operation to determine whether the controls were working throughout the audit period.

The auditor should gain an understanding of the application and general controls through interviews and inspection of documentation. Section 7, Forms contains sample forms for documenting the understanding of the EDP controls. The exact form of the documentation is less important than the content. Ordinarily, the financial auditor in charge of the audit should accumulate this information, but the EDP audit staff is available to provide technical assistance as needed.
Section 3. Planning to Test Controls

After documenting the understanding of the EDP control procedures, the auditor must decide which controls to test. This depends upon audit objectives and conditions.

For financial audits, to render an opinion on the statements, the auditor must decide which systems will be relied on to reduce the amount of substantive testing of details required. To rely on a system, the auditor must (a) determine that the design of the application control procedures is adequate, (b) determine that the control procedures were in place throughout the audit period, (c) test the application controls that ensure that the system is functioning reliably, and (d) therefore determine that the application's controls are operating effectively. As a rule, the data completeness, data accuracy, table maintenance, user access, and data backup procedures must all be operating effectively for the system to be reliable.

Alternatively, the auditor may choose to "audit around the system," bypassing the application system and its controls. However, to effectively audit around a system, the auditor must still test the data completeness control to ensure that all the input reaches the output reports, and test the transaction details to ensure that changes which occurred during processing, such as computations, are correct. Auditors will find it difficult to effectively audit around a system when the system processes large volumes of transactions, performs complex computations, leaves no paper-based audit trail, or interfaces with other systems.

Also, the auditor may decide to test some or all the application controls for other reasons. Knowledge of significant problems may require a more thorough examination of the controls. Compliance testing, either driven by the Single Audit Act or other legal requirements, may require testing pertinent application controls. Financial-related audits may include tests of application controls according to audit objectives.

After deciding which application controls will be tested, the financial and EDP audit Managers and Supervisors should have a planning meeting. The auditors should review the documented understanding of EDP controls, the history of audit findings at the agency, planned control testing, and planned data retrieval (see Chapter VIII, Data Retrieval Services).

At the planning meeting, the financial and EDP auditors must decide which general controls should be tested. Whenever the auditor intends to rely on an application system, the general controls that relate to the system should be operating effectively to provide a secure and dependable environment for the application system. At a minimum, when the auditor intends to rely on a system, the information security, program maintenance procedures, and disaster recovery planning should be tested.

Also, the financial and EDP auditors should decide how the control testing will be done. Ordinarily, the financial auditors will do the application testing to better integrate the review of the application controls with other controls over the flow of transactions. EDP auditors will provide technical assistance with areas such as user access control mechanisms. Similarly, the EDP auditors ordinarily do general controls testing because of the specialized knowledge of computer technology requirements. Financial auditors may assist and receive training in performing tests of general controls as circumstances permit.
The planning meeting between the financial and EDP auditors should be documented. The memo describing the meeting should be viewed by both the financial and EDP auditors as an agreement between them.
Section 4. Testing Application Controls

At this point, the auditor has identified all the financial and financial-related application systems at the agency, determined which systems are significant, gained and documented an understanding of the internal control procedures, determined which systems will be relied upon, determined which controls will be tested, and met with the EDP Audit Section to discuss coordination of the work.

As a rule, when the auditor intends to rely on an application system and therefore reduce the amount of substantive testing of details before rendering an opinion on the financial statements, the critical application controls that should be tested are: (a) data completeness, (b) data accuracy, (c) table maintenance, (d) user access, and (e) data backup. Other procedures, such as processing controls, may be added to this list if necessary. Testing of any of the controls may be cycled based on auditor judgment.

Financial auditors have overall responsibility for testing application controls on a financial audit, and EDP auditors are responsible for providing technical assistance as needed. Application controls are either user procedures or programmed procedures. User procedures related to application systems, such as reconciliations, should be tested by financial auditors. Programmed procedures, such as data accuracy edits, consist of internal computer processing and external evidence of their effectiveness. Financial auditors should review the external evidence of the effectiveness of the control, and EDP auditors should provide specialized support whenever the internal computer processing must be examined directly.

The application controls that should be considered critical when the auditor intends to rely on an application system are as follows:

Data Completeness - This is the collection of procedures designed to ensure that users enter each transaction once and only once, that the transactions completely update the databases, and that output reports contain all appropriate data. Common completeness control procedures include batch totalling and reconciliations. Testing this control is very similar to the audit procedures used when auditing around the computer. If this control is functioning effectively, we have strong support for the completeness assertion from the point at which data enters the system through to the output reports.

Data Accuracy - These are the controls to ensure that users enter the most important data elements correctly, and the system keeps them correct. Ordinarily, account numbers and amounts are the most critical data elements entered. Controls over the accuracy of account numbers include table lookups, check digits and visual verification. Controls over the accuracy of amounts include batch totals and rekeying for verification. If these controls are functioning effectively, we have strong support for the valuation and occurrence assertions.
Table Maintenance - These are controls to ensure that tables used in financial computations, such as the conversion from item counts to prices, include correct and timely values. These tables should be updated only by authorized user department personnel. When updated, an audit trail should be created and reviewed. Tables should be independent of computer programs and programmers. If these controls are functioning effectively, we have strong support for the valuation assertion.

User Access - This control ensures that only authorized persons can record, change or delete data, and that electronic signatures used to approve transactions are valid. Testing this control involves making sure the security software is working correctly, and the security rules reflect management's intentions and provide appropriate separation of duties. Testing this control is usually a joint effort by financial and EDP auditors. If this control is functioning effectively, we have strong support for the existence and occurrence assertion.

Data Backup - This control ensures that the system can be restored if a disaster destroys the primary data files. To be effective, the backup data files must be stored in a secure offsite location, and all essential files should be included. The frequency of the backup will determine the amount the data that must be reentered since all data entered between the last backup and the disaster must be recaptured. If this control is not functioning effectively, all assertions are jeopardized.

The auditor should determine whether the design of the critical application controls supports management's financial statement assertions and the controls are functioning effectively. In doing this, the auditor should integrate tests of application controls with other controls within the appropriate audit area.

Chapter II, Reviewing Application Systems presents detailed guidance on testing application systems. Chapter III, Reviewing Personal Computers and Local Area Networks presents additional guidance on testing personal computers and local area networks.
Section 5. Testing General Controls

Whenever the financial auditor plans to rely on an application system and tests the operational effectiveness of the application controls, certain critical general controls also should be tested to ensure that the application systems run in an environment that is secure and reliable.

As a rule, EDP auditors have overall responsibility for testing the general controls because these tests often require the use of technical specialists. Financial auditors may participate in testing the general controls to get training and gain experience. EDP auditors are also responsible for communicating the results of the general controls testwork to the financial auditors so that they can make any necessary adjustments in the nature and timing of their work. Financial auditors are ultimately responsible for integrating the results of the general controls tests into the overall audit effort.

The general controls that should be considered critical and tested whenever the auditor intends to rely on an application system are as follows:

Information Security - This group of controls protects the stored data and programs from unauthorized change, use or destruction. Testing these controls involves evaluation of the security software, consideration of the organizational structure of the information processing and user departments, and examination of the access authorizations of groups and individuals to various computer files. Unless this control is functioning effectively, any or all the assertions may be false.

Program Maintenance Procedures - These controls help ensure that changes to computer programs are authorized, reviewed, and tested. Unless these controls are strong, systematic errors and irregularities can become part of the production version of the application system. Unless this control is functioning effectively, any or all the assertions may be false.

Disaster Recovery Planning - This control provides the means to resume information processing if a disaster destroys the computer center. The plans should provide for offsite storage of backup files and the replacement of the computer facility, equipment, telecommunications connections, and supplies if needed. Assignments should be made in advance so that recovery efforts are well coordinated. Unless this control is functioning effectively, the organization may be put out of business by a disaster.

The auditor should determine whether the critical general EDP controls are adequate to protect the integrity of the programs and data from unauthorized alteration, use or destruction, and to ensure that critical application systems can process if a disaster occurs.

When testing the general controls, the auditor should construct a work program that includes the specific audit objectives and procedures needed to achieve this overall objective. Detailed guidance on testing general controls will be found in Chapter IV, Reviewing Information Security; Chapter V, Reviewing Systems Development and Maintenance; and Chapter VI, Reviewing Computer Service Centers.
Section 6. Communicating Findings and Recommendations

During the audit, the auditor may become aware of deficiencies in the design or operation of the internal control structure which could adversely affect the organization's ability to record, process, summarize and report financial data. The auditor has a responsibility to communicate these findings to the financial audit supervisor and manager to be included in the audit reports that the office issues. For the audits conducted at SIPS, AOC, and any other general controls or application controls audit conducted which is not directly associated with a financial, financially related, or performance audit, a separate report will be issued following the Yellow Book standards.

When communicating weaknesses in EDP controls, the auditor should attempt to convey the problem to the reader with clarity and simplicity. We usually begin our management comments with a simple, straight-forward statement of the problem. We explain the problem as much as necessary for the reader to understand the extent and significance of the finding. When we can identify the cause of the problem, we discuss it as well. Finally, we recommend corrective action that the agency should take to remedy the problem.

Management comments concerning EDP controls should be free of computer jargon and acronyms as much as possible. Both jargon and acronyms confuse the reader, making the communication ineffective. We must be careful to avoid using such words unless clearly explained.

Our recommendations should be practical, cost beneficial, and realistic given the level of technological expertise at the agency. Also, our recommendations should be consistent among the agencies.
Section 7. **Forms**

This section contains sample forms which can be used to document our understanding of internal controls as discussed in Section 2, **Gaining an Understanding**.
Application System Understanding

Name of entity: ________________________________________________________________

Name and description of application system:
    _______________________________________________________________________
    _______________________________________________________________________

Accounts affected by the application system:
    _______________________________________________________________________
    _______________________________________________________________________

User manager and department responsible for the system and data:
    _______________________________________________________________________

Has the system been changed since last year?
    _______________________________________________________________________

Developed by: _______________________________________________________________________
    Vendor ____________ In-house unit ____________

Maintained by: _______________________________________________________________________
    Vendor ____________ In-house unit ____________

Runs on which computer(s)? _______________________________________________________________________

System features (check all that apply):

Large data volume _________ Electronic signature approvals _________
Complex computations _________ Interfaces with other systems _________
Eliminates paper trail _________ Interfaces with general public _________
How is data completeness through the system assured?

_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

How is the accuracy of important data elements like account numbers and amounts assured?

_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

How are tables used in financial calculations maintained?

_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

How is access restricted to system functions?

_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

What are the provisions for data backup?

_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

Other notes:

_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

Completed by: _____________________________ Date: ______________
Information Security Understanding

Name of entity: __________________________________________________________

Has the agency performed a risk assessment?
_______________________________________________________________________

Has the agency identified its critical applications and sensitive information? If yes, describe.
_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

Has the agency developed an information security plan?
_______________________________________________________________________

Has the agency appointed an information security officer?
_______________________________________________________________________

Name, job title and phone number of agency security officer:
_______________________________________________________________________
_______________________________________________________________________

Names of security software products used by the agency:
_______________________________________________________________________
_______________________________________________________________________
_______________________________________________________________________

Completed by: ___________________________ Date: _________________________
Name of entity: __________________________________________________________

Manager and name of the systems development and maintenance group:

_______________________________________________________________________
_______________________________________________________________________

Group is responsible for which systems?

_______________________________________________________________________
_______________________________________________________________________

Does the agency have a systems development methodology and documentation standards that it uses on its projects? Explain.

_______________________________________________________________________
_______________________________________________________________________

Does the agency have application maintenance standards that it uses to make program changes? Explain.

_______________________________________________________________________
_______________________________________________________________________

Completed by: ___________________________ Date: ________________
Computer Center Understanding

Name of entity: __________________________________________________________

Location of computer center: ____________________________________________________

Computer make and model: ____________________________________________________
  Operating system: ____________________________________________________
  Security software: ____________________________________________________

Methods used to restrict physical access:
_______________________________________________________________________
_______________________________________________________________________

Methods used to prevent fire and water damage:
_______________________________________________________________________
_______________________________________________________________________

Does the center have standards for systems software maintenance? Explain.
_______________________________________________________________________
_______________________________________________________________________

Does the center have standard operating procedures including periodic data backup? Explain.
_______________________________________________________________________
_______________________________________________________________________

Does the center have a disaster recovery plan? Explain.
_______________________________________________________________________
_______________________________________________________________________

Completed by: ________________________________ Date: ___________________________