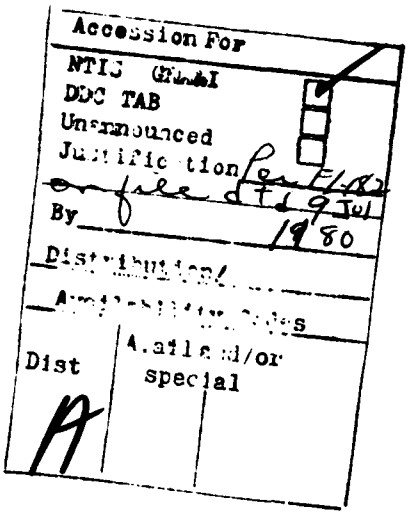
AD-A086 954 YOUNG (ARTHUR) AND CO WASHINGTON DC F/G 5/1
RESEARCH ON INTERNAL CONTROLS AND AUDITING. NAVY FINANCIAL MANA--ETC(U)
JUN 80 N00014-79-C-0935
UNCLASSIFIED NL


END
DATE FILMED
9-80
DTIC

AD86953

VOLUME II

TABLE OF CONTENTS



N00014 79 C 0935

I. INTRODUCTION

The purpose of this volume is to present the results of our research regarding the impact of the distributed system environment on internal controls. The discussion in this volume addresses general EDP procedures (e.g. environmental controls). General EDP procedures are concerned with overall organization, policies, procedures and controls which are common to all EDP applications. Because of the interrelated nature of application controls and the auditor's evaluation of internal controls, application controls will be considered in Task 4 of this project.

1. RESEARCH APPROACH-OVERVIEW OF VOLUME 2

To develop the proper framework for analysis, this chapter first introduces the characteristics which may be found in a distributed environment as well as general and specific procedures normally associated with a good system of internal control. This framework provides the basis for the analysis performed in Chapter II.

In Chapter II, the potential characteristics of distributed systems are compared to commonly applied general internal control procedures. The analysis performed in Chapter II then describes the impact which the specific distributed system characteristic is likely to have on the general internal control procedures. Chapter II continues with a discussion of specific internal control procedures which are particularly suited to a distributed system environment and concludes with a discussion of the impact of distributed systems on audit procedures.

Finally, Chapter III summarizes our major observations and

conclusions regarding the impact of distributed systems and presents our recommendations to ensure the implementation of adequate internal controls in a distributed system environment.

2. ANALYTICAL FRAMEWORK

To meet our research objectives, it is necessary to first view the distributed environment and internal controls in isolation.

At the outset, it is important to note that there are no commonly accepted definitions of distributed processing or distributed systems and we have not attempted to develop formal definitions. Instead, we have identified the potential characteristics of distributed systems to created a model of distributed systems in the broadest sense.

The objectives of internal control (e.g. safeguarding assets, fairness of presentation, etc.) do not change with the use of distributed systems. Our analysis framework is not concerned with objectives that remain unchanged, but with general and specific procedures which are likely to be affected by distributed systems.

The two research variables (distributed systems and general internal controls) form the framework for analysis. The remainder of this chapter defines this framework.

3. DISTRIBUTED SYSTEM CHARACTERISITCS

As previously noted, there is no consensus on the definition of distributed systems. At one extreme, any degree of decentralization (including simple remote inquiry capability) has been labeled distributed processing while at the other extreme only those configurations providing for full processing capability at each node within the system's network are classified as distributed systems. A further complexity is added by the alternatives available in the

distribution of data bases (e.g., centralized, distributed, duplicated, etc.). Finally, alternatives also exist in determining the system's communication form and network configuration.

However, determining which of the numerous possibilities regarding processing power, data distribution and communication networks (and related combinations and permutations) constitute distributed processing is not necessary for our research project. Our approach does not seek to define distributed systems, but rather identify the salient characteristics of the distributed environment to determine the impact of these characteristics on internal controls.

In analyzing distributed systems, there are three major areas of concern: distributed functions and processes, data distribution, and communications networks. Our analytical framework addresses each of these areas individually.

(1) Functions and Processes

The characteristic most commonly associated with distributed systems is processing. In many respects increasing EDP efficiency by bringing the "processing power" closer to the user has become the by-word of distributed systems. The term distributed processing has been applied to a number of distribution possibilities, including remote data input and inquiry capabilities, which are often not processing functions nor are they (in the absence of other attributes) characteristics of a distributed system. For the sake of simplicity and in keeping with our broad objective surrounding the identification of distributed systems, we have included commonly distributed functions and processes in this discussion without determining at what point the system may be considered a distributed system.

Under the distributed concept, each of the traditional EDP

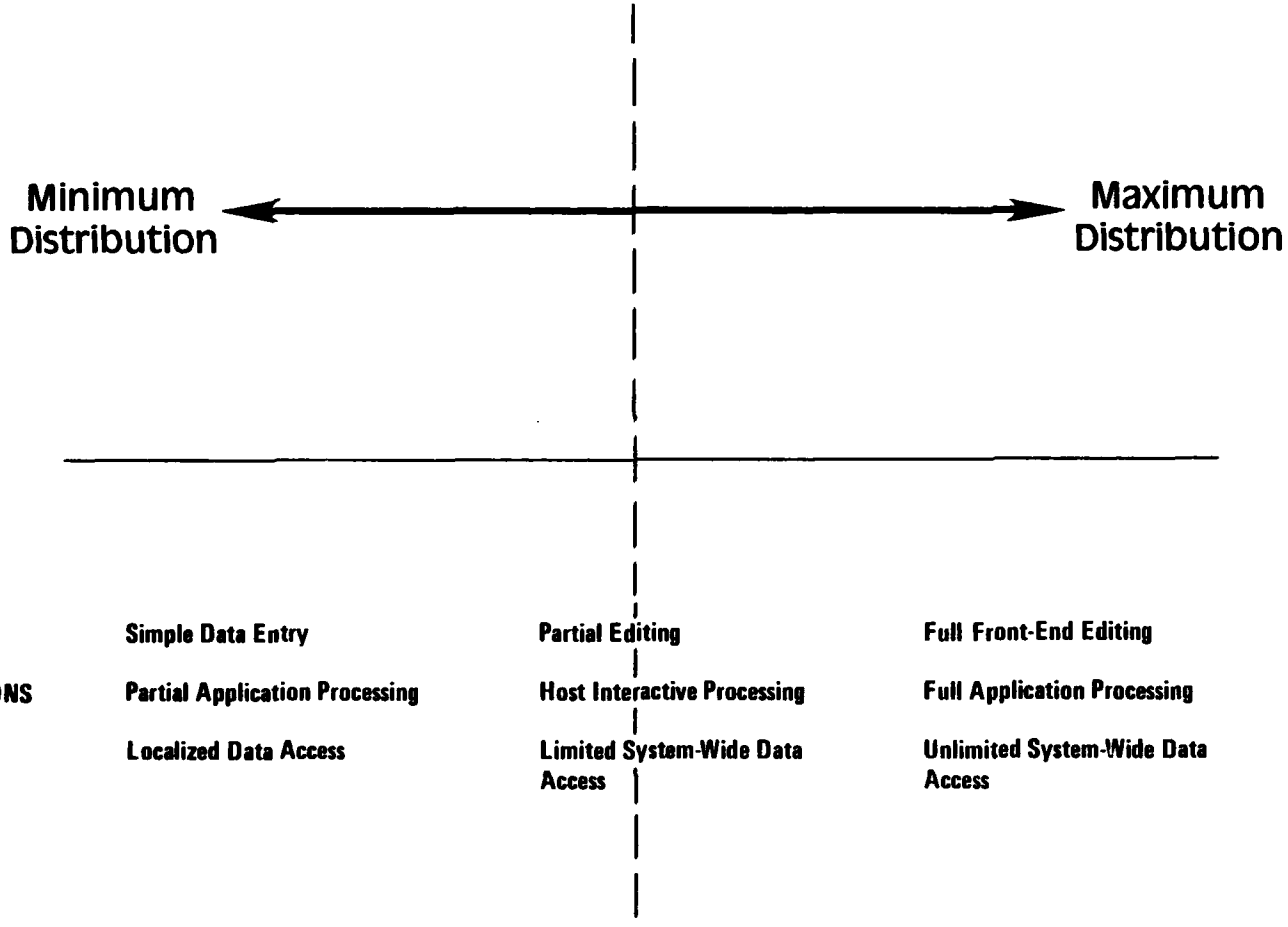
functions (input, processing, output) may be distributed (in varying degrees) at each system node. The distribution of functions is best viewed as a continuum where different degrees of distribution are possible. Exhibit I-1 graphically depicts the distribution continuum for the traditional input/processing/output functions. It is not always practical to define distributed functions and processes in terms of input, processing and output because functions: often overlap (e.g., is full front end editing an input or a processing function?); are combined at a node (e.g., combined input and processing functions); or are distributed in different degrees throughout the network (e.g., input terminals linked to a processor with front end editing capability which is in turn linked to a host processor, etc.).

The potential attributes are discussed below following the traditional input/processing/output flow. However, it is important to note that input and output functions usually involve processing, and that the data flow technique is used only to facilitate our presentation of these attributes.

- Simple Data Entry

  Simple data entry, as used in this report, refers to the decentralization of the input function (e.g. keypunching function transferred to the user) with no front-end data editing. Simple data entry by itself does not constitute distributed processing. However, it is not unusual to find a series of data entry terminals linked to a processing device (constituting a node) which itself has some of the more advanced processing characteristics associated with distributed systems.

Potential Distribution of Functions and Processes



INPUT FUNCTIONS	Simple Data Entry	Partial Editing	Full Front-End Editing
PROCESSING FUNCTIONS	Partial Application Processing	Host Interactive Processing	Full Application Processing
OUTPUT FUNCTIONS	Localized Data Access	Limited System-Wide Data Access	Unlimited System-Wide Data Access

EXHIBIT I-1

- Partial Editing

  Under partial editing, input data is subjected to a variety of checks (e.g. reasonableness tests, control totals, etc.), before input is accepted.

- Full Front End Editing

  This characteristic requires the application of full input processing including, depending on the application, system access to data files to perform input validity checks as necessary.

- Partial Application Processing

  In its broadest form, any type of front end editing constitutes partial application processing. However, for purposes of this discussion, this characteristic assumes a substantial amount of front end editing and the performance of additional processing (e.g., identification of required allotment deductions in a payroll system) at tne distributed site, prior to data pass-through to a host processor where the application is completed.

- Host Interactive Processing

  In host interactive processing, a substantial amount of the processing function takes place at the distributed location with only a limited requirement for host assistance (usually as a result of security, processing sophistication or centralized data sharing requirements).

- Full Application Processing

  In these instances, the entire application is processed at the node with no host intervention.

- Output Processing (Data Retrieval and Manipulation)

  Most of the functions discussed earlier involve the generation of output ranging from error messages (as a result of the front end edit function) to report generation as a by-product of application processing. In addition, inquiry type capabilities may be present involving either simple data extraction or data extraction and manipulation.

  As a general rule, inquiry capability will be limited to data available to a localized data base, and/or limited access to remote data bases. This limitation is due mostly to the technical difficulties inherent in achieving the high degree of communication required between nodes and host (or hosts) to provide system-wide data access at a node. In addition, this capability would require the node processor to provide the same range of services (e.g., security, manipulation, etc.) available in the more sophisticated processors usually associated with the host. This requirement would limit or even nullify the cost advantages available in a distributed system. Nevertheless, system-wide data access and manipulation capability at a node is still a possibility (particularly in the future) and should be considered by this project. For analysis purposes, we have identified the following data retrieval and manipulation characteristics:

  - Localized data access (and manipulation)

- Limited system-wide data access (and manipulation)

- Unlimited system-wide data access (and manipulation).

Needless to say, the type of access is affected by the extent of data bases and files distributed. This subject will be discussed next.

(2) Data Distribution

Closely related to the concept of "bringing processing power closer to the user" is the concept of bringing the user data closer to the user. In the prior section, we discussed briefly the difficulties and cost of accessing data not locally available. Under the distributed concept, an attempt is made to place the data as close as possible to the processes (including inquiry or output processing) that require it.

Invariably, any attempt to distribute data in this fashion runs into contradictory requirements with some requirements calling for distribution (e.g., quick inquiry response) while others call for centralization (e.g., data sharing). As a result, the distribution of data in any given system is not consistent for all data elements or groups of data elements. That is, depending on data use requirements, certain data elements will be stored centrally, others will be distributed at the user location, while still others will be replicated at different locations (including centrally). Common data distribution patterns are presented in Exhibit I-2.

(3) Communications Network

A final consideration in distributed systems is the communications network. The communications network refers to

Common Data Distribution Patterns

- Centralized Data

  Centralized data refers to data elements which are located at a central site. As a general rule, these data bases or files will contain data elements which are shared by multiple locations.

- Partitioned Data

  Partitioned data refers to the creation of independent data bases or files at the location or system node. As a general rule, these data bases or files consist of data elements unique to specific functions located at a system's node.

- Replicated Data

  Replicated data refers to the physical duplication and location of data elements at different locations. Data replication is commonly used in conjunction with centralized and partitioned data.

inter-processor communications between nodes, and between a node and a host processor or host system. The areas to be considered are the communications requirements and the network configuration.

Communication requirements may take one of two forms:

- One-Way Communication

  This requirement, often referred to as hierarchical communication, consists of a one-way flow (from node to host processor) of communications requests answered by a one-way flow (from host processor to node) of communication responses.

- Two-Way Communication

  This requirement, often referred to as peer communications, provides for a two-way flow of inquiries and responses regardless of the node/host processor relationships.

Network configurations are not as easily defined and it can even be argued that each existing distributed system has a unique configuration. There are, however, certain traditional configurations which cover the different network configuration alternatives. These configurations are graphically depicted in Exhibit I-3.

4. GENERAL INTERNAL CONTROL PROCEDURES

The second variable in our framework relates to the general internal control procedures commonly associated with a good system of internal controls. Our main objective is to identify these procedures to determine their applicability in a distributed environment (see Chapter II).

Potential Network Configurations

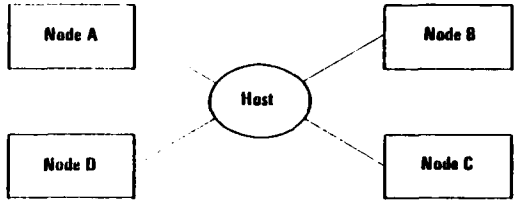
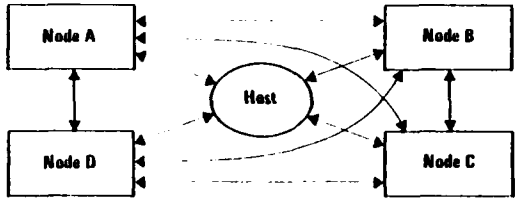
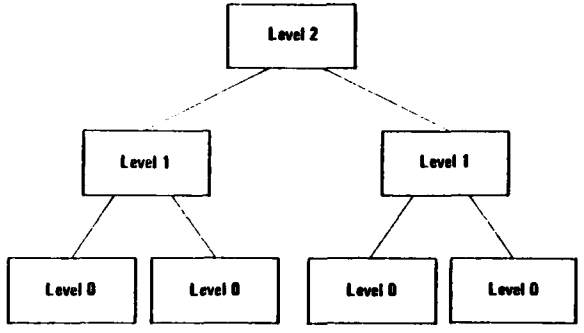
Configuration	Definition	Graphic Representation
Star Configurations	Under this configuration, there are no communications between nodes, and all nodes communicate with a central host processor.	
Multi-System Network	Under this configuration, communications are permitted between nodes as well as between the nodes and host processors in the network.	
Hierarchical Networks	As indicated by the title, this configuration provides for organizational levels within a network. Typically, the lowest level nodes are connected to a host processor while the host processor and other similar host processors in the network are in turn connected to a higher level processor. This processor may be either the highest level processor in the network or, in the more complex systems, connected to an even higher level processor.	
Job Network	In this type of configuration the system consists of a series of interconnected processors with no hierarchical relationship. One processor must assume scheduling responsibilities for the system, but all processors have similar capabilities.	

EXHIBIT I-3

Traditionally, general internal controls may be subdivided into three general areas: 1) organization and administration, 2) operations and 3) systems development and maintenance. This section identifies the traditional general internal control requirements of each internal control area.

- Organization and Administration

  Organizational and administrative controls address segregation of duties, contingency procedures and the librarian function. Traditional internal control requirements associated with organization and administration are summarized in Exhibit I-4.

- Operations

  Operations controls are designed to provide reasonable assurance as to the accuracy and completeness of operating results, prevent or detect errors which occur during processing, and provide security against accidental or deliberate destruction of data processing assets. Traditional internal controls associated with computer operations are presented in Exhibit I-5.

- System Development and Maintenance

  System development and maintenance controls are required to ensure the effectiveness of EDP systems. Controls must be developed to ensure that processing objectives and functions are explicitly defined and approved to properly control system development and implementation, program changes, and system maintenance requirements. Specific procedures are listed in Exhibit I-6.

Organization and Administration Controls

A. Segregation of Duties

Procedural requirements resulting in adequate segregation of duties include:

- Operators are prohibited from programming
- Operators and/or data entry personnel are not allowed to make corrections to erroneous source input data
- Programmers and/or systems analysts are not permitted to operate the computer without supervision and control
- The scheduling and control function is performed by other than operators
- The library function is independent of operations and programming
- Limited access to EDP facility.

B. Contingency Procedures

Conditions indicative of satisfactory contingency procedures include:

Organization and Administration Controls

- Formal (written) contingency plan
- Adequate insurance coverage
- Alternative processing and backup and recovery capability
- Offsite storage of all critical material (e.g., master files, transaction files, operating systems, source programs, etc.)

C. Librarian Function

An adequate librarian function will provide for the following:

- Formal (written) file retention procedures
- Segregation of systems/programming/operating functions from librarian function
- Adequate control over access to:
  - Application data files
  - System software
  - Production programs and job control
  - Source programs
  - Documentation

Organization and Administration Controls

D. Other

Other practices and procedures indicative of satisfactory internal controls include:

- The existence of a policy or steering committee to ensure that EDP practices satisfy and are consistent with the entity's objectives

- Formal, short (less than 1 year) and long (1 to 5 years) term plans to ensure the effectiveness, efficiency and responsiveness of the EDP function in the face of the entity's changing environment

- Competent personnel.

Operations Controls

A. Scheduling

Scheduling procedures should include:

- Job set-up instructions
- Logging jobs in and out
- Provisions for controlling computer workload
- Assurances that all jobs processed are authorized.

B. Processing Procedures

Processing Procedures should include:

- Requirement for authorization of production schedule changes
- Formal procedures for documenting schedule changes

C. Access Controls

Access controls should include:

- Restriction of physical access to computer room
- Physical segregation of operations and control personnel

Operations Controls

- Consistent supervision of all operating shifts
- Adequate terminal controls which include the following:
  - Terminal located in serviced area
  - Terminal identification
  - Operator validations
  - Logging of security violations
  - Audit trails and recovery procedures
  - Authorization of program modifications made through terminals.

Systems Development and Maintenance Controls

A. System Development and Implementation

Development standards should include:

- Adequate analysis and design
- Program development and testing procedures
- User coordination and acceptance procedures
- Documentation requirements including:
  - System specifications
  - Individual programs
  - Operating and control instructions
  - User processing and control instructions

B. Production Program Controls

Procedures should provide for separate program libraries for the development, testing and production stages.

Systems Development and Maintenance Controls

C. Program Change Controls

Program Change Procedures should include:

- Formal controls over authorization testing and implementation of system and program changes
- Change requests originated by user and approved by DP management
- Formal testing requirements
- Requirements for updating documentation
- Methods for detecting unauthorized changes
- Operations group acceptance for changes only after approval.

5. APPLICATION OF THE ANALYTICAL FRAMEWORK

The purpose of this chapter was to establish the framework for the analysis performed in Chapter II. We have identified the characteristics which may be found in a distributed environment and the overall organizational, policy, and procedural controls which are common to general EDP internal controls. In the next chapter we describe the impact each distributed system characteristic is likely to have on the general internal controls. This analysis is then continued with a discussion of specific internal control procedures which are most effective in a distributed environement and concludes with a discussion of the impact of this new technology on audit procedures.

II. IMPACT OF DISTRIBUTED SYSTEMS ON GENERAL INTERNAL CONTROLS

As noted earlier, Chapter I identified and defined the variables (i.e. distributed systems and general internal controls) making up the framework for our impact analysis. This chapter presents the results of our analytical effort.

In general, we have concluded that distributed systems have a very significant impact on traditional internal control procedures. In many instances, distributed systems will render certain traditional controls either inapplicable or cost prohibitive while in others, the impact is expressed in terms of increased system risk (if internal controls are not present or not complied with). Further, each application is likely to be affected differently by the characteristics of distributed systems. However, the impact is not always adverse and distributed system characteristics can often be effectively utilized to improve both operating efficiency and internal controls.

Regardless of the adverse or positive nature of the impact, it is clear that new procedures will have to be developed to ensure the adequacy of internal controls and that the new environment and emerging internal control procedures will in turn have a profound impact on the auditor.

This chapter presents our methodology in determining the impact of distributing systems and addresses each of the points made in this introductory discussion in the following sections:

- Analysis of Distributed Systems and General Internal Controls

- Impact of Distributed Applications on General Internal Controls
- Developing Compatible General Internal Control Procedures
- Impact of Distributed Systems on Audit Procedures.

1. ANALYSIS OF DISTRIBUTED SYSTEMS AND GENERAL INTERNAL CONTROLS

The purpose of this section is to synthesize the characteristics of the distributed system environment with commonly applied internal control procedures to determine the continuing viability or obsolescence of these common internal control procedures. To illustrate our approach, this section includes a series of matrices (discussed in more detail in each subsection) that compare specific distributed system characteristics to traditional internal control procedures.

The analysis performed in this section and in Section 2 (Impact of Distributed Applications on General Internal Controls) in turn, form the basis for our discussion regarding the development of compatible general internal control procedures (Section 3 of this chapter) and audit procedures (Section 4 of this chapter).

Our analysis is presented under these general topics:

- Distributed Functions and Processes
- Data Distribution
- Communications Network.

(1) Distributed Functions and Processes

Our analysis indicates that the different characteristics and attributes of distributed functions and processes will have an impact on many of the specific procedures associated with traditional internal controls. In general, potential impacts may be summarized as follows:

- The traditional internal control procedure is just as applicable (and practical) in a distributed system
- The distributed system reduces the effectiveness of the internal control procedure
- The distributed system renders the internal control procedure obsolete (or impractical)
- The distributed system offers new internal control alternatives
- The distributed system must place additional reliance on the internal control procedure (either as a result of specific system attributes or to offset other procedures that are not practical).

Our analysis of internal controls and distributed functions and processes is presented in Exhibits II-1 through II-6 at the end of this section.

A brief discussion of the results of our analysis is presented in the following pages:

- Organization and Administration (See Exhibits II-1, II-2 and II-3 at the end of this section)

Traditionally, effective organizational and administrative controls have relied on a large centralized EDP function requiring a large staff. As a result, the imposition of formal segregation of duties and other restrictions upon the EDP function did not hinder operating efficiency or unreasonably increase operating costs. However, the decentralization of functions and processes often results in the creation of "mini-EDP activities" where the formal segregation of duties usually present in an EDP operation may no longer be cost justifiable and in many instances may run contrary to the operating efficiency which the distributed system is attempting to achieve (e.g., bringing processing power closer to the user often implies increased user control and thus less segregation of duties). On the other hand, the distribution of the EDP function, by spreading the risk of catastrophe, creates a different environment in the area of contingency procedures. A final area of concern is the quality and experience of personnel responsible for EDP functions. Except for the distribution of major applications, a distributed system will not always be supported by experienced EDP personnel at each location. This is particularly true in user oriented functions, where the user personnel may be responsible for several non-EDP, as well as EDP functions and processes.

Overall, the major impacts disclosed by our analysis are:

- Segregation of duties may be harder to achieve (particularly when EDP functions reside with the user)

- Less experienced personnel are likely to be present in a distributed environment (at each location)

- Self-insurance may be facilitated in a distributed environment

- The distribution of functions tends to reduce the "total system catastrophe" risk

- The distribution of functions results in a data communications network which must be controlled independently of functions performed at each system node

- General guidance (e.g., user manuals, EDP standards) becomes more critical as there is a greater need to coordinate the activities of multiple locations.

. Operations (See Exhibit II-4 at the end of this section)

Control over operations revolve around scheduling, processing and access control procedures. Again, practical size limitations are a major constraint which affect the system's ability to achieve proper segregation of duties. In addition, the distribution of functions increases the need for coordination both in terms of sequential operating requirements as well as system-wide procedural changes. Finally, the distribution of functions and processes tends to increase the risk of unauthorized access while restricting the system's ability (from a cost-benefit point of view) to fully segregate and secure system hardware.

Overall, the major impacts disclosed by our analysis are:

- Loss of centralized control over scheduling to:

  .. Meet sequential file update requirements

.. Prevent concurrent file updates

.. Control total system CPU workloads.

- Increased need for coordination to:

  .. Offset lack of centralized control over scheduling

  .. Ensure the system-wide applicability and adaptability of procedural changes.

- Increased emphasis (and reliance) on the development of system-wide standards and guidance to meet the increased coordination requirements discussed above.

- Increased risk of unauthorized access through:

  .. The potential proliferation of system access devices (e.g. terminals)

  .. The impracticality in many instances (from a cost-benefit point of view) of fully secured facilities.

- Increased reliance on system design to prevent unauthorized access including:

  .. Provision for ID codes, passwords, etc.

  .. Design limitations restricting each system device and/or node to the bare minimums (e.g. limited input, access, update, etc. capability) required to fulfill the requirements of the specific function or process.

- System Development and Maintenance (See Exhibits II-5 and II-6 at the end of this section)

  System development and maintenance procedures are designed to ensure the adequacy of systems development/implementation efforts and properly control the system's programs. In general, the decentralization of the EDP function creates a series of interdependencies which complicates and taxes the EDP function's ability to develop adequate internal controls. The result is an added reliance on system-wide standards and guidance to offset the loss in centralized controls.

  Overall, the major impacts disclosed by our analysis are:

  - System development standards must emphasize a design approach that is cognizant of both specific functions/process/node needs as well as total system requirements

  - The interdependencies created by the distribution of processing functions complicate the program development process and increases the criticality of testing procedures

  - A major justification for distributed processing is providing better service to the user. Under these circumstances, it is clear that user involvement in systems development and user oriented documentation are essential

  - Traditional controls over program changes remain in effect and the need for control over these changes is even more critical given the potential increase for

unauthorized system access in a distributed environment.

- Summary Analysis of Distributed Functions and Processes

Exhibits II-1 through II-6 which summarize our analyses of distributed functions and processes and general internal controls are presented in the following pages. The columns shown in the exhibits list the different functions and processes which can be distributed as discussed in Chapter I of this volume. The rows of the exhibits show each of the traditional major areas of general internal control (i.e., Organization and Administration, Operations, and Systems Development and Maintenance). In addition, for each major area, the exhibits identify specific procedures which are indicative of adequate internal controls. The list of specific procedures is not an exhaustive one, but rather represents some of the most significant procedures which are traditionally (e.g., in a centralized environment) associated with good internal controls. The matrix itself, discusses the applicability of traditional procedures, conditions which are likely to change, and minimum control requirements which should be present given the specific distribution of functions and processing alternatives.

INTERNAL CONTROL REQUIREMENTS	POTENTIAL DISTRIBUT		
	SIMPLE DATA ENTRY	PARTIAL EDITING	FRONT END EDITING
A. Segregation of Duties **1. Operators are Prohibited from Programming**	No impact. As a general rule, the distribution of input responsibility is not accompanied by distribution of programming (including editing capability). Responsibility for edit programs (if any) should be segregated. If partial or full edit programming responsibilities reside with the user, the input and edit programming responsibilities should be segregated.		
2. Operations and/or Data Entry Personnel are not Allowed to Make Corrections to Erroneous Source Input Data	Data entry personnel will often be users. The main purpose of this control is to prevent uninformed keypunchers from making corrections. If the user has a good understanding of the application, this control can be waived. Data entry personnel should be familiar with the application. In addition, proper authorization and approval of data entry should continue to be observed. Segregation of data entry and output control review should continue. User access to system should be restricted.		
3. Programmers/System Analysts not Permitted to Operate Computer Without Supervision	As a general rule the distribution of input responsibility is not accompanied by the distribution of programming or systems development responsibilities. Responsibility for edit programming (if any) should be segregated. If partial or full edit programming responsiblities reside with the user, programming/system responsibilities should be segregated from computer operations.		
4. Scheduling and Control Function not Performed by Operators	In general, this procedure controls the processing function, not the input function. However, data entry personnel should similarly not be responsible for the scheduling and control function.		
5. The Library Function is Independent of Scheduling and Programming	This requirement should have no impact on input related functions. Again, data entry personnel should be independent of the librarian function.		
6. Limited Access to EDP Facilities	Except for major data input operations (e.g., multiple data entry terminals) fully secured locked facilities may not be cost justified. Access to input devices should be controlled. If separate facilities are not practical, terminal locks (in addition to password requirements) should be installed.		

General EDP Procedures

EXHIBIT II-1

ibuted Systems on Internal Controls

nization and Administration

POTENTIAL DISTRIBUTED SYSTEM CHARACTERISTICS: FUNCTIONS AND PROCESSES				
END EDITING	PARTIAL APPLICATION PROCESSING	HOST INTERACTIVE PROCESSING	FULL APPLICATION PROCESSING	OUTPUT PROCESSING (DATA RETRIEVAL/MANIPULATION)
lity is not lity).	No Impact. Partial processing normally requires standard centrally controlled programs throughout the network.	In many instances programming responsiblity will be distributed and may reside with the user.		Data retrieval and manipulation capability is user oriented. Specific programs will often be user responsibility.
partial or ut and edit	If programming responsibility resides with the user, operations and programming should be segregated. Centrally controlled programming and operations should continue to be segregated.	Operating and Programming responsibility at the distributed site should continue to be segregated.		Segregation of duties requirements will depend on nature of application and specific output use.
ntrol is to has a good	Data entry personnel impact the same as for input oriented functions. In addition, depending on the size of the application, full processing responsibility (including equipment operation) may reside with the user.			Same impact as input and processing oriented functions.
tion, proper observed. User access	Data entry personnel requirements the same as for input function. If processing operation is large enough, equipment operation responsibility should not reside with user. In small applications where user has processing responsibilities, the equipment operation function should be segregated from all other user functions.			Same requirements as for input and processing functions.
accompanied ilities.	No Impact. Partial processing normally requires standard central control of programs throughout the network.	In many instances programming/systems responsibility will be distributed and may reside with the user.		Data retrieval/ manipulation capability will often be a user responsibility.
If partial ming/system	If programming/systems responsibility resides with the user, these responsiblities should be segregated from operations. Centralized activities should continue to be segregated.	Programming/system responsibility at the distributed site should continue to be segregated. Except for small applications; systems (and when feasible programming) should be segregated from the user.		Segregation of duties requirements will depend on nature of application and specific output use.
ut function. le for the	Depending on the size of the application full processing responsibility (including scheduling and control) may reside with the user. If processing operation is large enough, scheduling and control responsibility should not reside with the user. In smaller applications where user has processing responsibilities, scheduling and control should be a supervisory level responsibility.			
Again, data	Library function and scheduling will be distributed. Programming will usually be centralized. Organization size may prevent full segregation.	Library and scheduling functions will be distributed. In many instances programming responsibility will be distributed. All of these functions may reside with the user.		Same potential impact as for processing oriented functions.
	Subject to size constraints, these controls should be observed.	At a minimum, the programming and library functions should be segregated. Depending on size constraints, the library and scheduling function should also be segregated. (Requirements apply regardless of extent of user control over these functions.)		Same requirements as for processing oriented functions.
inals) fully	Depending on the size of the operation, fully secured EDP facilities may not be feasible.			Same impact as for input and processing functions.
les are not should be	At a minimum, physically segregated (e.g., separate rooms under lock and key) should always be present.			Same requirements as for input and processing functions.

Impact of Distribu

I. Organiz

INTERNAL CONTROL REQUIREMENTS	POTE		
	SIMPLE DATA ENTRY	PARTIAL EDITING	FRONT END EDI
B. Contingency Procedures **1. Contingency Plan Should be Formalized (Written)**	The distribution of these functions will often require a separate contin plan at each location. Central guidance should be provided for contingency planning. However, d distribution the lack of formal contingency planning at any specific loc is not as risky (depending on specific application).		
2. Contingency Plan Should Include Adequate Insurance Coverage	Multiple sites and input devices may justify a self-insurance policy. Central guidance should be provided for contingency planning. However, d distribution the lack of formal contingency planning at any specific loc is not as risky (depending on specific application).		
3. Contingency Plans Should Include Backup and Recovery and Alternative Processing Capability	Alternative processing capability is not a major issue. Lacking formal arrangements for alternative processing capability, the contingency plan should identify procedures to be followed if existing input capability is lost.	Contracts or agreements providing for al processing capability are critical unless com equipment is readily available in the dist location's geographical area. In the absence of proximity to other distribute (with compatible equipment and applications), arrangements for alternative processing is t internal control procedure.	
4. All Critical Material Should be Stored Offsite	No significant impact on simple data entry operations.	No significant impact. Transaction files will be on to a processing function. Edit progra normally be standard system-wide programs. To the extent that edit program files are s throughout the system, no offsite storage is ne (unless replacement is likely to cause serious Location unique edit programs require offsite s	
C. Librarian Function **1. File Retention Procedures Should be Formalized (Written)**	Transaction files will be passed on to a processing function. Only likely documentation is hardcopy input run and/or source data. Centrally developed guidance should be issued for source data and hardcopy input retention policy.	Edit programs likely to be system-wide standar impact on transaction files and related docum for simple data entry. Centrally developed guidance should be prese source data, hardcopy input, and edit program fi documentation (whether centrally developed or l unique).	
2. The Librarian Function Should be Segregated from Systems Programing/ Operating Function	SEE INT		
3. Control Established Over Access to: • **Application Data Files** • **System Software** • **Production Programs** • **Source Programs** • **Documentation**	No significant impact on simple data entry operations.	The library function for edit programs may resi the user. Proper segregation of the library function sh present even if under user control.	

Distributed Systems on Internal Controls

Organization and Administration

POTENTIAL DISTRIBUTED SYSTEM CHARACTERISTICS: FUNCTIONS AND PROCESSES				
FRONT END EDITING	PARTIAL APPLICATION PROCESSING	HOST INTERACTIVE PROCESSING	FULL APPLICATION PROCESSING	OUTPUT PROCESSING (DATA RETRIEVAL/MANIPULATION)
separate contingency ng. However, due to y specific location	There is a need for centralized contingency planning supplemented by local unique planning at each distributed site. Contingency plans should be in effect at each location.			Same impact as for input and processing functions. Same requirements as for input and processing functions.
ce policy. ing. However, due to y specific location	Depending on equipment loss risk, self-insurance is possible. Same as for input oriented function. Adequate justification of self-insurance (if any) is critical.	No impact. As a general rule equipment loss risk is too high for self-insurance. Adequate insurance should be present. As a general rule centrally controlled insurance is least costly.		Impact depends on equipment loss risk. See other functions. Requirements depend on equipment loss risk. See other functions.
viding for alternate ical unless compatible le in the distributed other distributed sites l applications), formal processing is the best	Back-up and recovery capability should be an integral part of the system's network. More efficient back-up and recovery and alternative processing capabilities are possible in a distributed system, if these are centrally designed, to make full use of the communications network and processing power throughout the system. In the absence of localized (e.g. at the node) back-up and recovery and alternative processing capability, precise system documentation and contingency guidance should be developed to document the system-wide capability and procedures to be followed at the distributed site. In addition, plans should cover the possibility of total system failure.			Depend entirely on nature and criticality of application. See other functions.
tion files will be passed . Edit programs will ide programs. ram files are standard te storage is necessary o cause serious delays). equire offsite storage.	Entire transaction files may be passed on to a host processor. Master files, source programs, etc., may be standard system-wide. Off-site storage not critical where transaction files, master files, source programs, etc., are duplicated throughout the system. Node-unique system documentation and files require off-site storage.	A large amount of node-unique files, documentation is likely to be present. Off-site storage will be required for all critical material. Even where files are duplicated throughout the system, accidental loss may cause long delays if nodes depends on other system nodes (or the host) to duplicate files.		Function is often user oriented and thus files may be location unique. Off-site storage required for all critical unique files and documentation.
tem-wide standard. Same nd related documents as should be present for l edit program files and ly developed or location	Requirement for retention policy remain in effect when processing functions are distributed. Central guidance is required. However, specific retention policy must be tailored to files and documentation present in the node. Standardization less feasible as node processing power is increased.			Requirement for file retention policy remains in effect. However, a large amount of location unique files may be present. Only general guidance feasible. Specific policy should be developed at the location.

SEE INTERNAL CONTROL REQUIREMENT A5 IN THIS EXHIBIT

programs may reside with rary function should be trol.	The library function may be under user control. Ideally, the library function should not be a user responsibility. Organizational size constraints may prevent organizational segregation of this function. At a minimum, the function should be properly segregated within the user organization. In any event, physical access controls (e.g. restricted access, documentation under lock, supervision, etc.) should be observed.

General EDP
Impact of Distributed Syst
I. Organization and

INTERNAL CONTROL REQUIREMENTS	POTENTIAL DISTRIBUTE			
	SIMPLE DATA ENTRY	PARTIAL EDITING	FRONT END EDITING	
D. Other **1. Steering Committee Ensures that EDP Practices Satisfy and Are Consistent with Entity's Objectives**	As a general rule, a steering committee is not required (at the location) to control input functions.			Un ap co If pr co at
2. Short Term (Less than 1 year) and Long Term (1-5 Years) Plans Ensure Effectiveness Efficiency and Responsiveness of the EDP Function	Short and long term planning should be present at all locations. However, to the extent that only input functions are distributed, local EDP plans are not critical (as long as EDP considerations appear in the overall plan).			The de m a ap op an ap re
3. Competent Personnel	The tendency to integrate input responsibility with the user may result in a loss of data entry proficiency. Large volume operations will normally require "professional" data entry personnel (but see internal control requirement A2). The use of personnel not proficient in data entry requires comprehensive guidance, (e.g. user's manuals) simple input screens, clear error messages and similar techniques to facilitate data entry.			

General EDP Procedures

buted Systems on Internal Controls

EXHIBIT II-3

nization and Administration

POTENTIAL DISTRIBUTED SYSTEM CHARACTERISTICS: FUNCTIONS AND PROCESSES				
ND EDITING	PARTIAL APPLICATION PROCESSING	HOST INTERACTIVE PROCESSING	FULL APPLICATION PROCESSING	OUTPUT PROCESSING (DATA RETRIEVAL/MANIPULATION)
ocation) to	Unless there are numerous applications a steering committee is not required. If numerous users are present, a steering committee should be formed at the location.	Applications are likely to be large enough and/or involve enough users to require a steering committee. A central steering committee should always be present and responsible for providing guidance to the local committees.		
ever, to the ot critical	The need for local ADP plans depends on the nature and materiality of the application. Material operations, multiple users and user control over application will normally require a separate EDP plan.	Applications are likely to be large enough in terms of materiality and scope to require a local EDP plan. The local EDP plan must be coordinated with a centralized EDP plan.		The need for local EDP plans depends on the nature and materiality of the application. Requirements will depend on nature and materiality of application. See processing oriented functions.
result in a	The economics of scale of a centralized operation will not be present. It may not be feasible to build the EDP function around a cadre of experienced highly skill individuals supported by a less experienced staff. The distribution of competent EDP personnel to perform processing operations is a major management problem.			
y personnel proficient imple input ata entry.	The requirement for competent personnel remains. While the distribution of the processing function may lower the personnel experience and technical requirements at any given node, it is important that a correct matching of personnel and distributed function take place throughout the network.			

General EDP Procedu
Impact of Distributed Systems o
II. Operations

INTERNAL CONTROL REQUIREMENTS	POTENTIAL DISTRIBUTED SYSTEM CH			
	SIMPLE DATA ENTRY	PARTIAL EDITING	FRONT END EDITING	PARTIAL PRO
A. Scheduling **1. Scheduling Procedures Include Job Set-Up Instructions, Logging of Jobs, Provisions for Controlling CPU Workload and Job Authorization**	In an environment characterized by multiple terminals (at different user locations) there will be a tendency towards inexperienced data entry personnel, a loss of control over sequential file update requirements (e.g. processing personnel actions before processing the payroll) and increased risk of concurrent file updating (e.g. concurrent processing of personnel actions and payroll actions). Finally, the risk of unauthorized users is greatly increased. Scheduling requirements remain the same with added emphasis on detailed instructions (for inexperienced personnel), data communications monitoring capability (to control sequential requirements and prevent concurrent file updates), and logging and authorization procedures (to decrease risk of unauthorized access).			Schedul there s network to cont Schedul (e.g. in unique etc.).
B. Processing Procedures **1. All Production Schedule Changes Must be Authorized**	The distribution of data entry to different users places a premium on controlling sequential processing requirements and preventing concurrent file updates (see requirement A1). The requirement for proper authorization remains. In addition, there is a greater need to coordinate changes with other users.			The dist increases between processor The requ addition with the
2. Procedure for Documenting Schedule Changes Should be Formalized (Written)	The requirement for formal documentation remains unchanged and is even more critical in the light of coordination requirements. General system-wide guidance should be provided; however, specific requirements should be tailored to the location.			As noted wide coo The req unchange developed of all c
C. Access Controls **1. Physical Access to Computer Room is Restricted**	SEE INTERNAL CON			
2. Data Processing Equipment Should be Situated to Provide for the Physical Segregation of the Operation and Control Function	The distribution of the input function will not always justify the physical segregation of input devices. As a general rule, even if separate facilities are available, the same degree of security present in centralized operations will not be cost justified. Ideally, terminals should be physically segregated and under lock. At a minimum, terminal locks and effective system access controls (e.g. passwords) should be present.			Dependin segregat justifie The req unchange control physical
3. Access Controls are Observed on All Shifts	This is a basic Internal Control requirement wh potential impact is the reduction in the numb functions are distributed to the user.			

EXHIBIT II-4

L DISTRIBUTED SYSTEM CHARACTERISTICS: FUNCTIONS AND PROCESSES				
e	PARTIAL APPLICATION PROCESSING	HOST INTERACTIVE PROCESSING	FULL APPLICATION PROCESSING	OUTPUT PROCESSING (DATA RETRIEVAL/MANIPULATION)
er l, ng nt ll ng or ol nd	Scheduling procedures remain the same when processes are distributed. Again, there should be an emphasis on procedures to prevent unathorized access. Complex networks with partial or host interactive processing will tax the system's ability to control CPU workloads. Scheduling procedures should be tailored to fit the particular characteristics (e.g. interdependence of network processors) of the system as well as location unique considerations (e.g. experienced personnel, risk of unauthorized access, etc.).			Except for periodic outputs (e.g. monthly reports), the user oriented nature of this function prevents the development of strict scheduling procedures. Authorized users should have access to the system's data. The access cannot always be scheduled. Logging procedures are critical to control unauthorized use. A data communication monitor will usually be required to control CPU workload and prevent this function from interfacing with critical processing functions.
ng ee er re ce he	The distribution of some processing functions also increases the need for coordination, in this case between nodes and between the node and the host processor. The requirement for proper authorization remains. In addition there is a greater need to coordinate changes with the rest of the network. As noted in requirement B1, there is a need for system-wide coordination. The requirement for formal documentation remains unchanged. In this case, guidance should be centrally developed to insure proper system-wide coordination of all changes.		The processing procedures requirements under full application processing will not differ significantly in a distributed environment. Depending on the relationship between processors in the network, coordination requirements may not be as critical. The authorization and procedures formalization requirements remain. Specific procedures should be developed for the location. System-wide requirements depend on the degree of coordination needed.	As noted in requirement A1, access to system data cannot always be scheduled. In addition, users will require timely data. As a result, schedule changes may prevent the user from obtaining timely data. The formalization of processing procedures should take into account the impact of schedule changes on the user's information requirements to maximize the system's ability to produce timely data and prevent the erroneous use of incomplete data by the user.

SEE INTERNAL CONTROL REQUIREMENT IA6

al re ll m, be	Depending on the size and materiality of the operation, segregated physical facilities may not be cost justified. The requirement for physical segregation remains unchanged in a distributed environment. The internal control risk should be carefully balanced against the physical security cost.	This type of processing will usually be significant enough to warrant physical segregation. Again, risk analysis is required to determine the degree of physical segregation required.	The user oriented nature of this function emphasizes easy authorized user access to EDP equipment. Physical segregation remains as a requirement but should be tempered by efficiency requirements. Internal controls should emphasize physical segregation when equipment is not in use. Risk reduction can be achieved through system access controls (e.g. passwords, "output capability only" terminals, etc.).

ntrol requirement which remains unchanged under a distributed environment. Only
duction in the number of shifts when the input and certain output/retrieval
to the user.

al m	In partial application processing, the system will usually provide for the	In host interactive processing, the bulk of the programming responsibility	In full application processing the entire programming responsibility	The user oriented nature of this function emphasizes easy authorized user access

Provide for the Physical Segregation of the Operation and Control Function	[illegible] not be cost justified. Ideally, terminals should be physically segregated and under lock. At a minimum, terminal locks and effective system access controls (e.g. passwords) should be present.	The unch contr physi
3. Access Controls are Observed on All Shifts	This is a basic Internal Control requirement, potential impact is the reduction in the n functions are distributed to the user.	
4. Terminal and Data Access Controls are Thorough and Effective 3	Terminal and data access controls are the primary means by which the internal control risks normally associated with the distribution of the input function (e.g. less segregation of duties, increased risks of unauthorized access, etc.) can be reduced. Traditional internal control requirements include location of terminals in a secured area, utilization of user ID codes and passwords, system detection of security violations, etc. These traditional requirements remain unchanged. Other requirements which are particularly suited to the distributed environment are: the identification of authorized users by the use of physical artifacts (e.g. a card or badge) or physical characteristics (e.g. voice print) and limiting the capability of input terminals to input functions only.	In part processi usually distribu proces through nodes. limited take pl the pro passed processo Internal prevent standa program software to preve the host and pro

the physical cilities are rations will At a minimum, s) should be	Depending on the size and materiality of the operation, segregated physical facilities may not be cost justified. The requirement for physical segregation remains unchanged in a distributed environment. The internal control risk should be carefully balanced against the physical security cost.	This type of processing will usually be significant enough to warrant physical segregation. Again, risk analysis is required to determine the degree of physical segregation required.	**Physical segregation remains as a requirement but should be tempered by efficiency requirements. Internal controls should emphasize physical segregation when equipment is not in use. Risk reduction can be achieved through system access controls (e.g. passwords, "output capability only" terminals, etc.).**	
Internal Control requirement which remains unchanged under a distributed environment. Only is the reduction in the number of shifts when the input and certain output/retrieval istributed to the user.				
the internal input function access, etc.) erminals in a detection of changed. Other vironment are: ifacts (e.g. a limiting the	In partial application processing, the system will usually provide for the distribution of standard processing programs throughout the system's nodes. As a general rule, limited processing will take place at the node with the processed data being passed on to a host processor. Internal controls should prevent the access to standard processing programs. In addition, software should be designed to prevent system access to the host processor's files and programs.	In host interactive processing, the bulk of the programming responsibility will often reside at the distributed locations. Under these circumstances, there should be access to processing programs (e.g. there will have to be more reliance on the traditional segregation of duties and documentation controls). However, the software should be designed to prevent unauthorized access to the host processor (e.g. node can only pass/receive data specifically required to complete processing function).	In full application processing the entire programming responsibility will often reside at the site. Again, access to processing programs should be controlled in accordance with traditional controls. In addition, access to other nodes or processors should be limited through the software design.	The user oriented nature of this function emphasizes easy authorized user access to data bases and files. The software should be designed to ensure that these types of application have no access to processing programs (except the user's own data manipulation programs) have no input capability and have access to only those data bases and files relevant to the specific application.

Impact of Distributed Sy

III. System Developm

INTERNAL CONTROL REQUIREMENTS	POTENTIAL DISTR		
	SIMPLE DATA ENTRY	PARTIAL EDITING	FRONT END EDITING
A. System Development and Implementation 1. System Development Standards Include Adequate Analysis and Design	This requirement remains unchanged. The distribution of the input function adds additional complexity to the system development and design process, particularly the impact of decentralization on internal controls and the need to attain an effective degree of system-wide standardization.		
2. System Development Standards Include Program Development and Testing Procedures	Generally, this requirement has no impact on simple data entry.	Development and testing of edit programs remain as critical requirements when the input function is distributed.	
3. Development Standards Require User Coordination and Acceptance	Generally, this requirement has no impact on simple data entry.	Since the input function will often be distributed to the user, it is even more important than in centralized systems that the user fully understands the edit applications for which he is responsible.	
4. Development Standards Require System Documentation Including System Specifications, Program Documentation, Operating and Control Instuctions, and User Procedures and Control Instructions	The potential for inexperienced data entry personnel will require descriptive, user oriented manuals.		
B. Production Program Controls 1. Procedures Should Establish Seperate Program Libraries for Programs in Development, Testing, and Production Stages	Generally, this requirement has no impact on simple data entry.	As a general rule, programming responsibility for edit programs will not be distributed. However, if it is, the requirement remains unchanged. (See impact/requirements for processing oriented functions.)	

General EDP Procedures

EXHIBIT II-5

ibuted Systems on Internal Controls

Development and Maintenance

POTENTIAL DISTRIBUTED SYSTEM CHARACTERISTICS: FUNCTIONS AND PROCESSES				
ND EDITING	PARTIAL APPLICATION PROCESSING	HOST INTERACTIVE PROCESSING	FULL APPLICATION PROCESSING	OUTPUT PROCESSING DATA RETRIEVAL/MANIPULATION
nction adds rticularly o attain an	Partial application and host interactive processing add a new dimension to careful system design through the creation of an interrelated network of input devices and processors which should be analyzed and designed individually as well as within the perspective of the total system.		Under full application processing, systems development and design will tend to be more decentralized (e.g. performed by the location). There will be a greater need for clear control guidance to ensure system-wide compliance with systems development standards.	Very often, output oriented applications and related data manipulation capability will be user controlled. System development standards should provide for sufficient analysis and design to control user access to the system and ensure the presence of competent EDP personnel in user controlled design efforts.
ms remain as function is	The distribution of processing functions throughout the system creates a series of interdependencies which will tend to complicate the program development process. Under these circumstances, adequate system-wide testing of programs is an even more critical requirement.		This requirement remains unchanged under full application processing. Again, it is important that central guidance be developed to ensure system-wide compliance with program development and testing standards.	The impact requirements are the same as for input and processing functions.
distributed to in centralized nds the edit e.	If the concept of "bringing processing power closer to the user" is to have any meaning, then the users should be fully aware of their "processing power" to take full advantage of the distributed system environment.			
descriptive,	As in data entry, there is a need for better user oriented documentation. In addition, there is a need for system-wide documentation on all standard applications. Finally, general documentation guidance is essential to ensure proper documentation of location unique processes.		As a general rule this type of processing does not lend itself to system-wide documentation. Instead, there is a need for general documentation guidance to ensure consistency throughout the system.	The impact and requirements are generally the same as for input and processing functions. However, the user oriented nature of this function makes the user-oriented documentation requirement even more critical.
ility for edit ver, if it is, ged. (See ng oriented	This is a basic internal control requirement which remains valid in a distributed environment. However, as is the case in small size centralized operations, it will seldom be cost justified to assign librarian responsibilities to different individuals. The physical segregation of the libraries, however, should aways be present.			

INTERNAL CONTROL REQUIREMENTS	POTENTIAL DIS		
	SIMPLE DATA ENTRY	PARTIAL EDITING	FRONT END EDITING
C. Program Change Controls 1. Formal Controls are Present Over Authorization/ Testing/ and Implementation of System and Program Changes	These requirements will normally have no impact on simple data entry functions.	This requirement remains unchanged. It is important to note that edit programs will often be system-wide standard. Changes under these circumstances should be centrally controlled.	
2. Program Changes are Requested by User, Approved by D.P. Management		This requirement remains unchanged. However, the same system-wide interrelationships discussed throughout this exhibit cannot be overemphasized. Documentation updates, and a documentation changes trail are critical in a distributed system environment.	
3. Program Changes Require Formal Testing		These requirements remain unchanged in a distributed environment.	
4. Program Change Procedures Require a Documentation Update			
5. Procedures are Designed to Detect Unauthorized Changes	The system software should be designed to prevent input terminals from accessing system programs.		
6. Operations Group Only Accepts Changes Which Have Been Approved	This requirement will normally have no impact on simple data entry functions.	Again, this type of segregation of duties may not be present. Approval responsibility should be at a high supervisory level (See internal control requirements C1 and C2 above).	

General EDP Procedures

stributed Systems on Internal Controls

em Development and Maintenance

POTENTIAL DISTRIBUTED SYSTEM CHARACTERISTICS: FUNCTIONS AND PROCESSES				
FRONT END EDITING	PARTIAL APPLICATION PROCESSING	HOST INTERACTIVE PROCESSING	FULL APPLICATION PROCESSING	OUTPUT PROCESSING DATA RETRIEVAL/MANIPULATION
ed. It is important often be system-wide rcumstances should be	The interrelated nature of these functions in a distributed system increase the critical nature of these internal control requirements.		The same requirements as under a centralized system will normally apply. Again, depending on the system's total interrelationships, the requirement becomes more critical.	Generally, the same impact and requirements as discussed for input and processing oriented functions will apply. However, it is important to note that this type of function will be user oriented and thus will tend to be location unique and under a considerable amount of user control. Under these circumstances one is likely to find a loss of EDP proficiency and a lack of complete understanding of internal control requirements. User training on program documentation requirements, segregation of duties requirements and clear centrally developed internal control guidance are essential requirements.
anged. However, lationships dis- lt cannot be n updates, and a re critical in a nt.	As a general rule, application will be system-wide standard and will require a centrally controlled approval process.	Location unique programs should comply with this requirement. If size limitations prevent this type of segregation of duties, approval authority should reside at a high supervisory level. System-wide programs should be centrally controlled.		
nged in a distributed	This requirement remains unchanged; however, the testing process will be more complex in a distributed environment.		The same requirements as under a centralized system will normally apply.	
	This requirement remains unchanged. However, the same system-wide interrelationships discussed throughout this exhibit cannot be over emphasized. Documentation updates, and a documentation changes trail are critical in a distributed system environment.			
nals from accessing	The best possible control in this area is to design the system to prevent location access to standard system programs.	Certain applications will normally require system-wide standard programs. Again, the distributed location should not have access to these. Location unique programs should be controlled in the traditional manner.	The same requirements as under a centralized system will normally apply.	Once again, the best control lies in a software design that prevents user access to processing programs and standard retrieval programs (as opposed to data manipulation/user controlled programs).
of duties may not be y should be at a high control requirements	This requirement remains unchanged in a distributed environment. The major impact is the need for central approval of changes to system-wide standard programs and high level supervisory approval of changes to location unique programs.			See internal control requirements C1 - C4 above.

(2) Data Distribution

A second issue to be considered in evaluating distributed systems is the data distribution characteristics within the system. Data distribution does not have as direct an impact on specific internal control procedures as functions and processes. Instead, the impact is one of decreased or increased system risk if internal controls are not present or complied with, and/or centralized standards and guidance are not provided.

The impact of data distribution alternatives may be summarized as follows:

- Centralized data bases tend to increase system-wide risk. That is, if each distributed location interacts with a central data base, procedural internal control weaknesses at any location may have a system-wide impact. If instead, the data base was distributed to the location and the location interacted only with the distributed data base, then the impact of procedural weaknesses could be limited to that location only (depending, on the impact which the distributed data base has on the total system).

- The distribution of data bases and/or the presence of replicated data bases decreases the potential for system-wide catastrophe and, thus, total data loss risks.

- A central data base increases the total risk of unauthorized data access/manipulation. Distributed data bases may limit this risk to a specific location. However, while access to the total data base (e.g., the sum of all distributed data bases) may be limited, the risk of unauthorized access to

specific distributed data bases is not and depends entirely on the location's internal control procedures.

- A central data base facilitates the development of system-wide internal control practices and procedures. Distributed data bases will often carry unique local requirements which must rely on general guidance and not specific procedures.

- Replicated data bases are a useful means of meeting specific information requirements without increasing the risk of unauthorized data manipulation. However, it increases the risk of unauthorized data access (e.g., national security, competitor sensitive information, privacy law considerations, etc.).

Exhibits II-7 and II-8, following this page, present our analysis of the impact of data distribution on internal controls. The columns shown in the exhibits list the general data distribution alternatives discussed in Chapter I of this volume. The rows of the exhibits show each of the traditional major areas of general internal control (i.e., Organization and Administration, Operations, and System Development and Maintenance).

Impact of Distributed Systems on Internal Controls
Potential Data Base Characteristics

INTERNAL CONTROL REQUIREMENTS	CENTRAL DATA BASE	DISTRIBUTED DATA BASE	REPLICATED DATA BASE
I. Organization and Administration A. Segregation of Duties C. Librarian	A central data base tends to increase system-wide risk particularly in the access area. Segregation of duties are essential to reduce the risk of unauthorized access.	Depending on the communications network, a distributed data base would tend to reduce the system-wide risk of unauthorized access (e.g. lack of segregation of duties at one location does not have system-wide impact).	A replicated data base may enhance internal controls. For example, in user oriented operations which must emphasize data access at the expense of segregation of duties, a replicated data base may satisfy this requirement without creating an internal control risk.
B. Contingencies	As a general rule, a central data base carries the same risk of loss as that present in a centralized EDP operation.	By distributing the data base, the system-wide risk is decreased.	The presence of replicated data bases may reduce the requirements for copies of critical files (e.g. copies already exist throughout the system). However, controls over replicated data bases should be considered (See IA above).
II. Operations A. Scheduling B. Processing Procedures	Since a central data base tends to increase system-wide risks, there is a greater need to formalize these controls on a system-wide basis.	A distributed data base will often result in location unique requirements. General guidance will be required; however, specific procedures will usually have to be developed for each location.	Replicated data bases are used in conjunction with centralized and distributed data bases. The internal control impact of the original data base will vary accordingly. Specific scheduling and processing procedures will vary with the application.
C. Access Control	A central data base increases the risk of system-wide access. The system software should be designed to limit access to the minimum necessary to complete each function or application.	The access limitation requirements remain the same. Again, depending on the communication network, system-wide risk of unauthorized access may be reduced.	As noted earlier, a replicated data base may be used to limit access to specific data elements and reduce the risk of unauthorized data access.

EXHIBIT II-7

Impact of Distributed Systems on Internal Controls
Potential Data Base Characteristics

INTERNAL CONTROL REQUIREMENTS	CENTRAL DATA BASE	DISTRIBUTED DATA BASE	REPLICATED DATA BASE
III. Systems Development and Maintenance A. Systems Development and Implementation	In general, regardless of the data base characteristics, the development and implementation process will tend to be more complex. Central data bases are more suited to a centralized systems development and implementation function and as a result may be easier to control.	Distributed data bases will still require centralized systems development and implementation (at least initially). However, the fact that the data base is distributed, implies location-unique applications and thus, decentralized development and implementation efforts. In this case, there is a need for centrally developed guidance to support and control decentralized development.	The internal control impact on the original data base will vary according to its centralized and distributed characteristics. The related copy impact will depend on the specific applications which the copy supports.
B. Production Program Control C. Control Over Program Changes	The impact of a central data base on program control requirements depend on the extent to which the processing function is distributed. Minimum distribution of processing enhances the ability to control programs centrally while maximum distribution requires decentralized controls supported by general system-wide guidance. In addition, data elements will often be centralized because of data sharing or security requirements. In these instances, control over programs affecting or using these data elements are critical since they have a potential system-wide impact.	A distributed data base will usually be associated with a significant amount of distributed processing. As a result, program control will be decentralized and should be supported by general guidance. In certain cases, data will be distributed even though it contains high data sharing and/or security requirements. Under these circumstances, general guidance may not be sufficient for adequate program control.	Replicated data bases are a common technique to resolve data sharing requirements and will thus reduce the system-wide risk of inadequate program controls at any given location. However, the traditional internal control requirements remain in effect. The impact of work controls will depend on the specific application. Finally, it is apparent that replicated data bases increase the risk of unauthorized data access and should normally not be used for highly confidential data.

EXHIBIT II-8

(3) Communications Network

Finally, the characteristics of the communications network also have an impact on internal controls. As was the case with data distribution, the impact of the communications network relates to the increased/decreased system-wide risk and need for centralized standards and guidance.

The impact of communications network may be summarized as follows:

- One way communications and star configurations (e.g. providing for node to host communications only) limit the system-wide impact of localized internal control weaknesses and facilitate system-wide coordination and centrally developed procedures.

- Two way communications, multi-system networks, hierarchical networks and job networks will normally have the following impact:

  - Increase the system-wide risk of local internal control weaknesses

  - Increase the possibility of providing alternative processing capability within the system

  - Increase the need for system-wide coordination and the development of general guidance and standards to achieve this coordination.

Exhibits II-9 and II-10 following this page present our analysis of the impact of communications networks on internal control.

The columns of the exhibits list the potential communications network characteristics discussed in Chapter 1 of this volume and the rows list the traditional major areas of internal control.

Gener

Impact of Distribute
Potential Communica

INTERNAL CONTROL REQUIREMENTS	COMMUNICATIONS FORM	STAR CONFIGURATI
I. Organization and Administration A. Segregation of Duties C. Librarian	One-way communications limit the impact of a given location's internal control weaknesses. Two way communications expand the scope of internal control requirements. For example, if a distributed payroll application requires input at both the node and from a central location, segregation of duties at both places affect the application.	This configuration the system-wide r internal control wea at any given locati
B. Contingencies	Two way communication will enable the system to provide alternate processing capability in case of localized system failure.	This configuratio normally not prov efficient capabili alternative proc within the system of localized s failure.
II. Operations A. Scheduling B. Processing Procedures	Two way communications increase the need for proper coordination and formalization of these procedures. As was the case with segregation of duties, two-way communications expands the scope of internal control requirements (see example in IA above).	This configuration the system-wide internal control we at any given locat addition, ther normally be a requirement for sc and processing coor on a system-wide b
C. Access Control	Two way communications increases the capability of the node/processor in the network and thus the risk of unauthorized access.	This configuration the system-wide internal control we at any given l (However, als communications for

EXHIBIT II-9

Distributed Systems on Internal Controls
Communications Network Characteristics

STAR CONFIGURATION	MULTI-SYSTEM NETWORK	HIERARCHICAL NETWORKS	JOB NETWORKS
This configuration reduces the system-wide risk of internal control weaknesses at any given location.	Since this configuration provides for communication between nodes, weaknesses at any given location have a system-wide impact.	The risk exposure of internal control weaknesses will be directly related to the organizational (hierarchical) location of each node/processor in the network.	Since communications between processors will normally be present, weaknesses at any processor will have a system-wide impact.
This configuration will normally not provide an efficient capability for alternative processing within the system in case of localized systems failure.	Communications between nodes increase the possibility of providing alternative processing within the system in case of localized system failure.	Depending on communication capability at each level within the hierarchy, this configuration may facilitate alternative processing within the system in case of localized system failure.	Assuming a similarity of processing throughout the network, this configuration provides the best capability for alternative processing throughout the network.
This configuration reduces the system-wide risk of internal control weaknesses at any given location. In addition, there will normally be a lesser requirement for scheduling and processing coordination on a system-wide basis.	Under this configuration, weaknesses at any given location have a potential system-wide impact. To the extent that processing is affected by more than one node (or processor), coordination requirements and thus scheduling and processing procedures become more critical.	The risk exposure, and condition requirements will be directly related to the organizational (hierarchical) location of each node/processor in the network.	Weaknesses at any location will normally have a system-wide impact. As a general rule, this type of configuration will require a substantial amount of coordination.
This configuration reduces the system-wide risk of internal control weaknesses at any given location. (However, also see communications form.)	This configuration increases the system-wide risk of internal control weaknesses at any given location (also see communications form).	Risk exposure will be directly related to the organizational (hierarchical) location of each node/processor in the network.	Weaknesses at any location will normally have a system-wide impact.

General EDP Procedur

Impact of Distributed Systems on Potential Communications Netwo

INTERNAL CONTROL REQUIREMENTS	COMMUNICATIONS FORM	STAR CONFIGURATION	MULTI-SYS
III. Systems Development and Maintenance A. Systems Development and Implementation	In general, distributed systems will tend to complicate the system development process. In all cases, there is a need for a centralized development and implementation evaluation. Two-way communications increases the need for system-wide coordination and will require more centralized systems development and implementation.	Once the distributed system is developed and implemented, the requirement for system-wide coordination (except host-node relationships) is decreased. Centralized control is still necessary but it may take the form of general guidance.	Centralized this funct critical bec to coordin between nod Activities program te often requi review and System-wide be specif prevent th adverse imp unique effe
B. Production Program Control C. Control Over Program Changes	Two-way communications increase the need for system-wide coordination and thus the need for centralized control.	This configuration decreases the system-wide risk of internal control weaknesses at any given location. In addition, local applications will often be self-contained thus reducing the need for central control over programs.	Weaknesses location ma wide impac cases, loc will not b (e.g. will nodes) thu need for control.

General EDP Procedures

EXHIBIT II-10

Distributed Systems on Internal Controls
Communications Network Characteristics

STAR CONFIGURATION	MULTI-SYSTEM NETWORK	HIERARCHICAL NETWORKS	JOB NETWORKS
nce the distributed system s developed and mplemented, the equirement for system-wide oordination (except host-ode relationships) is ecreased. Centralized ontrol is still necessary ut it may take the form of eneral guidance.	Centralized control over this function is more critical because of the need to coordinate activities betwe nodes. Activities such as design, program testing, etc. will often require system-wide review and coordination. System-wide guidance should be specific enough to prevent the potentially adverse impact of location unique efforts.	The impact will at least be similar to that of multi-system networks. Assuming that more powerful processors will be present in this configuration, all supporting different applications throughout the system (e.g. processing support to multiple locations in the network) the need for system-wide control is most critical.	The imact will at least be similar to that of multi-system networks. Assuming that more powerful processors will be present in this configuration, all supporting different applications throughout the system (e.g. processing support to multiple locations in the network) the need for system-wide control is most critical.
his configuration ecreases the system-wide isk of internal control eaknesses at any given ocation. In addition, ocal applications will ften be self-contained hus reducing the need for entral control over rograms.	Weaknesses at any given location may have a system-wide impact. In certain cases, local application will not be self-contained (e.g. will affect other nodes) thus increasing the need for system-wide control.	Risk exposure and need for system-wide control will be directly related to the organizational (hierarchical) location of the program in question within the network.	Weaknesses at any location will normally have a system-wide impact. As a general rule, this type of configuration will require a substantial amount of system-wide program control.

2. IMPACT OF DISTRIBUTED APPLICATIONS ON GENERAL INTERNAL CONTROLS

The prior discussion has analyzed the impact of distributed system characteristics individually, without considering the nature of specific applications supported by the system.

The nature of the application itself has a significant impact on internal controls. In analyzing the impact, we have adopted the criteria used by IBM in developing and planning distributed systems. Although the criteria was designed to support systems development efforts, we feel it is equally applicable to the analysis of internal controls.

In general, IBM's criteria points out that business applications have certain qualitative and service level requirements which can be grouped into four categories: timeliness, quantity, quality and security. Depending on the specific requirements, a particular application will best be supported by distribution or centralization (of both processes and data bases) and may or may not require a single copy of the data base.

However, very often there will be applications which will be distributed even though certain requirements call for centralization and vice versa. By the same token, single copies of the data base will not always be present even when the application is best served by a single copy. The reason for these contradictions is not necessarily poor system design (although the auditor must, of course, be aware of this possibility). Instead, contradictions will arise because each application is likely to have contradictory requirements. Thus, the design of distributed systems seeks to reduce the conflict created by contradictory requirements, but ultimately, will result in the distribution or centralization of applications and the duplication of

data bases even though the configuration is not optimal from the specific application's (as opposed to system-wide) point of view. Invariably, these contradictions will result in inefficiencies which in turn may impact internal controls.

Exhibit II-11 summarizes specific requirements which may be present, or should be considered for each application; it also shows the optimal processing/data base characteristic associated with each requirement and the potential impact of requirements and optimal processing/data base characteristics on internal controls.

The requirements listed in Exhibit II-11 are based on material developed by IBM, System Science Institute, Los Angeles, California.

General EDP Procedures

Impact of Processing/Data Requirements on Internal Control (Note)

REQUIREMENT	REQUIREMENT DEFINITION	OPTIMAL PROCESSING/DATA CHARACTERISTICS	INTERNAL CONTROL IMPACT
I. Timeliness		Quick response time and/or continuous data availability requirements. Ideally, require the distribution of the supporting process.	Quick response time and/or continuous data availability requirements without distribution of the supporting process are indicative of potential internal control weaknesses. As a general rule, the result is a loss in efficiency (e.g. lost revenues, operating delays, etc.) However, procedures will often be developed to offset these deficiencies. These procedures may in turn, affect internal controls. For example, in a warehousing operation, data on purchase orders may be required prior to accepting delivery of shipments. If the purchase order processing and related data files are not distributed, alternative procedures may provide for the distribution of copies to the warehouse, or the creation of a duplicate data file to support this operation. These procedures may satisfy the function's requirement and thus provide adequate control. Alternatively, however, the procedures may be insufficient, or there may be no procedures so that shipments are accepted
A. Responsiveness	Time elapsed between inquiry and response.		
B. Scheduled Availability	During what time period(s) is information required.		

			may satisfy the function's requirement and thus provide adequate control. Alternatively, however, the procedures may be insufficient, or there may be no procedures so that shipments are accepted without purchase order information (an internal control weakness).
II. Quantity A. Data Volume	Amount of data processed.	Large data volume and complex processing requirements usually requires the consolidation of the supporting process.	The need for single copy is dictated principally by efficiency considerations (e.g. a large amount of data requires substantial store space and data sharing, if supported by duplicate data bases, will again utilize a large amount of storage.)
B. Activity Complexity	Processing sophistication required.		
C. Activity Frequency	Addresses how often (as opposed to "how much") an activity or process will take place.	Frequency of processing (e.g. how many times process will take place during the day). Ideally requires the distribution of the process.	This requirement is closely related to the timeliness of the data (See I above). If the activity is an output activity, distribution of the process will facilitate its performance. If distribution is not present, the same potential weaknesses as in I above may be present. If the activity is input oriented, the lack of distribution will affect the currency of the data (see Requirement III) and may create an input backlog.

NOTE: Adapted from course material developed by IBM, Systems Science Institute (Los Angeles, Cal.): "Distributed Information System Planning and Design".

General EDP Procedures

Impact of Processing/Data Requirements on Internal Control

REQUIREMENT	REQUIREMENT DEFINITION	OPTIMAL PROCESSING/DATA CHARACTERISTICS	INTERNAL CONTROL IMPACT
II. Quantity (continued) D. Aggregate Data Volume	Amount of data required to support application.	A large amount of data required to support an application and/or a large number of users (applications) requiring the data should be supported by a single copy of the data base (e.g. without resorting to duplicate data bases). Further, a need for data sharing, unless it is localized, will normally require a central data base.	The need for single copy is dictated principally by efficiency consideration (e.g. large amount of data requires substantial store space and data sharing, if supported by duplicate data bases will again utilize a large amount of storage.) Other than operating efficiency, the presence of duplicate copies will not necessarily affect internal controls. However, if the processor containing the duplicate copy is inadequate, there is a risk of data loss. Further, duplicate data bases may result in data inconsistencies between the different copies.
E. Data Sharing	Number of users (applications) using the same data.		
III. Quality A. Currency	Degree of data currency (e.g. up-to-the-minute, day old, etc.).	A high degree of currency usually requires a single copy of the data base.	The need for a single copy is dictated by the delays that would be present if multiple (copies) data bases had to be updated for each transaction. If a single copy is not present, the data base may not be current enough to support the application. This deficiency may in turn impact internal controls.
B. Consistency	Requirement for common	A high degree of consistency throughout the system	Decentralization of processing obviously

			each transaction. If a single copy is not present, the data base may not be current enough to support the application. This deficiency may in turn impact internal controls.
B. Consistency	Requirement for common system-wide processing (or procedures) supporting an application.	A high degree of consistency throughout the system ideally requires centralized processing.	Decentralization of processing obviously implies a loss in the ability to control activities at each location and enforce consistency of application. The distribution of a process requiring system-wide consistency increases the risks of processing errors and accumulation (classification) of incorrect data.
C. Independence	Requirement for location unique processing (or procedures) to support an application.	Independence requirements in processing are more efficiently met by distribution of the process.	The centralization of processing functions with location unique characteristics would tend to complicate programming, and central documentation requirements. Further, user involvement in the development of applications will be hindered. All of these possibilities may weaken internal controls.
IV. Security	Sensitive nature of the data (e.g. national security, legal requirements, competitor interest).	Confidentiality and strict control over data changes requirements will usually be supported by a single copy of the data base. It is important to note that this requirement does not preclude distribution of the data base.	The presence of multiple copies of data bases with high confidentiality or mutability requirements will always increase the risk of unauthorized access and are indicative of internal control weaknesses (even though multiple copies may be justified for reasons other than internal controls). Alternative procedures should be present to offset the internal control weakness.
A. Confidentiality			
B. Mutability	Requirement for strict control over changes.		

3. DEVELOPING COMPATIBLE GENERAL INTERNAL CONTROL PROCEDURES

The purpose of this section is to identify internal control practices and procedures which are most effective in the new technological environment of distributed data processing systems. As we stated in the preceding section, the effectiveness of specific internal control practices and procedures is affected by this new technology. Some traditional controls are no longer practical or effective while other controls become more critical. The objectives of internal control have not changed, the techniques and emphasis of certain controls have. We have divided our discussion of compatible general internal controls into the following categories:

- Organization and Administration
- Operations
- System Development and Maintenance

(1) Organization and Administration

As noted earlier, organization and administration controls address segregation of duties, contingency procedures and the librarian function. The development of compatible internal control procedures must address first the impact of distributed systems as discussed in Section 1 of this chapter and then, those procedures which are in effect to offset this impact. In general, procedures must be present to ensure the following:

- Offset the decrease in traditional segregation of duties (if applicable)

- Proper control over (potentially) inexperienced personnel
- Adequacy of contingency procedures
- Adequacy of control over the data communication network.

Exhibit II-12 following this page presents procedures which should be present in a distributed system environment.

(2) Operations

Operations controls address scheduling, processing and access internal control procedures. The development of compatible internal control procedures must address the following points:

- Loss of centralized controls
- Increased need for coordination
- Increased risk of unauthorized access.

Exhibit II-13 following this page presents procedures compatible with a distributed environment.

(3) System Development and Maintenance

System development and maintenance controls relate to system development and implementation and control over programs. Areas of concern include:

- Centralized control over systems development and implementation
- Increased requirement to properly control program changes.

Organization and Administration
General Internal Control Procedures

A. General Organization and Segregation of Duties Considerations

Where traditional segregation of duties within the EDP function is not practical as a result of size limitations or increased user involvement and control, the following procedures are indicative of adequate internal controls:

- Segregation of programming, operating and librarian functions within the user organization (or within the distributed location)
- Adequate involvement of supervisory personnel, including proper approvals and authorization
- In-house training programs on EDP and internal control requirements
- User procedures to minimize segregation of duties conflicts in the assignment of functional (e.g., user) and EDP responsibilities
- Adequate user oriented documentation.

B. Controls Over the Data Communications Network

Installation and subsequent use of a distributed system typically requires the following:

Organization and Administration
General Internal Control Procedures

- One or more systems programmers assigned to install and maintain the data communications software

- One or more data communications analysts responsible for designing and configuring the teleprocessing network

- One or more programmers/analysts responsible for designing and implementing CRT screens, hardcopy or other I/O formats customized to the teleprocessing applications.

Normally, adequate segregation of duties within the data communications area would consist of separating the activities and functions between two groups as listed below:

- Systems programming personnel and/or data communications analyst group, who:

  - Install the data communications software (e.g., TP Monitor)

  - Maintain the data communications software (i.e., add terminals to TP configuration, extend network, fix software bugs)

  - "Fine tune" the data communications software (i.e., improve response time)

  - Design the communications network

  - Recommend purchase of necessary hardware and software (e.g., TP Monitor, communications controller, terminals, modems, multiplexors)

  - Oversee installation and use of the communications network.

Organization and Administration
General Internal Control Procedures

- Application programmer/analyst group responsible for on-line system development, who:
  - Design screen or hardcopy formats for input and output of data
  - Implement the screen or hardcopy formats by use of the TP Monitor, message formatting software or both
  - Design and code application programs that process data utilizing the screen or hardcopy formats.

C. Contingency Controls

When the decision is made to take advantage of the self-insurance and alternative processing possibilities provided by distributed systems, the following should be present:

- Total system-wide self-insurance plan supported by:
  - Detailed risk/benefit analysis
  - Extent of self-insurance
  - Location unique insurance plan and risk/benefit analysis
- Total system-wide alternative processing plan supported by:
  - Detailed risk/benefit analysis
  - Location unique contingency plan
  - Provision for total system failure contingencies.

Organization and Administration
General Internal Control Procedures

Procedures should be developed to ensure accurate and timely recovery of the distributed system in the event of hardware or system software failure. Some of the elements that may be included in the recovery of an on-line system are:

- Checkpoint/restart. (When a system failure occurs, the system is restarted from the last checkpoint, with all data intact as of that checkpoint.)

- File recovery. (In the event of a data access or system error, a file recovery program restores the files to their previous status.)

- Transaction recovery. (In the event of a system failure, input and output transaction queues are restored to their previous status.)

- Program error handling. (The on-line system is able to recover from program errors and continue normal processing.)

- Teleprocessing error handling. (The on-line system is able to recover from an error in the terminal or communications line.)

- Dial back-up. (The ability of a terminal in the network to switch over to the dial-up telephone network should a node in the private line network become inoperative.)

- Audit trails and statistics. (The on-line system is able to capture and record significant transaction data.)

Finally, procedures should be developed to continue recordkeeping and production operations without the availability of the system for a temporary or extended outage.

Operations
General Internal Control Procedures

A. Scheduling

A key consideration in a distributed environment is ensuring that different processing functions do not interfere with each other. This requires a data communications monitor to maintain file integrity.

The system's monitoring capability should:

- Prevent files from concurrent updating
- Queue competing transactions for serial updating
- Control total CPU workload.

B. Processing Procedures

Processing procedures should be established for normal processing, using the data communications monitor, and for abnormal conditions. Processing procedures should include the following:

- Activating the data communications monitor at the beginning of the day and deactivating the monitor at the end of the day
- Restarting the monitor after a hardware or operating system software problems

Operations
General Internal Control Procedures

- Taking a malfunctioning terminal or communication line out of service and assigning its functions to a substitute terminal or line

- Logging and reporting of terminal security violations along with appropriate follow-up action.

Assigning and reassigning terminals and communications lines, among other functions, is often accomplished using a master terminal. The functions performed at the master terminal will vary with the data communications monitor in use. Where master terminals are present access to them should be strictly controlled.

C. Data Access

In a distributed system environment, data access is achieved by using on-line terminals. The following are indicative of good data access controls:

- Terminal users are identified to the computer by password, physical artifact (e.g., badge) or physical characteristics (e.g., voiceprint)

- The transactions and functions permitted at each terminal should be limited to those specifically authorized

- Unused terminals should be automatically disconnected after a predetermined period of inactivity

- Software should be designed to ensure that unauthorized terminals have no access to application programs or data.

Exhibit II-14 following this page presents procedures compatible with a distributed environment.

Systems Development and Maintenance General Internal Control Procedures

A. System Development and Implementation

Good controls over system development and maintenance would include the following:

- Controls should be present to prevent programmers from staging production-like jobs that access production data sets

- Controls should be present to prevent operations personnel from staging development-like jobs that access program libraries or compilers

- A record showing computer resources used by each programmer (e.g., terminal time, CPU time, data sets retained) should be kept and reviewed periodically by management.

In addition, the controls listed below are segregated by the two basic methods of system development and implementation utilizing data communications:

- Remote Job Entry (RJE). With RJE, batch jobs are submitted from a remote location to the central computer. Printout from the batch jobs is normally returned to the remote location. Good control over RJE terminals would consist of one or more of the following:

Systems Development and Maintenance
General Internal Control Procedures

- An operator assigned to the terminal

- A manual job log maintained of input and output

- Use of job account numbers (unauthorized job account numbers will cause a job to be rejected).

. Timesharing. Using timesharing, programmers access the computer by utilizing low speed terminals. Timesharing may be used to enter and update programs; compile, link and execute programs; and stage jobs for batch submissions. Control over a timesharing system will require the use, control and periodic change of log on, identification and passwords.

B. Data Communications Program Control

Adequate control over production programs would include:

. Procedures which provide that separate program libraries be used for programs in the development and production stages

. New or modified application programs are tested in such a way that they do not impact production programs that are running under the same communications monitor (e.g., by use of a facility that allows programs to be tested in a batch environment that is simulating the on-line system).

4. IMPACT OF DISTRIBUTED SYSTEMS ON AUDIT PROCEDURES

In the previous section we have presented internal controls related to distributed systems in the context of what system designers, operators and users must do to react to this new environment. Here we present a summary of where the auditor must become involved in this environment. The majority of our project efforts in the remainder of this engagement will be directed towards the auditor and how he can better accomplish his mission of service to management in a distributed environment.

One of our major findings in conducting this investigation is the fact that the objectives of internal controls do not change in a distributed processing environment. However, as this chapter points out the emphasis and techniques which are most effective in the system of internal controls have changed, and, in some cases, drastically. Given the infancy stage of the distributed environment in the Navy and the relatively new NARDAC/NAVDAC concept, we feel tne auditor can take positive steps to establish himself as an effective management resource in the data processing environment of the Navy. While subsequent tasks will address this issue in more detail, we feel a brief discussion of the potential impact of the distributed environment on auditing procedures is appropriate.

As part of our research we have been interested in how other audit organizations have reacted to the advancements in data processing systems. We have been presented with several alternative methodologies and have evaluated the effectiveness of each. The alternatives considered included computer audit checklists, audit programs, audit test data, and simulation models. Our conclusion is that few traditional audit tools are adequate for evaluating controls in a distributed environment.

We have, however, been introduced to a new methodology which we feel may prove applicable to the Naval Audit Service's environment. Our research into this methodology has been limited, and this discussion is accordingly sketchy. However, because of its potential, we believe an initial discussion is appropriate. This approach is presented here as an illustration of the type of methodology the auditor may wish to adopt. The methodology has many features, one of which is the flexibility it possesses. Systems which are operational, as well as those still under development may be evaluated from a total internal control perspective. The approach also features versatility in that extensive EDP experience is not required to perform the review. The approach is comprehensive in that it considers the total system environment which includes manual procedures as well as electronic data processing functions. An overview of this methodology is presented in the remainder of this section.

The overall objective of this methodology is to evaluate the adequacy of the system of internal controls. It requires an analysis of activities performed, controls in place, and an analysis of the testability of those controls. The approach requires the preparation of several independent matrices and the comparison of the results of each. The first step is to prepare a matrix (Exhibit II-15) which lists all activities, both manual and automated, which occur in the system processing. The second axis of the matrix lists exposure which results from such activities. The second matrix (Exhibit II-16) takes the list of activities performed in the system and relates these activities to controls present in the system. Once this second matrix has been prepared the auditor can analyze the system. The analysis should identify all uncontrolled activities and those activities which may be overcontrolled. It is not uncommon for one system activity to be overcontrolled while other activities lack any control at all. The third and final matrix (Exhibit II-17) is then prepared relating the exposures and controls previously identified.

Exhibit II-15 presents a representative analysis of system activities and related system exposures using a typical disbursement application. The example lists some normal activities which one would expect to find in a disbursing system. For purposes of demonstrating the methodology we will concentrate on the activity titled "Input Invoice Data" to trace through the methodology. As shown in Exhibit II-15 there are multiple exposures associated with this activity. The exposure areas are identified for a remote input terminal. To develop this list of activities and exposures the auditor would need to develop a system flowchart which traced an invoice from its receipt to final disposition.

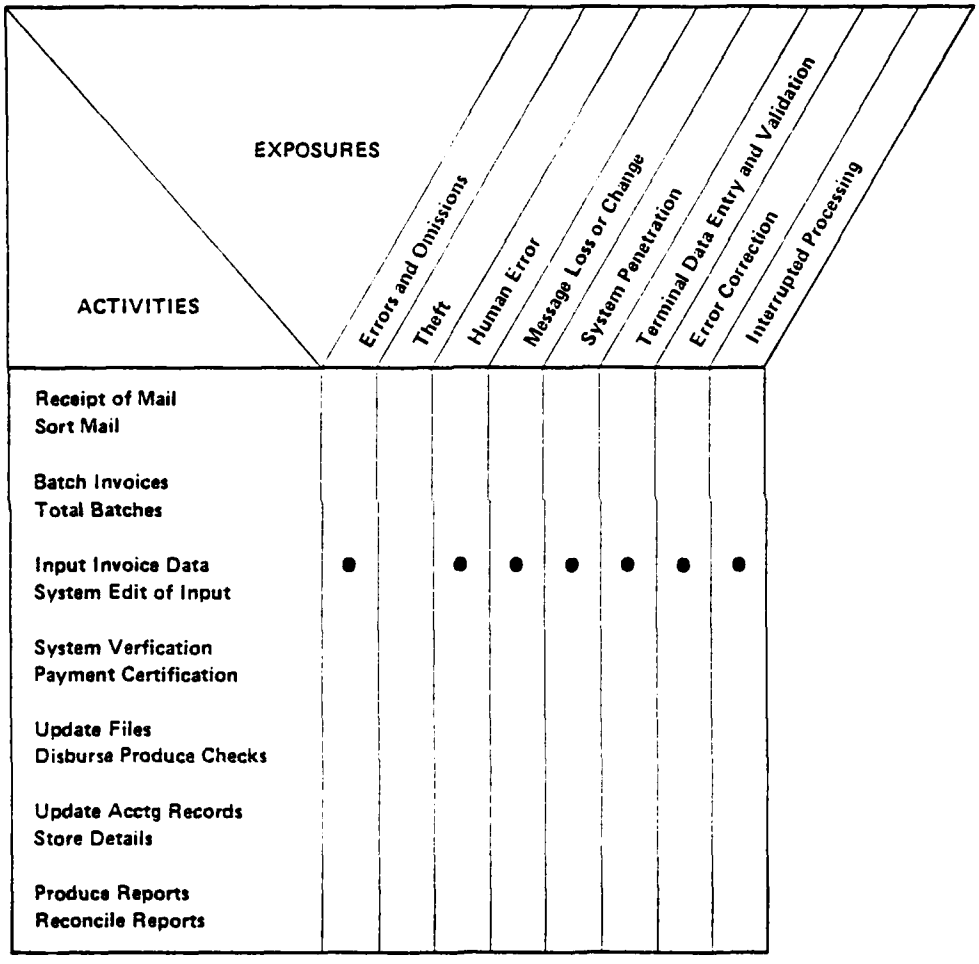
The second matrix, presented in Exhibit II-16, lists the same system activities identified previously but relates these activities to the system of internal controls associated with the process. These controls should include manual as well as EDP controls and all controls associated with an activity should be identified for each activity. Again utilizing our sample activity we have identified all controls applicable to the input invoice data activity.

The auditor must now analyze the controls in light of the exposures. To perform this step a third matrix is prepared. This matrix, presented in Exhibit II-17, lists all controls associated with the activity "Input Invoice Data" and the associated exposures. The exposures associated with the activity are listed across the horizontal axis of the matrix. Controls that relate to that exposure are then identified within the table of the matrix. Once this table is complete, the auditor can decide which controls he desires to test and develop appropriate audit test procedures to verify the effectiveness of the control.

The desirability of this methodology is its simplicity and thoroughness. It considers the total system and provides a metnod of evaluating efficiency and identifies duplicated controls.

We feel the adoption of a standard methodology by the auditor is of paramount importance in being successful in the future. The results of the lack of a standard methodology are independently developed approaches which vary in quality and effectiveness. Utilization of a standard approach provides the capability to exchange experiences and learn from others using the same tool. The methodology can then evolve and improve with experience.

Activity and Exposure Matrix



Activity and Control Matrix

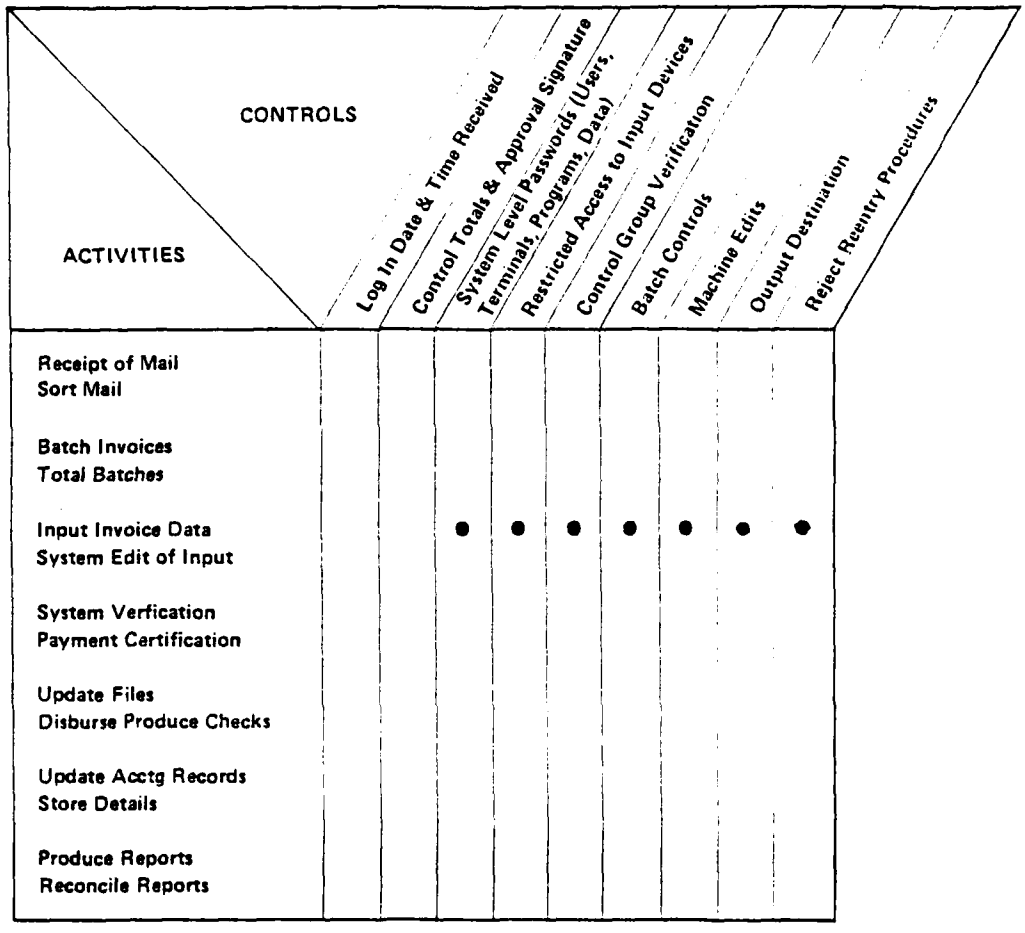


EXHIBIT II-17

Control and Exposure Matrix

ACTIVITY INPUT INVOICE DATA

CONTROLS \ EXPOSURES	Errors and Omissions	Theft	Human Error	Message Loss or Change	System Penetration	Terminal Data Entry and Validation	Error Correction	Interrupted Processing
Log In Date & Time Received								
Control Totals & Approval Signature								
System Level Passwords (Users, Terminals, Programs, Data)					●			
Restricted Access to Input Devices					●		●	
Control Group Verification	●		●	●	●		●	
Batch Controls	●		●	●		●		●
Machine Edits	●		●	●			●	
Output Destination				●	●			
Reject Reentry Procedures	●		●	●	●		●	●

Chapter III.

Observations and Recommendations Related to Distributed Systems and General Internal Controls

III. OBSERVATIONS AND RECOMMENDATIONS RELATED TO DISTRIBUTED SYSTEMS AND GENERAL INTERNAL CONTROLS

As a result of our research effort, we have several observations in the area of distributed system and internal controls. Because of the related nature of all the tasks in this engagement, these observations and recommendations are preliminary in nature.

This chapter is intended as a brief summary of our research work. No attempt has been made to provide a high level of detail. The observations and recommendations included in this chapter will be developed further in future deliverables and incorporated in the final report.

1. OBSERVATIONS

- **Distributed Systems do not have an Impact on the Basic Objectives of Internal Controls.**

  The overall objective of internal controls in an EDP system may be broadly defined as procedures to ensure the accuracy and completeness of transaction processing and the resulting management reporting. Distributed data processing systems have not modified this objective. However, the emphasis and effectiveness of specific internal control procedures are affected by this new technology. We discuss the impact of this new environment in Chapter II of this volume. Here our point is that the concept of controls and the objectives of a system of internal controls is not changed by the introduction of this new EDP technology.

- Effective Control Over the EDP Function is More Difficult in a Distributed System Environment.

  Distributed systems have moved data processing equipment out of the computer room and made control of the EDP function one of the most difficult areas to monitor. Traditional systems provided centralized system development and processing and made control of the EDP functions an isolated problem. With distributed systems placing processing power at remote locations, controls must be effective in multiple environments. Users must be educated and capable of enforcing controls in order to effectively maintain a distributed system. The dispersion of data processing capability must be accompanied by the assumption of system control responsibilities by system users. Without users who understand the system's functions and procedures, the system will not operate in a properly controlled environment.

- Total System Coordination is Essential in a Distributed System Environment.

  The need for system coordination is an aspect of system operations as well as design which has increased in importance with the development of distributed processing systems. With the distribution of processing functions throughout the system, interdependencies are created which complicate the need for total system coordination. Scheduling must be tailored to the system and a complex system with interactive processing requires the system to have the capability to control CPU workloads. These coordination constraints must be carefully considered and analyzed in order to distribute processing capability and

still maintain a system which is operational at geographically dispersed locations.

- Internal Controls in a Distributed System Environment are Heavily Dependent on the System's Design.

Distributed systems by their very nature are often large, complex systems. These systems require a more critical review and analysis during the system design stage. Should necessary control features be ignored during the system's design and testing, the ramifications of such oversights are multiplied by the number of locations operating that system. The development process must also consider the system user in a different perspective in a distributed processing system. For in reality, the users will often be operating the system. This situation calls for a design which is logical, straightforward, and considers the users' operating environment, not the designers' computer room, in performing the design analysis. System design has always been considered an important control element. In a distributed environment, it is more important than ever before.

- The Characteristics and Requirements of Specific Applications Have a Direct Impact on the System of Internal Controls.

Obviously, there is no one set of internal controls which is applicable to all application systems. Application systems are all unique in some respects and the internal controls most efficient and effective in one particular application system may not be justifiable in another application system. The point here is to stress that the operational characteristics and objectives for an individual application system must be considered when analyzing the

propriety of any given internal control and the application's total system of internal control. Unique system requirements will dictate a unique system of internal controls.

- Personnel and Staffing Considerations Significantly Affect the Development of Internal Controls in a Distributed System Environment.

Consideration for the user, his environment and background has been emphasized in the past as an important system design consideration. In a distributed environment, the user's role is elevated to include some system operating responsibilities. It is important that users be properly trained and user procedures be properly documented. The distributed system must be designed to provide internal controls which compensate for the lack of control over tnese users/operators. Users typically are not data processing oriented and if system controls are inadequate they may attempt to compromise the system's integrity. The internal controls placed in the system should be designed to discourage experimentation and report any attempt to violate the system's integrity.

- The Risk of Unauthorized Data Access and Manipulations is Significantly Increased in a Distributed Environment.

This observation is closely related to the previous item concerning user personnel and internal controls. Not only are system users a consideration, but distributed system designers must also consider unauthorized attempts to enter the system. When terminals are located in remote locations, there is a terminal security problem not previously found in data processing systems. When communications lines are utilized there is a threat to system integrity previously

nonexistent. System designers must realize the value of system information to outsiders and protect this asset with an appropriate level of system controls. The dispersion of terminals and the utilization of communications lines provide new opportunities for system penetration which must be offset by adequate system controls.

- Distributed Systems Often Provide Internal Control Procedure Alternatives in the Area of Contingencies and System Failure.

Traditional data base systems require a substantial duplication of critical files in order to maintain system backup capability. Distributed systems, with distributed or replicated data bases, provide opportunities to examine the need for backup and recovery procedures in the system in a different light. The simple fact that files are located in various locations tends to reduce the risk of system-wide failure and provides some protection against a catastrophic loss. We have previously mentioned the increased risks associated with the distribution of data; here our point is a new opportunity exists to modify traditional backup and recovery requirements. This new flexibility may also apply to system processing capability if local unique requirements are not predominant.

- Specific Characteristics of Distributed Systems may be used to Strengthen Internal Controls.

It is obvious that distributed processing presents unique problems and negates some traditionally effective internal controls. Distributed systems also provide opportunities to expand the limits of traditional controls. For example, these advanced systems can provide user oriented screens to

prompt input operators, instantaneous editing and validation of system input and immediate error correction while original source documents are still at hand. These capabilities should increase the reliability of input data. In the area of contingencies, it is apparent that distributed systems tend to decrease total system risk and provide improved backup processing capabilities. Finally, the distribution and/or replication of data bases can be effectively used to improve operational efficiency while limiting the impact of unauthorized access.

- The Internal Audit Function is Significantly Affected by the Characteristics of Distributed Systems.

The audit profession, in general, has lagged behind in the area of data processing auditing. Computer auditing has tried to catch up with computer technology and continues to develop audit techniques to react to the data processing environment. Distributed systems are another advance which auditors must react to and the problem is that most traditional computer auditing techniques are insufficient in this environment. The distribution of data, input capability and the utilization of communications links require the audit profession to modify its traditional approach. It may no longer be realistic to audit an application from one facility and depending on the degree of distribution, physically impossible to review every system location simultaneously. This situation places an increased demand on computer audit tools and audit capability being designed into a system. Network architecture may result in a system being unauditable unless audit capability is provided for during the design phase. This situation results in an increased need for auditors to participate in the system's design and define their needs during the requirements analysis phase of development.

2. RECOMMENDATIONS

In this section we present our recommendations related to the observations previously discussed. We briefly discuss each recommendation and outline the rationale of each. The order in which these recommendations are presented in no way signifies their relative importance or attempts to prioritize their need.

(1) Computer Systems and EDP Internal Control Training Should be Required for all Auditors.

Although the remainder of our project efforts will expound on this issue, it is worthy of mention at this point in time. Even though the bulk of the Audit Service's auditors are not involved in computer auditing, they should understand the basic capabilities of computer systems and generally be aware of EDP internal control requirements. The advance of data processing capability has not been accompanied by a corresponding adjustment of the traditional audit approach. Should this gap continue to expand, the auditors ability to serve the organization he is auditing will be significantly reduced. The concepts of traditional internal controls are being impacted by the development of distributed systems and auditors must understand the ramifications of these systems in order to continue to perform their functions.

(2) The Design of Distributed Systems Should Place Added Emphasis on Internal Control Considerations.

Although retrofitting is always an expensive means of eliminating internal control weaknesses, traditional EDP systems are comparatively easier to modify after installation. For example, additional control features can be added to centralized applications within minimal production disruption. This

capability is lost in a distributed system and thus the ramifications of placing an uncontrolled system in multiple locations can be extremely high. There is a definite need to more critically review and analyze the need for internal controls in the design phase of distributed systems. Controls must minimize system exposures and increase system manageability. Internal control considerations must be analyzed and evaluated by the system designers in light of the functions of the system and the system's objectives. System designers must be congizant of the operating environment in which the system will operate and realize that data processing department organizational controls will have little impact on a user's operation of a distributed system.

(3) Standards and Procedures Should be Developed to Ensure Adequate System-Wide Controls over Distributed Processes, Related Data Bases and the Network Configuration.

The migration of data processing resources out of the computer room increases the need for adequate system-wide controls. If the distribution of processing power and system data is permitted, standards must be developed to protect the system and prevent the unauthorized use of system resources. Procedures which dictate review and approval are needed to prevent unauthorized changes to the system, assure proper documentation, and system-wide notification of any modifications. These standards and procedures must be formalized, provided to all system users and enforced, if system integrity is to be maintained. Standards and procedures also provide a means of reconstructing a system's evolution from its initial form to the current version. The importance of this type of control can not be overemphasized.

(4) System Design Priority Should be Given to Controls over the Operating System as a Key Element in the Overall Control of Distributed Systems.

System designers are often so concerned with the specific applications program they are developing, they disregard controls or the lack of controls present in the operating system. It is important that operating system features be considered in a distributed system's development, in that they may provide the opportunity to modify the application program and related files by changing the operating system itself. Designers should understand the capabilities of the operating system and review the procedures in place to assure themselves that this capability is not improperly used. The operating system must receive the same level of supervision and control and be documented as well as any individual application program.

(5) The Development and Implementation of Distributed Systems will Require more User-Oriented Documentation.

We previously described the increased role the user assumes in a distributed environment. In the implementation of such systems, user needs increase in importance. The user's terminology as well as his manual operating procedures must be considered when developing system procedures manuals. His computer background and other job responsibilites are also important. A simplified approach is usually most effective in developing procedures and an outline of a procedures or a picture of an input screen can eliminate much confusion in a user's mind. System developers must remember that users will actually be interacting with the system and their understanding is critical to system success. User documentation should be prepared with the same level of care as the actual system programs or system failure will likely result.

(6) Emphasis Should be Placed on the Training of all Personnel Involved in the EDP Function.

We cannot overemphasize the fact that proper training is required to orientate the user to his system-related responsibilities and familiarize him with the system, its capabilities and functions. The training should be informative and concentrate on what the user needs to know to effectively operate the system.

Additional training is also needed for data processing professionals. They should be aware of the exposures as well as the capabilities of distributed systems. They should be aware of the purpose and value of internal controls and the impact distributed processing has on traditional controls.

(7) Operating Controls Should be Cognizant of the System's Total Coordination Requirements.

Distributed system place a new level of coordination requirements on the system of operating controls. This aspect of system control is almost non-existent in traditional systems and must be analyzed and decisions made from a total system viewpoint. System scheduling requirements are part of these operating controls, and an important part of the user's procedures. The user must not only be infomred of what scheduling constraints he must operate under, but also what procedures to follow where delays are apparent. These decisions need to carefully consider the ramifications of delayed processing versus the results of processing with only partial data.

(8) Procedures should be Developed to Esnure the System-Wide Consistency of Duplicated Data Bases.

With the distribution of data to various nodes in a system, comes the requirement to develop reconciliation procedures to assure consistency between various nodes that may have duplicated data. These procedures should be based on the type of data duplicated, but at a minimum should require periodic reconciliations. There should also be an analysis of the conditions under which various users should request a reconciliation, as well as the determination as to which location ultimately controls the data. These types of decisions should be made early in the system's life cycle and should be understood by all system users. The criticality of these procedures increases with the amount of duplication, but the necessity for their existence can not be overlooked even if the replication of data is relatively small.

(9) Staffing Decisions and Specific Personnel Assignments Should Consider the Related Impact of these Decisions on Internal Controls.

Distributed systems can significantly modify the traditional segregation of duties concept of control over the various data processing functions. The distribution of functional responsibilities will typically result in a lowering of the level of data processing experience within the various functional areas. Personnel assignments within user groups must also consider non-system responsibilities in order to assure that reconciliation and other manual controls are not compromised. The traditional level of segregation of duties is probably unrealistic in certain user groups, but the value of this basic element of internal control cannot be ignored. There may be a need to increase the

level of system controls to compensate for the ineffectiveness of this traditional concept of internal control.

(10) Decisions to Self-Insure Against Catastrophe and Contingency Plans Should be Centrally Determined and Properly Documented.

In a distributed environment, it is critical that the impact of any level of system failure be evaluated in light of that failure on the total system. Isolated analysis of any one node can overestimate the value of that particular node or be unaware of total system capability. This is why we stress an overall evaluation from a system-wide viewpoint. When considering tne entire system, its capabilities and exposures, decisions can be made in light of overall system objectives and requirements and the vulnerabilities either eliminated or accepted. Once these decisions have been made, it is also important that they be formalized and transmitted to system users. They should understand the perspective from which these decisions were reached and their individual responsibilities in each regard.


DATE
FILME
8