1995

Auditing in common computer environments; Auditing procedure study;

American Institute of Certified Public Accountants

Auditing
Procedure
Study

Auditing in Common Computer Environments

AICPA
American Institute of Certified Public Accountants

Auditing in Common Computer Environments
AICPA

Statement of Policy

Auditing Procedure Studies are issued by the Auditing Standards Division and are part of the research program of the American Institute of Certified Public Accountants (AICPA). Each study is designed to inform auditors of developments and advances in auditing procedures. The studies present the views of the author or study group.

Auditing Procedure Studies are intended to provide practitioners with nonauthoritative practical assistance concerning auditing procedures. Comments on this study should be addressed to the Institute's director of audit research. Comments will be treated as public information unless a writer requests that his or her comments be kept confidential.

This Auditing Procedure Study has not been approved, disapproved, or otherwise acted on by the Auditing Standards Board, the membership, or the governing body of the AICPA. Therefore, the contents of this study, including the recommendations, are not official pronouncements of the Institute.

Auditing in Common Computer Environments

American Institute of Certified Public Accountants

Library of Congress Cataloging-in-Publication Data

Auditing in common computer environments / American Institute of Certified Public Accountants.
p. cm.—(Auditing procedure study)
Includes bibliographical references.
ISBN 0-87051-161-0
1. Auditing—Data processing. I. American Institute of Certified Public Accountants. II. Series.
HF5667.12.A92 1995
657'.45'0285—dc20 94-41127
CIP

1 2 3 4 5 6 7 8 9 0 AudS 9 9 8 7 6 5

Contents

Foreword

This study provides guidance to auditors when clients use microcomputers, local area networks, end user computing, database management systems, or telecommunications in conjunction with their accounting systems. It is part of the Auditing Procedure Study series of the American Institute of Certified Public Accountants (AICPA). It was prepared by the following task force of the Auditing Standards Board Computer Auditing Subcommittee:

Gary Riske, CPA, Chair
Kenneth Fullerton, CPA
James Hickman, CPA
David Haeckel
Michael Murphy, CPA
Paul Warner, Ph.D., CPA

Dan M. Guy
Vice President, Auditing
American Institute of Certified Public Accountants, New York

AICPA staff support was provided by Jane M. Mancino.

January 1995

Introduction

This Auditing Procedure Study (APS) identifies a number of electronic data processing (EDP) technologies and software applications that may affect the financial statement audit, describes how these technologies and applications work, and discusses possible ramifications for the financial statement audit. It is intended for the generalist auditor.

As use of new EDP technologies by business, government, and not-for-profit organizations becomes more pervasive, it becomes more likely that the use of such technologies by a client may have an effect on the financial statement audit. The effect on the audit will depend on a number of factors, including the following:

1. Whether or not the application generates a financial statement line item or provides a basis for an accounting estimate
2. The significance of the financial statement line item(s) affected by the client's use of technology
3. The controls placed over the application or system
4. The effectiveness of the design and operation of those controls

ORGANIZATION OF THIS AUDITING PROCEDURE STUDY

Each chapter in this APS is self-contained and can be read alone, although it may be helpful for the practitioner to read the entire text. A number of chapters include information that is relevant to other chapters. For instance, chapter 1, "Microcomputers," describes the use of microcomputers as stand-alone computers, while chapter 2, "Local Area Networks," describes how microcomputers may be used as part of a local area network (LAN). Chapters are cross-referenced to other chapters, as appropriate.

The appendixes that appear at the end of the book present detailed technical information, and a bibliography provides sources of further information.

Although the APS does not identify all possible effects of the technology on the audit process, each chapter discuss the impact of the technology on the following:

- The client's business
- Assessment of inherent risk
- The auditor's consideration of the internal control structure, including assessment of control risk and possible effect on substantive testing

Each chapter also describes possible recommendations to clients regarding controls over the technology or application. Appendix C includes scenarios that are not actual case studies, but that describe client situations in which the relevant technology is used. This APS devotes a chapter to each of the following technologies.

Microcomputers

Microcomputers have become an integral feature in many client accounting systems. Use may be confined to nonfinancial applications such as word processing or applications related to financial statements. Applications related to financial statements may include a complete general ledger system or an accounting subsystem to track, for example, the following:

- The detail of a financial statement line item
- Experience with loans as a basis for substantiating the adequacy of the allowance for loan losses

Local Area Networks

Microcomputers within an organization are often linked to form a LAN. A LAN enables users to access data files and programs from central file servers and other microcomputers in the network. LANs facilitate access to information, provide greater processing power, and permit more efficient use of computer resources.

End User Computing

A simple, yet common, example of end user computing (EUC) is the financial spreadsheet in which the user designs the calculations to be performed by the worksheet. In EUC, the user of the information, as opposed to a centralized management information system (MIS) department, is responsible for both the development and execution of the EDP application. Better segregation of duties is typical of applications developed by the MIS department (or non-end user computing) in that the MIS department develops, documents the logic of, and participates in testing the application.

Databases

A database system stores a collection of structured and interrelated data that can be used by one or more applications. Such a system makes it possible to maintain central control over information, yet allows that information to be accessed by many different users. This enables a more efficient use of resources since data required for more than one application need be stored on only one file.

Telecommunications

Telecommunications is the electronic transmission of information by radio, wire, fiber optics, microwave, laser, or other electromagnetic system. The information transmitted may be voice, data, video, facsimile, or other types of information. A telecommunications system consists of both hardware

and software. Examples of applications that use telecommunications are electronic data interchange (EDI), electronic funds transfer (EFT), and point of sale (POS) systems.

ASSESSMENT OF INHERENT RISK

Each chapter addresses the effect of inherent risk factors that are relevant to the client's use of that technology. Since the five technologies described in this APS do not give rise to the same inherent risk factors, each chapter addresses only those that are relevant to the technology under discussion.

In assessing inherent risk for each of the financial statement assertions, the auditor considers the effect of these factors in conjunction with the other factors unique to the client, such as a lack of sufficient working capital, or factors relevant to a particular financial statement line item, such as the susceptibility of an asset to theft. See AICPA Statement on Auditing Standards (SAS) No. 47, *Audit Risk and Materiality in Conducting an Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 312).

CONSIDERATION OF THE ENTITY'S INTERNAL CONTROL STRUCTURE

An entity's internal control structure consists of three elements: the control environment, the accounting system, and control procedures. SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319), states that, "In all audits, the auditor should obtain a sufficient understanding of each of the three elements of the internal control structure to plan the audit by performing procedures to understand the design of policies and procedures relevant to audit planning and whether they have been placed in operation."

SAS No. 31, *Evidential Matter* (AICPA, *Professional Standards,* vol. 1, AU sec. 326), states that most of the independent auditor's work in forming an opinion on the financial statements consists of obtaining and evaluating evidential matter concerning the assertions in such financial statements. These assertions are embodied in the account balance, transaction class, and disclosure components of financial statements and are classified according to the following broad categories:

- Existence or occurrence
- Completeness
- Rights and obligations
- Valuation or allocation
- Presentation or disclosure

In planning and performing an audit, an auditor considers these assertions in the context of their relationship to a specific account balance or class of transaction.

Possible Effect on the Auditor's Consideration of the Internal Control Structure

Controls implemented by management to provide reasonable assurance that the financial statements are complete and accurate may be integrated within the usage of the technology or external to it, in the form of input/output controls or exception reporting. Technology may be used in such a way that it is considered part of the accounting system. Thus, the auditor may need to gain an understanding of the flow of transactions through the system to gain knowledge of the internal control structure sufficient to plan the audit and design substantive procedures.

CONTROL RISK ASSESSMENT

The purpose of this APS is to identify the possible effect of specified technologies on the financial statement audit. In assessing control risk with respect to the financial statement assertions, the auditor considers many factors in addition to those relating to the client's use of the technologies described in APS. Also, technologies that might affect the auditor's control risk assessment for one client may have no such effect on another client for a variety of reasons. Also, the auditor may assess control risk at the maximum because he or she believes policies and procedures are unlikely to pertain to an assertion, are unlikely to be effective, or because evaluating their effectiveness would be inefficient. The auditor should consider the guidance in SAS No. 55 in assessing control risk.

Chapter 1

Microcomputers

Microcomputers are playing an increasingly important role in processing or generating financial data, a role that is attributable to the advent of electronic spreadsheets and the tremendous growth in the number of applications that are available. This chapter focuses on the stand-alone applications of microcomputers that may directly affect financial statements.

DEFINITION AND DESCRIPTION OF TECHNOLOGY

A microcomputer typically consists of the following:

- A microprocessor
- A minimum of 640 kilobytes of memory, and more often 4 million or 8 million bytes, or an even larger number of bytes of extended memory
- A hard disk of 40, 80, or an even larger number of megabytes of storage
- A printer
- A monitor
- One or two floppy disc readers

Microcomputers are normally used in one or more of the following configurations:

- Stand-alone personal computers (PCs)
- An element of a local area network (LAN), such as a network file server or intelligent terminal

EFFECT ON THE BUSINESS

Fortune 500 companies and small entities alike depend on financial information derived from microcomputers. Microcomputers may be used—

- For stand-alone applications.
- On networks that share data and peripherals.

- In links that connect the microcomputer to other computers, via modem.
- As terminals to regularly download data to or upload data from a mainframe or other computer system.

A larger client may use the microcomputer to run a general ledger package, analyze profits or cash flow with the aid of a spreadsheet, or maintain a database of customer information. On the other hand, such a client might use a laptop microcomputer. A laptop can interface with a network. It can be used to update a user's sales commission spreadsheet or link through a gateway into a corporate mainframe to query a database. Or it can download files to a hard disk, manipulate the data using a microcomputer database program, and upload data to a mainframe.

Some concerns for the entity using microcomputers are the—

- Use of incompatible software. A coherent management plan for the purchase of microcomputers might help to ensure the purchase of compatible software or computer operating systems. The use of compatible software reduces the risk of error, since there will be no need to transfer data from one format into another.
- Size of memory or disk storage, which may not be sufficient, especially if the entity's needs are growing.

EFFECT ON THE AUDIT

A client's use of microcomputers may significantly affect the auditor's consideration of the internal control structure and the assessment of control risk. Control risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by an entity's internal control structure policies or procedures.

Understanding of the Internal Control Structure

An entity's internal control structure consists of three elements: the control environment, the accounting system, and control procedures. According to Statement on Auditing Standards (SAS) No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319), the auditor should obtain a sufficient understanding of each of the three elements to plan the audit by performing procedures to understand the design of policies and procedures relevant to audit planning and whether they have been placed in operation. Use of microcomputers by clients may affect each of the above three elements.

The applicability and importance of specific control environment factors, accounting system methods and records, and control procedures that an entity establishes should be considered in the context of the following:

- The entity's size
- Its organization and ownership characteristics

- The nature of its business
- The diversity and complexity of its operations
- Its methods of processing data
- Its applicable legal and regulatory requirements

For example, a formal written code of conduct or an organizational structure that provides for the formal delegation of authority may be significant to the control environment of a large entity.

However, a small entity with effective owner–manager involvement may not need a formal code or organizational structure. Similarly, a small entity with effective owner–manager involvement may not need extensive accounting procedures, sophisticated accounting records, or formal control procedures, such as a formal credit policy, information security policy, or competitive bidding procedures.

Control Environment

There are a number of control environment factors that may relate to microcomputers. The following sections address these factors.

Management Philosophy and Operating Style

Management philosophy and operating style encompass a broad range of managerial characteristics. Such characteristics may include management's approach to taking and monitoring business risks, attitudes and actions toward financial reporting, and emphasis on meeting budget, profit, and other financial and operating goals. These characteristics have a significant influence on the control environment, particularly if management is dominated by one or a few individuals, regardless of the consideration given to the other control environment factors.

Organizational Structure

An entity's organizational structure provides the overall framework for planning, directing, and controlling operations. An organizational structure includes consideration of the form and nature of an entity's organizational units, including the data-processing organization, and related management functions and reporting relationships.

Methods of Assigning Authority and Responsibility

The methods used to assign authority and responsibility affect the understanding of reporting relationships and responsibilities established within the entity. The auditor might wish to inquire about the client's use of the following:

- Employee job descriptions delineating specific duties, reporting relationships, and constraints
- Documentation indicating the procedures for authorizing transactions

Clear job descriptions are important in establishing good internal control over microcomputers. Job descriptions can state (1) those functions that can

be performed on a microcomputer and (2) limitations on the use of utilities or other software, for example, to prohibit the unauthorized use of file-altering utilities.

The client may have documentation that describes the following:

- Functions to be performed by different personnel
- Procedures for authorizing transactions
- Procedures for authorization of systems changes, for example, altering data files, or performing file maintenance
- Responsibility for testing software, when applicable

Management Control Methods

Management's control methods affect management's direct control over the exercise of authority delegated to others and its ability to effectively supervise overall company activities. Control methods relating to use of microcomputers include policies for developing and modifying programs and data files.

Internal Audit Function

The internal audit function, if it exists, may include an auditor who is able to perform tests of the microcomputer systems. If in-house personnel are developing custom programs or spreadsheet templates, the auditor may wish to inquire about the extent to which internal auditors are involved in the testing of these custom templates of software programs. Internal auditors may also review procedures for backing up microcomputer files.

Personnel Policies and Practices

Personnel policies and practices affect an entity's ability to employ sufficient competent personnel to accomplish its goals and objectives. Personnel should be adequately trained in the use of microcomputers and software.

External Influences

External influences are those established and exercised by parties outside an entity that affect an entity's operations and practices. They include monitoring and compliance requirements imposed by legislative and regulatory bodies, such as examinations by bank regulatory agencies.

In the community banking environment, for example, a bank's accounting system can be run on a microcomputer. The outside auditor might wish to inquire whether the client has policies and procedures in place to review the requirements of outside regulators, such as EDP Bank Examiners. The questionnaires used by these examiners are often available to the outside auditor and may be reviewed to gain further information about the client. They might include, for example, requirements for backing up microcomputer files and storing them at an off-site location.

Accounting System

SAS No. 55 defines the accounting system as the methods and records established to identify, assemble, analyze, classify, record, and report an

entity's transactions and to maintain accountability for the related assets and liabilities. An effective accounting system gives appropriate consideration to establishing methods and records that will—

- Identify and record all valid transactions.
- Describe on a timely basis transactions in sufficient detail to permit proper classification of transactions for financial reporting.
- Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements.
- Determine the time period in which transactions occurred to permit the recording of transactions in the proper accounting period.
- Present properly transactions and related disclosures in the financial statements.

A microcomputer used for accounting applications may run a wide variety of software, ranging from off-the-shelf general ledger packages to custom in-house applications. Applications that normally affect the financial statement audit may include the following:

- Financial systems (general ledger, inventory, payroll, cost accounting)
- Spreadsheets used to prepare summary general ledger entries
- Database programs used to store financial data such as inventory records
- Utility programs, which are used for a variety of specialized functions such as backing up files, retrieving data stored on discs based upon a key word, or managing the microcomputer's use of memory space (Some utility programs can be used to bypass controls by directly modifying programs or file data.)
- Communications software (networking, terminal emulation, modem programs), which might allow a microcomputer to access financial data on another system

Control Procedures

The third element of an internal control structure consists of the control procedures. SAS No. 55 describes control procedures as "those policies and procedures in addition to the control environment and accounting system that management has established to provide reasonable assurance that specific entity objectives will be achieved." Generally, they pertain to the following:

- Proper authorization of transactions and activities
- Design and use of adequate documents and records
- Segregation of duties
- Documents to help ensure proper recording of transactions
- Adequate safeguards over access to and use of assets and records
- Independent checks on performance and proper valuation of recorded amounts

The auditor may inquire about the client's policies regarding the following:

Authorization of transactions. Authorizaton may be evidenced, for instance, by a manager's signature or by supporting documents.

Segregation of duties. The appropriate segregation of duties varies according to the size and complexity of the organization. Owner–manager review of output might be an effective control in a small owner-managed entity. In a larger entity, appropriate segregation of duties over microcomputers might be required.

Procedures for data input. Examples of typical control procedures for data input include approving journal entries by initial controls for entries to suspense accounts, batch control forms.

Access authorization. The existence, if any, of access authorization, such as program password control, may be relevant. Unlike a minicomputer or mainframe system, microcomputers often will not be implemented with password protection over data files and programs. Without that protection, a user may be able to enter any or all sections of a general ledger or other financial package, and perform file maintenance, for example, changing the address of an accounts receivable customer. Lack of access restrictions within a microcomputer program increases the need for the appropriate segregation of duties or owner–manager review. Password control may be installed over the operating system using a DOS shell program to prevent the user from accessing menu options of a program. Even if such a restriction exists, a sophisticated user can often bypass the DOS shell by using a utility. Therefore, the use of utility programs should be controlled or monitored carefully.

Security. Backup is the only protection for data disks, and the microcomputer against hardware or software failure in microcomputers. Diskettes or high-speed cassette tapes provide the primary means of backup.

Software controls. There may be software-driven controls such as exception reports and defined field parameters (ranges, field type, and parity checks). A comparison of subsidiary totals with control totals may be appropriate.

Spreadsheet controls. Control procedures over the development of microcomputer spreadsheet templates are an important part of spreadsheet development. For example, a client company may be using a spreadsheet to maintain a depreciation schedule. Control procedures to ensure the accuracy of the underlying spreadsheet formulas might provide a basis for assessing control risk below maximum for one or more financial statement assertions. The client or the auditor may use a spreadsheet auditor package for such purposes.

Assessing Control Risk

Assessing control risk is the process of evaluating the design and operating effectiveness of an entity's internal control structure policies and

procedures in preventing and detecting material misstatements in financial statement assertions.

In assessing control risk, the auditor considers whether evidential matter sufficient to support a reduced level of control risk is likely to be available and whether performing tests of controls to obtain such evidential matter would be efficient.

The auditor may conclude that the controls over microcomputers are directly relevant to the financial statement assertions and that such controls (in addition to others) would support an assessment of control risk below the maximum with respect to one or more assertions. In this case, the auditor may perform appropriate tests of control as a basis for assessing control risk below the maximum. Tests of controls in the microcomputer environment would, most likely, relate to controls in the accounting system, other than those embedded in the microcomputer software and hardware.

AUDITOR'S RECOMMENDATIONS TO CLIENTS

Auditors can provide the client with useful management recommendations by noting security problems and the matters relating to the internal control structure, such as those described above, and by identifying areas in which microcomputers could be used to improve efficiency. Examples include converting manual operations to computerized accounting systems, automating budget functions, computerizing customer records, and linking microcomputers and mainframes together with a network in order to achieve file-sharing.

Software Piracy

It may come to the auditor's attention, in the course of the audit, that there is unauthorized copying of software by employees or software piracy. Unless a client has a site license, no more than one copy of a purchased program should normally reside on a computer disk drive at any time.

Software piracy is a violation of federal law and the entity is legally responsible for the action of its employees in this respect. In addition, almost every state has passed statutes addressing software piracy. Software vendors can and have identified and brought charges against entities that copy software without proper authorization. Therefore, an entity that allows unauthorized software duplication is running the risk of being liable for fines or damages.

In any event, the auditor should follow SAS No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards,* vol. 1, AU sec. 317), if specific information concerning possible software piracy comes to his or her attention.

Microcomputer Software and Viruses

Computer viruses can cause the loss of data and programs. A virus has the ability to attach itself to a program and infect other programs and systems. Although some viruses merely write messages across the screen, others can

cause serious damage to disk files or shut down a network by replicating millions of times and filling all available memory or disk storage.

Methods to prevent the introduction of viruses in a microcomputer system and to recover from a virus attack include the following:

- Obtain recognized software from reputable sources and only accept delivery if the software is in the manufacturer's sealed package.
- Make multiple generations of backups. A virus that is not detected initially may be copied onto more recent backup copies, while the older versions may not be infected.
- Prohibit the use of unauthorized programs introduced by employees.
- Prohibit downloading of untested software from sources such as dial-up bulletin boards.
- Use virus protection software to screen for virus infections.

Chapter 2

Local Area Networks

Local area networks (LANs) are in use in entities of all sizes. For smaller entities and their auditors, LANs may be the first encounter with complex formal computer applications and powerful processing environments. Large LANs that support many users and resources can be placed under controls comparable to those in traditional mainframe systems. In any case, the auditor may be able to assist the client in developing effective application and system controls. Strong controls may enable the auditor to lower the assessed level of control risk and thereby change the nature, timing, and extent of substantive audit procedures necessary. This chapter addresses the use of microcomputers as elements of LANs.

DEFINITION AND DESCRIPTION OF TECHNOLOGY

A LAN is a communications facility that interconnects computers within a limited area. LANs are distinguished from other networks by their limited span of control and use of specific data transfer technologies. LANs typically have the following characteristics.

- LANs are local. They link equipment such as workstations, printers, and various other devices that are usually within a single building or a small cluster of buildings.
- LANs are private in the sense that they are usually used only for intra-company traffic and are not shared like public telephone networks.
- The computers and devices connected by a LAN do not lose their individual capabilities because they have been connected by a LAN.
- LANs are based on commercially available technology. Although custom-built LANs can be used, commercial LANs are generally more efficient and cost-effective.
- LANs can connect every device on the network to every other device on the network.

LANs are widely used for a number of reasons. They allow the sharing of resources so that every network workstation can use application software,

data, printers, other hardware devices, and access to services (server functions) with the other users on the LAN.

An excellent power-to-cost ratio can be achieved by connecting the least costly computers via the least costly high-speed communications media to form a LAN. In addition, often, a LAN can be inexpensively implemented with existing computer equipment.

There is a rapidly growing number of commercially available software packages to support server features. As a result, very complex new applications can be supported on LANs.

LANs are used for a wide variety of applications, ranging from the relatively simple, such as electronic mail, to complex strategic decision-based information systems designed to improve competitive positioning. A LAN comprises (1) the network software, (2) the physical pathway from device to device, and (3) the computers and other hardware devices that communicate on the network. These major components are described briefly in the following sections and in more detail in appendix A, "Local Area Network Technology and Terms."

Local Area Network System Software

A LAN transfers data or programs from one computer or other device on the network (a station or workstation) to another station. Software is needed so that the devices can function cooperatively and share network resources such as printers and disk storage space.

The network system software may reside on a stand-alone network server, or it may reside partially or completely on the network interface cards (see the following section, "Hardware Components") or it may operate as an application on one or more of the workstations.

Server is the term used to describe both the device on which the service function resides and the software through which LAN workstations share resources. The implementation of a specific server option is accomplished by installing software on all workstations, which invokes the software on the appropriate server machine.

Common service functions include the following:

Network server manages access to the network and serves the needs of the network.

File server provides shared storage space for files and allows multiple users to have access to the files.

Print server permits sharing of a common printer or printers by all workstations on the LAN, and handles their printing requirements.

Communications server manages access to the communication devices on the LAN.

Depending on the network configuration, server functions may be run on one computer, or on multiple computers and other hardware devices on the network.

Hardware Components

The following list summarizes and defines the most important hardware components.

Workstations are the microcomputers and other microprocessor hardware that have been configured to run on a network.

Peripherals are input/output devices such as printers, magnetic tapes, disks, optical scanners, facsimile boards, and modems that provide support for data entry, data storage, and data output.

Transmission media constitute the physical path that connects the different components of the LAN, generally twisted-pair wire or coaxial cable.

Network interface cards connect the workstation and the transmission media.

Network Management

Network management has become an increasingly important issue as networks become larger and more complex. Network management functions include the following.

Fault management maintains high availability of network services and resources.

Configuration management initializes and establishes intended network relationships.

Performance monitoring provides efficient service with acceptable response times and throughput.

Security management defines and regulates access to network resources via authentication, authorization, and encryption.

Accounting management tracks network usage.

Local Area Network Application Software

Emerging developments in microprocessor and network operating systems will promote development of multiuser and integrated applications by providing multitasking, more memory, faster processors, and programming interfaces that facilitate applications development.

The three basic kinds of LAN application software are single-user, multiuser, and integrated. The following sections briefly discuss each application.

Single-User Applications

Applications for single users are written for use on one computer by one user. The application software is stored on a file server and used by LAN users at their workstations. Control and security problems can arise if two users try to use a single-user application at the same time. For example, if two users use a spreadsheet package at the same time and work on the same spreadsheet,

the person making the last change to the spreadsheet will overwrite all the changes made by the first user.

Multiuser Applications

Applications for multiusers are designed to be used by several users at a time. They have concurrency control features such as file and record locking to coordinate usage. Multiuser applications make up the majority of programs written for networks.

Integrated Applications

Integrated applications usually share the processing power of several computers. For example, a user request can be passed to a back-end database server where the records are stored. Data, which is found on the database, is then sent to the *front end* workstation for further processing. Both the application and computer general control procedures are spread across multiple computer devices.

EFFECT ON THE BUSINESS

A number of key business issues should be considered in selecting and installing a LAN. Because LANs are relatively inexpensive, automated systems may proliferate. There is the danger, however, that decision making will fall to people who are neither trained nor experienced in managing the security and other control issues of information technology.

LANs can rapidly grow from relatively simple systems to highly complex systems even when implementors are initially in control.

LANs can be used to support very complex applications that are difficult to manage and support outside of a traditional management information system (MIS) organization.

EFFECT ON THE AUDIT

Understanding of the Internal Control Structure

To the extent that applications relating to significant financial statement assertions are being processed in a LAN environment, the auditor should obtain an understanding of the elements of the internal control structure as they relate to such applications. The understanding should include the computer-based components of the accounting system and related control procedures, to the extent considered necessary by the auditor.

This may include the configuration of the LAN, including server and workstation hardware, the locations of the workstations, and the operating system, network software, and network management software, if any. Computer general control procedures, such as controls over access and changes to application programs, may also be considered.

Assessing Control Risk

The focus on fast communication and easy access to data led to the development of LANs that are often outside the control of MIS departments. As a result, many of the orderly development processes common in traditional systems may not have been followed. However, LANs can be controlled in such a way as to support a lower assessed level of control risk.

There are a number of possible inadequacies of control procedures to be considered by the auditor in making this control risk assessment. General control procedures (including controls over development of new programs, changes to existing programs, access and computer operations) are not likely to be as formal or as rigorously applied as those in centralized MIS environments. There may be much greater emphasis on end user controls in a LAN environment; end users may not always be control-oriented.

LAN system users may not have adequate resources for problem resolution, troubleshooting, and recovery support.

The ability to impose rigorous separation of functions through access control software and accountability through logging mechanisms serves to enforce a stricter segregation of duties.

The continued operation of control procedures is dependent on good management controls. These include, for example, the management of access codes and passwords and timely reaction to evidence of control breakdown or degradation.

Safeguards over assets, including computer-based accounting records and computer programs, must be in place. These include backup and recovery procedures.

The effectiveness of the security and access control procedures built into LAN networks varies widely and is a function of the capabilities as well as the installation and management of the LAN software. LAN operating software generally does not provide the security features available in midrange or large-scale computer environments, although improvements are continuously being made. The access controls generally present in a LAN may not be appropriate for applications with highly sensitive data.

The audit may also be complicated by a mixture of multivendor software and equipment accompanied by the absence of audit trails.

Designing Substantive Audit Procedures

LANs offer a number of possibilities for the effective and efficient use of computer audit techniques, including audit software and the transfer of data to the auditor's microcomputer for processing and analysis.

The auditor may find that the use of LAN technology results in a paperless transaction processing environment where much of the traditional audit trail has disappeared. The use of computer assisted audit techniques (CAATs) may be the only effective way to gather and analyze audit evidence in this environment. A complete and accurate understanding of the LAN environment as well as the computer-based application is important for the effective use of CAATs in this situation.

Audit software can be used to access the potentially large amounts of data stored in LAN systems, especially if many file servers are spread across the

network. Because LANs generally are microcomputer-based, the auditor can normally use a wide range of microcomputer-based spreadsheets and database products to perform this work.

The auditor may be able to use a workstation on the network to access remote data if audit capabilities are built into the application, or may arrange for data to be transferred electronically to a workstation where it can be examined by audit software.

AUDITOR'S RECOMMENDATIONS TO CLIENTS

In addition to recommendations to clients on the control of computer-based systems operating on the LAN, the auditor can consider the following areas in forming general comments:

- Effectiveness of management control over the LAN planning, acquisition, and installation process
- Adequacy of implementation and conversion plans
- Access control procedures and monitoring
- Training and competence of users, MIS
- The adequacy of the audit approach, especially during initial audits, if internal audit performs work involving LANs

Chapter 3

End User Computing

End user computing (EUC) activities are significantly influencing entities today and present the auditor with the challenge of understanding these activities sufficiently to make appropriate risk assessments and plan appropriate audit procedures. Not all EUC activities have direct or significant audit implications. For those that do, however, the auditor must have a clear understanding of how they were developed and how they function to execute an effective audit. This chapter describes how EUC might affect the audit and the financial statements of clients.

DEFINITION AND DESCRIPTION OF TECHNOLOGY

The common thread in the various kinds of EUC defines it for purposes of this chapter: An end user is responsible for the development and execution of the electronic data processing (EDP) application that generates the information employed by that same end user. That is, the user has substantially eliminated the formal management information system (MIS) department from the process. EUC can be performed in a stand-alone environment on a laptop personal computer (PC) or in a formal information center environment, using files privately held on mainframe storage.

Actually, the objective of EUC is to put resources in the hands of the users. From an audit standpoint, the concerns center on the manner in which EUC is used and implemented, and the effect on the audit and the financial statements.

EUC can use, or be influenced by, a number of information technologies and approaches. The reader is encouraged to refer to chapter 1, "Microcomputers," which are often used as the primary hardware tool in EUC; chapter 2, "Local Area Networks," which are critical to the downloading and uploading of data under EUC; chapter 4, "Database Management Systems," particularly when the end users create their own database in an EUC environment; and chapter 5, "Telecommunications," which links the other pieces. Following are three examples of end user systems, functions, and audit issues.

Example 1

System Description

This is a loan system application for a $4 billion commercial banking organization. The midrange system supports the EUC activities. The midrange system communicates with the bank's primary system, the mainframe. This is generally limited to access of information in the mainframe environment, meaning that there is little information input throughout the midrange system. The end users make use of various proprietary system utilities, including the report generator and the communications software.

End User Functions

The loan system contains all loan information, including that pertaining to customers. The bank uses it for all aspects of marketing, including the marketing of products and the measurement of market penetration. Other applications include asset and liability management, liquidity analysis, risk analysis (for example, concentrations, industry analysis, and collectibility), and to support the analysis of adequacy of the allowance for loan losses.

Audit Issues

The auditor may be interested in several operational and audit issues. Operational issues include how the bank provides for backup, confidentiality of records, and virus protection and response. Audit issues include the validity of the analysis of the allowance for loan losses.

Example 2

System Description

This system provides a retail company with a general ledger application, as well as inventory, accounts payable, and accounts receivable subledger applications. The end user activities are supported by the entity's primary system, the minicomputer system. The end users make use of various proprietary system utilities, including a file utility, communications software, and report generator.

End User Functions

The data for the various applications are used for direct mail marketing and developing market strategy. Other uses are planning purchases, analyzing inventory levels, and developing liquidation strategies. The data also support the company's analysis of the adequacy of the allowance for doubtful accounts.

Audit Issues

The auditor may be interested in several operational and audit issues. Operational issues include how the company addresses backup, virus protection and response, and general ledger access. Audit issues include the validity of the analysis of the allowance for doubtful accounts, and the analysis of inventory levels that might affect inventory obsolescence issues.

Example 3

System Description

This network of PCs lacks direct access to the manufacturing company's mainframe. Information requested from the main processing system must be loaded onto tape and then downloaded to the PC network via tape drive. There is no dedicated file server, and users share applications and data freely.

End User Functions

The users compare marketing data and trends with their own. Another group monitors production data, including cost variance analysis. Backlogs and cancellations are also closely monitored to avoid buildup of inventory. This system is used to support the company's inventory obsolescence analysis.

Audit Issues

The auditor may be interested in several operational and audit issues. Operational issues include how the company addresses backup, the confidentiality of records, and virus protection and response. Audit issues include the validity of the inventory obsolescence analysis.

EVOLUTION OF END USER COMPUTING

In the traditional data processing environment, all information needed by users is delivered by programs purchased or written and tested in the MIS department. Any changes or modifications to the content or format requires formal request forms, appropriate authorization, and a waiting period for the changes to be implemented. Delays in implementation and systems that do not match user specifications increasingly result in frustration for decision makers and other users of information. As timely information becomes critical to an entity's ability to compete, such delays become increasingly unacceptable.

Hardware, software, and microchip makers provided a solution to the preceding problem by putting tremendous computing power into the hands of users. Desktop microcomputers have more computing power than the minicomputers of just a decade ago. If these machines or special function devices are used as intelligent terminals, or workstations, they may use both their own resources as well as exploiting the memory and computing power of a host mainframe or minicomputer.

Along with the improvements in hardware, the most significant factor in the vigorous growth in EUC has been the development of higher level software languages known as fourth-generation languages (4GLs). In fact, microcomputers and 4GLs appeared about the same time. General characteristics of 4GLs include the following.

- They are user-friendly.
- Programming can be performed by a nonprofessional.

- Programming code is principally nonprocedural (that is, developers code what is to be accomplished and not how to accomplish it).
- In their simplest form, they are easier to maintain and understand compared with prior languages, even for someone other than the developer.
- They are easier to learn; for example, they often can be self-taught.
- They are easier to debug.
- Results can be obtained in significantly less time than with third-generation languages.

With a well-designed 4GL, a user can develop in a short period of time an application that delivers the desired results, focusing on the problem to be solved rather than on how to program.

Not only is the hardware and software used in EUC dramatically more sophisticated than even a decade ago, but the applications are more sophisticated. Early EUC applications tended to be simple word processing and spreadsheet functions. These applications saved time by eliminating a number of redundancies and improving clerical accuracy. Although these applications are still widely used, much more advanced functions are being performed in the EUC environment. Many user-developed applications can become critical to the entity as a whole.

In a number of organizations, the traditional MIS function remains the optimal choice for filling information processing needs. In other organizations, however, EUC is a more viable solution, whether on a stand-alone basis or in concert with traditional MIS services. The relatively low cost of putting this computing power directly into the hands of users has accelerated the acceptance of EUC. It is not uncommon for entities to empower virtually every employee with some level of EUC capability.

The MIS department is responsible for the development of policies and procedures that ensure adherence to adequate data access and physical access controls. Issues such as software version control, data security and integrity, hardware standardization, and acquisition guidelines fall under the umbrella of this department or a separate information security function.

In an EUC environment, however, the relatively low individual cost of the system components makes them available to individual departments within the entity. As a result, users can purchase computing power with their own budget dollars and bypass the approval process and time delays traditionally associated with the MIS department. Users generally decide which hardware and software will be purchased, and how those resources will be used and controlled.

POSSIBLE END USER APPLICATIONS

Any application with the following attributes may be a candidate for EUC.

- Users are unable to obtain new applications and changes in a timely manner.

- Programs developed by the formal MIS function have errors or simply fail to work as a result of poor systems development life cycle controls.
- Systems developed by the formal MIS function do not match user requirements.
- Communication between MIS and users is ineffective.
- Users are unable to decipher system specifications developed by MIS.
- Systems are expensive to develop and maintain.
- Critical decision-support systems are never implemented because of long development time.
- Routine analyses or reconciliation procedures are performed manually.
- An application will be rarely used or is a "one-shot" application.
- The application is a prototype for a significant system.
- The application is used by either only one person or a very few people.

Generally, users are developing applications and systems based on the availability of hardware and 4GL or other easy-to-use software. Most of these applications are still simply extractions from a database (or part of a database), report generators, and spreadsheets. However, a number of significant systems are in use that were developed by end users, particularly in the data entry area.

An understanding of how a particular EUC application affects the entity as a whole is critical to properly assessing risk. It is important to know not only how data are accessed and shared, but how the results of the application are used (for example, for critical decision-making or inputting to another application).

EFFECT ON THE BUSINESS

The centralization of data processing activities facilitates control over the development of applications, access to data files, and the security of hardware, including backup procedures and contingency planning. A number of organizations have established information centers to maintain some control over these processes, not only centralizing hardware and software acquisition and maintenance, but also providing training and direct application development assistance to users. In a number of cases, these centers have established formal controls over the development and implementation of EUC. In other cases, the centralized information center has been eliminated or is being phased out. If data processing functions are delegated to the end user, MIS either no longer functions or functions less effectively as the *central* or general control group.

An EUC environment can assume one of the following three forms, depending upon the approach taken by the entity. (1) EUC can exist as a microcomputer environment, with no central functional control. (2) It can also exist "side-by-side" within an MIS environment, but not linked to the

data-processing operations. (3) It can be fully linked to the MIS functions of the entity.

In a decentralized environment where EUC is assuming increasing importance, the entity is faced with heightened operational risks related to the following:

- Acquisition and use of hardware
- Acquisition and use of software
- Application development
- Logical access to sensitive data
- Physical security of data and systems

These risks may be compounded by the fact that many user-developed applications can become critical to the entity as a whole over time or as a result of change in volume of transactions or activity.

Acquisition and Use of Hardware

An entity heavily involved in EUC without standard policies relating to the acquisition of hardware could easily suffer significant waste of its resources. The coordination of departments involved in EUC activities will mitigate this risk.

Generally, entities have a significant investment in hardware and in a number of cases have not given adequate consideration to protecting and controlling their investment. Inattention to the hardware and its purchase may result in any one of the following problems:

- There may be duplication of time-consuming research to identify the products most suited to the entity's needs.
- Individual departments may negotiate with vendors for their purchases only, even though the entity as a whole might be able to negotiate better price and support terms.
- There may be unnecessary duplication of hardware, such as printers and storage devices, that could be shared efficiently.
- Systems that have been improperly installed place at risk the investment that the entity has made in the hardware and create safety hazards. For example, microcomputers should be used with surge protectors and the wires that attach to peripherals (such as printers, communications modems, and display terminals) should be organized and stored out of the way.
- Lack of standard maintenance procedures result in units that are not being maintained properly.
- Communications capability within a microcomputer environment without any standards or controls may, by some estimates, increase telephone costs by 30 percent to 50 percent. Additionally, time-sharing costs (where applicable) can become excessive.

The degree of risk to the entity is a function of the following:

- The criticality of the EUC applications
- The level of connectivity between EUC and MIS
- The breadth of distribution of EUC output
- How EUC fits into the entity's strategic plan (that is, whether EUC will become more or less critical to business continuation)

Acquisition and Use of Software

The unique information needs of user groups drive EUC and complicate the software acquisition process. The purchasing of software without centralization can easily breed frustration and inefficiency for users.

Informal purchasing procedures can result in various groups using incompatible software products or different versions of the same software. Otherwise, very valuable information may not be transferrable among different applications (for example, from a database program to a different vendor's spreadsheet program). A more frustrating situation occurs if users cannot access information from a shared storage device because the information was created with an incompatible version of the same application (for example, one database program to another database program).

Poor planning and coordination also may result in shelves of unused software. This indicates inadequate training and educational planning within an entity. Entities waste thousands of dollars on software products that are not properly researched and that, therefore, do not meet the needs of the intended users.

Entities can reduce these risks with guidelines or policy statements addressing the acquisition of software. Guidelines should include a requirement to justify the acquisition of software and identify any hidden costs, such as training or hardware enhancements. Users should also provide a requirements definition of the needs that the solution must satisfy. This procedure should require the input of all user groups who may need to use this product in the future to ensure that it has an appropriate amount of flexibility and growth capability. Finally, an evaluation of applications developed in-house should be included in the software selection process.

Policies addressing software acquisition and use should be commensurate with the risks involved. For example, policies for software for personal computing only can be very informal. The cost of personal computing is low and the results are not used for critical decision making or as input to other systems. On the other hand, stringent acquisition guidelines should apply in a number of circumstances. One is acquisitions and installations that involve a relatively significant investment of dollars or manpower. Another is software that will be used by a number of people within an entity or that will be used to produce output that is relatively critical.

Most applications are developed in spreadsheets, 4GLs, or report writers. Individuals involved in EUC must be given direction and guidance to prevent complex applications that consume a significant amount of time, even though an equivalent application could be purchased relatively cheaply or may be already available elsewhere in the entity.

Application Development

The application development process (how an idea is transformed into a working system with relevant data and program steps performed on or with that data) is particularly vulnerable in an EUC environment. Generally, end users have no training in the formal application development process. Accordingly, applications developed by end users are often inadequately tested and the development process is often not documented. This situation can cause significant difficulties for an organization if the EUC applications are critical to making business or financial decisions. Program maintenance becomes extremely difficult without proper development documentation, even in 4GLs.

Poor planning and design may eventually leave an entity with many incompatible end user applications. In a number of entities, this will not be a significant issue because the EUC applications may never need to be part of a coordinated information system. However, it is good policy and business practice to have general guidelines for application development that will facilitate integration.

Logical Access to Sensitive Data

The ability to use data resident on mainframes or to send the results of the application to the corporate mainframe is critical to the functioning of many end user applications. This downloading and uploading of information, if uncontrolled, can have an adverse effect on operations and financial reporting. In a shared information environment, controls should be in place to ensure that the proper data are being used and protected against the unauthorized access.

The following are access risks, not necessarily unique to EUC activities, that should be addressed by the entity:

- Users may access confidential or proprietary data which should not be available to them.
- Data may be manipulated by EUC in such a way that the database is corrupted.
- Data may be vulnerable to irregularities.
- Unauthorized transactions may be entered into processing.
- Data may be accidentally erased.
- Performance of the operating system may be impaired.

These risks are described in a general way and will be affected by the number of EUC applications, the nature of EUC activities, and the volume of EUC accesses to the mainframe.

One of the major drawbacks of most 4GL report writers is their inability to restrict access. They usually come with on-line systems that are capable of restricting users to specific applications, specific departments, or even specific fields. Often, however, these access restriction facilities are not implemented, either in total for the systems, or with respect to who can access and use the report writer with read capabilities. If no access security has been implemented over any of the system, users with access to the

report writer have access to all fields in all files. This is a concern if the report writer capabilities are restricted to reading, but it becomes an even greater risk if update facilities are available within the report writer.

It is often impossible to restrict users of such facilities to specific areas of information. There are similar problems with uploading features, if this facility is available at all. The user performing the upload or running the report writer may have no intention of abusing his or her privilege. Nevertheless, for most microcomputers, lack of control means that other users can gain access.

As is more fully discussed in chapter 1, "Microcomputers," viruses also represent a risk. Viruses are programs that are designed to delete or corrupt data or programs, or otherwise disrupt processing. They are triggered by normal operations, and, once triggered, cannot be easily stopped other than by switching off and reverting to a clean backup. Connected systems will transmit viruses freely. An example is LANs, which are as described in chapter 2 "Local Area Networks." Virus detection software is available.

Physical Security of Data and Systems

Physical security, primarily backup and contingency planning, often is ignored in the EUC environment. Lack of training about security issues lead to a lack of appreciation of these issues among users. Since some end user applications are as essential to the entity as those maintained on the mainframe, it is imperative that backup and contingency planning be addressed by the end users.

Poor backup procedures can result in the loss of important data that are very difficult, time-consuming, and costly to recreate, if they can be recreated at all. Critical applications and files should be stored off-site with corresponding documentation in the event that on-site files become unavailable. The master copy of manuals pertaining to all security software and hardware should reside in a central group, as well as at a centralized, off-site, secured location, which may also be used for storing backup copies of software and corporate data.

The sensitivity of the EUC activities should guide the entity's security decisions. Data frequently seen on microcomputers that would be considered confidential include the following:

- Personnel data
- Cost information
- Customer lists
- Senior management memoranda
- Engineering design information

EFFECT ON THE AUDIT

The auditor may encounter EUC systems that affect the audit approach and conclusions in a number of circumstances. These may include the following:

- Distribution of the accounting function to end user applications

- Areas in which separate supporting systems have been developed to help responsible individuals make decisions; for example, accounts receivable credit decisions or writeoffs, inventory obsolescence, sales commissions calculations
- Treasury functions (such as investment portfolio activity)
- Footnote disclosure in which the detailed information is retained and managed outside of the MIS function (building and property lease data, stock option information)

The auditor may find that an entity has various EUC activities, none of which affects significant financial statement assertions. In this case, the auditor need not evaluate the EUC activities further. Nevertheless, the auditor may choose or be asked by the client to perform a number of additional procedures in this area.

Assessing Inherent Risk

The inherent risk factors that are discussed in the following section are those that are more commonly affected by the existence of EUC in a client environment. The auditor should also consider the effect of other inherent risk factors arising from unique client circumstances.

If the auditor assesses inherent risk for a significant financial statement assertion, the relevance of EUC activities to that assertion should be considered. End user developed applications are not always adequately tested before implementation. Inherent risk is further affected because more client personnel need to understand EDP control concepts and also how their piece of the EUC fits into the entity's financial accounting system as a whole. Other factors the auditor may wish to consider include the following:

- Adequacy of testing of the application before implementation
- Whether management reviews the results of the application
- Whether old or existing applications have been updated or reviewed for current applicability and accuracy

Although the assessment of factors that affect inherent risk should be made at the assertion level (rather than at an entity-wide level), the auditor will typically find these factors to be pervasive.

Understanding of the Internal Control Structure

The auditor gains an understanding of an entity's internal control structure sufficient to plan an audit. It is during this process that the auditor would normally become aware of EUC activities that affect the audit. EUC has an extremely wide range of usage, from personal applications to critical entity-wide applications. The auditor should consider the nature of an entity's EUC activities (for example, in the most fundamental sense, "How is EUC being used by the client?"), and use judgment when evaluating or recommending control policies and procedures. Other factors that should be taken into account when determining the impact of EUC include the following:

- The significance of EUC to the financial statement assertions
- The degree of dependency the client has on the data or application software
- Whether EUC is being used to accumulate data over a significant period of time or from a wide range of sources for reporting or analytical purposes
- The sensitivity of the data

Assessing Control Risk

Internal control structure policies and procedures will vary significantly by entity due to the wide range of possible EUC activities. As noted earlier, however, the focus for the external auditor will be primarily on EUC activities that affect financial reporting. Most of the relevant risks have been discussed in previous sections of this chapter. Although the overall control risk assessment in some cases may not change because of EUC (when contrasted with a centralized MIS), it is at least significantly affected by the fact that there may be many more places to look for controls.

Control Policies and Procedures

To ensure that EUC applications process data completely and accurately, the auditor should generally look for control policies and procedures that—

- Require all significant end user applications to be adequately tested before use.
- Prescribe documentation standards for significant end user applications.
- Provide for adequate access controls to data resident on the microcomputer as well as data available for downloading from the mainframe.
- Record access of the database by EUC applications.
- Provide a mechanism to prevent or detect the use of incorrect versions of data files.
- Require a level of backup that is compatible with the critical nature of the applications and data files to be maintained on-site and off-site.
- Provide for appropriate applications controls (for example, edit checks, range tests, reasonableness checks).
- Support meaningful programmed or user reconciliations.

Hardware and software acquisition procedures are important to an entity but, since they do not have direct audit implications, they are not discussed here. On the other hand, application development standards help ensure the integrity of output. The minimum standards of program development documentation should generally include the following:

- Summary of the program objectives (business purpose) and design characteristics
- Unique processing requirements

- Data definitions, including record layouts for machine readable data
- Operating procedures, including start-up and back-up procedures
- Testing plan and actual output from previous tests

As the applications become more complex, the development documentation should be similar to that expected in a formal MIS development process.

Access control is such an important issue that many entities employ information security specialists to protect corporate information assets. The following procedures (which will not necessarily require the services of a specialist) will serve to minimize logical access risks associated with EUC activities:

- Password and user ID administration procedures
- Use of menus for EUC access to the database
- Use of EUC applications as prototypes for more efficient coding if the applications become significant to the entity
- System protection through parameter files, for example, to restrict uploading to only the budget and forecast records
- Transaction processing of uploaded data, which subjects the data to the same level of validation, authorization, and reporting control as any other transaction
- Batch processing of uploaded data, with control totals of what has been uploaded produced by both the EUC system and the mainframe system, and procedures in place to review and agree control totals
- Regular independent review of the transactions input by means of EUC

Password and security guidelines are typically established centrally; however, for those guidelines to be implemented successfully, they must be the user's responsibility.

Once taken outside the controlled MIS environment, access controls become much more difficult for organizations to administer and much more dependent upon individual users. Clients who download sensitive information onto microcomputers should consider the following additional security measures:

- Physical clamps or chains to prevent the removal of hard disk computers or their internal boards
- Control over access from outside (for example, using dial-pack protection)
- Security software to limit access to those who know the correct user identification and password
- Diskless workstations
- Regular back-up and archive procedures and secure, remote storage facilities for these copies
- Commitment to security matters written into job descriptions or employment contracts and personnel evaluation procedures.

Once an organization commits itself to EUC, there must be back-up and data recovery procedures similar to those required for a traditional mainframe or minicomputer environment. The entity should also have a disaster recovery plan (or perhaps more appropriately, a business resumption plan).

Tests of Controls

Tests of controls can often be performed simultaneously with gaining an understanding of the internal control structure. This approach is usually the most efficient and involves some combination of inquiry, observation, and inspection of documentary evidence. Specific procedures may include extended walk-throughs of applications, review of documentary evidence of compliance with standards, simulated processing, or processing of test data. Typically, inquiry alone is not sufficient evidence of effective operation of controls.

EUC applications often are less likely to have effective controls over access and system development and program changes controls than applications under centralized MIS control. The auditor should perform tests of controls before assessing control risk at less than the maximum. Use of evidence obtained in prior years should be carefully considered for the same reasons.

Designing Substantive Audit Procedures

The extent, nature, and timing of substantive audit procedures applied to significant financial statement assertions will depend on the inherent and control risk assessments. The auditor may find it useful to classify the results of EUC activities into those that have a direct effect on financial statement assertions and those that have an indirect effect. This classification will help the auditor determine the most effective and economic approach to substantive auditing.

If the results of the EUC activities have an indirect effect on the financial statement assertion, the auditor may obtain sufficient evidential matter without directly testing the EUC application. That is, the auditor may obtain the evidence from other sources. For example, although the maintenance of inventory purchase records in an EUC application may provide data used for testing accuracy and ownership of the inventory, evidence will likely come from observation, vouching, and confirmation.

However, if the results of the EUC activities have a direct effect on the financial statement assertion, the auditor may perform different substantive procedures. For example, these will likely include a combination of the following (determined by cost effectiveness in the circumstances):

- High-assurance substantive analysis techniques using independent data (that is, analytical tests that provide a high degree of audit evidence about the financial statement assertion)
- Recreation of the results with software written by the auditor
- Detailed testing of the results using a sampling plan

For example, if the allowance for uncollectible receivable accounts is determined based on results of EUC activities, the assumptions used in the model can be analyzed and the computation reperformed.

Even though in the past, a review of program code might have been considered a viable option for substantive testing, it is rarely if ever used today, especially in light of the evidence that can be gained from a combination of the foregoing procedures.

The auditor's selection of substantive procedures will also be affected by the dispersion or even the loss of the transaction trail. For example, recomputation of the activity in an account is more complicated if, because of EUC, a single file of transaction activity does not exist. In this case, sampling from each of the subpopulations may be a more efficient approach, particularly if the inherent risk and control risks for each subpopulation are different.

AUDITOR'S RECOMMENDATIONS TO CLIENTS

As a client service, the auditor may consider the entity's planning, organization, and policy and procedures guidelines to determine how well EUC is managed.

The client entity should have a comprehensive MIS plan that is reviewed at least once a year. This plan should incorporate all hardware platforms—mainframes, minis, microcomputers, and other office systems. One of the most critical elements for success is the entity's continued commitment to supporting EUC. This will provide for the proper maintenance of standards in hardware, software, and operating systems.

With the dispersion of data in an EUC environment, it is important that the entity have an information (data) security policy to protect corporate information. Provisions should be made for data ownership and privileges that establish who creates and owns the data, who can change the data, and who can view but not change. Various forms of data protection are needed—both physical (for diskettes and tapes) and logical. Control over both the accuracy and completeness of data over time is also needed. The policies should also address environmental matters (electrical, humidity, and heat), and business resumption issues: More people must practice good habits concerning backup and recovery in order to avoid negatively affecting the operations of the entity.

There is an increased risk that the entity will inadvertently rely on end user prepared data. For example, there may be inadequacies among the checks or controls over the initial development and testing of the end user systems; ongoing maintenance and updating to keep both the application and the underlying data current; and ongoing accuracy if data are shared among end users without being filtered through MIS.

The auditor is in an excellent position to help an entity identify risks and develop strategies for addressing them as part of the overall plan.

Chapter 4

Database Management Systems

The significant impact of database management systems (DBMSs) on business today presents the auditor with a special challenge. Auditors often encounter computer-based accounting applications that use DBMSs to process transactions and maintain files, especially in the microcomputer area. The auditor must understand the nature of the activities sufficiently to make appropriate risk assessments and plan appropriate audit procedures. For all DBMSs that have direct or significant audit implications, the auditor should understand how these DBMSs were developed and how they function so that the auditor is able to execute an effective and efficient audit. This chapter explores the characteristics of DBMSs that may affect the audit.

DEFINITION AND DESCRIPTION OF THE TECHNOLOGY

Definition

Each database is a collection of interrelated files stored on-line. Theoretically, a database could contain all of the information that would ever be required by the client in one file. However, the auditor will frequently encounter separate databases for each application (for example, one for the revenue cycle, another for the purchase cycle).

In the nondatabase environment (frequently referred to as a flat file system), each application tends to have its own files, while in database environments many applications share the same file(s). To define it more technically, a database system stores a collection of structured and interrelated data that are used by one or more applications. The DBMS provides a facility for simplifying and regulating the access of multiple users and computer systems to common data and for centrally maintaining information regarding the definition, structure, and relationships of data. DBMSs use specialized software developed by commercial vendors, rather than by the client's personnel. The data used are defined by the DBMS rather than by the application programs which use the stored data. This makes the data independent from application programs.

Although there are many microcomputer-based database packages, few are true DBMSs. Many of the microcomputer-based database packages contain

features commonly found in minicomputer and mainframe systems, for example, the relational database commands project, select, and join. These packages lack one of the basic requisites: they do not serve as the data interface between the application programs and the operating system. Instead, they are programming languages that handle the data directly. Many are, in fact, higher level programming languages that contain structured table-oriented data. The audit considerations, however, remain the same. For more information on microcomputer-based databases, refer to chapter 1, "Microcomputers."

Database Structures

Databases are basically structured in one of three ways: *hierarchical, networked,* and *relational.* The hierarchical and networked databases have the logical structure of an organization chart. In a hierarchical structure, the only way to get from the top to the bottom, or vice versa, is to go through all of the intervening levels. Networked databases can jump over this organizational structure. Relational databases have the *logical structure* of a spreadsheet (meaning that they have rows and columns; each row represents a record, which is an accumulation of all of the fields related to the same identifier or key; each column represents a field common to all of the records). See appendix B, "A Primer on Database Structures," for further description of these three database structures.

The term *logical* describes the way the data are viewed by the user. The *physical structure* determines how the data are actually stored on the computer files. The actual (physical) structure of a database is dependent upon hardware and software design factors. The DBMS provides the linkage between the logical and physical structure.

Management's decision as to which one of the three logical structures to select is usually based on a trade-off between the desire to maximize throughput (meaning, how fast they want the transactions processed) and the need to provide users with the ability to query the database for matters such as "what if?" scenarios. Briefly, hierarchical and networked databases provide the fastest processing of data; relational databases provide the most flexibility in data extraction and "what if" scenarios because of their extensive cross-referencing capabilities. Currently, most system developers are designing relational databases.

Database management systems typically consist of three major components:

- Data definition language (DDL)
- Data manipulation language (DML)
- Data control language (DCL)

Additionally, they may contain a *data dictionary* and a *query language.*

The DDL is used to define the logical structure of the entire database (schema) and its contents. The *schema* specifies the name and other characteristics (for example, character type, length of each field) of the *data elements* and their relationships. Subschemas define the specific logical views of the

data required by an application program and control what the application program can access and how.

The DML is used by the application programs to store, modify (meaning add, modify, or delete data or relationships) or retrieve data from the database.

The DCL provides facilities for maintaining the integrity of the database. These include such features as *recovery/restart routines,* generalized edit and validation procedures, and security and control features.

DBMSs typically use a data dictionary to keep track of the structure of data within a database and to establish standardized documentation and definitions of the database environment. Technically, data dictionaries are not part of databases, but are supplemental. Some DBMSs make use of the data dictionary to define the data and establish editing rules.

Most DBMSs include a query language that gives the user the ability to interrogate the database without the assistance of a programmer. For example, an auditor could determine the total of all customer accounts that have negative balances with the query "summarize all customer accounts with a negative balance." Currently, the most popular type of query language is Query by Example (QBE).

Databases provide different degrees of *data independence.* The degree of data independence helps determine the ease with which personnel can accomplish changes to application programs or to the database (for example, changing the zip code from five to ten digits). Complete data independence is achieved only when data in the database can be changed without affecting the application programs and vice versa.

The DBMS may either be separate software, an integral part of the operating system, or hardware. Mainframes typically use separate software which functions under the operating system. Minicomputers frequently have their DBMS integrated into their operating system. The use of separate *back-end processors* is still relatively rare and usually encountered only in mainframe environments.

Microcomputer-based DBMSs frequently provide a lower level programming language capability (meaning, the ability to write application programs using the database programming language rather than a standardized language such as COBOL). Mainframe systems generally do not have this capability; rather, they require the use of separate programming languages (for example, COBOL) for development of the application programs that are needed to process the DBMS data.

EFFECT ON THE BUSINESS

Management tends to favor DBMSs because it is commonly perceived that they—

- Reduce the *data redundancy* present in application-based systems.
- Improve control over the data.
- Enhance data integrity.
- Make the data portable from computer to computer.

- Provide a basis for obtaining information that spans organizational functions and departments (for example, insurance underwriters can access premium information by line-of-business, actuaries can look at the same data by loss reserves, insurance agents can look at premiums by amount and type of coverage).
- Make the data independent of the application programs, thereby reducing maintenance problems.

Data redundancy occurs when the same data exist in more than one file. For example, payroll data, such as the employee numbers and pay rates, may exist in the human resource, payroll, inventory production, and cost accounting files. The cost of maintaining and updating the duplicate data, and keeping all files synchronized (for example, making certain that the employees' pay rates are the same in all files), is far greater than if the data only had to be kept in a single database accessible to these systems.

DBMSs have been favored by MIS departments because they provide a basis for a strong centralized control over data processing. Data used by several applications require only one data validation procedure and, as a result, the ability to control data appears to be greatly improved. On the other hand, database systems may result in a weakening of control over the data since many users accessing the same data may have the ability to change it. This scenario also affects *data integrity* (meaning that data integrity problems occur when validated data subsequently become corrupted).

In theory, database structures are independent of the computer disk files in which they are stored. This feature attracted many early users of databases. In practice, databases tend to be very dependent upon the physical hardware in which they reside, and, as a result, they may not be transportable from the computer hardware of one vendor to that of another.

The Database Administrator

The implementation of a large mainframe or minicomputer database system is often so complex that many organizations assign the task to a specialist who is known as the database administrator (DBA). Most clients do not have DBAs, but for those who do, the DBA's functions typically include—

- Implementing the database; defining the rules by which data are accessed and stored; and incorporating the security, integrity, performance, and data requirements of the various users to ensure that all requirements are met on a timely basis.
- Developing, implementing, and enforcing the rules for data integrity, completeness, and access, including the following.
  - — Determine who may access data and how the access is accomplished; in some organizations, this is carried out by a separate security administrator.
  - — Prevent the inclusion of incomplete, inaccurate, or invalid data.
  - — Detect the absence of required data.
  - — Prevent unauthorized access and destruction.
  - — Develop and implement contingency plans in the event of a loss.

- Documenting computer procedures (for example, reorganization of the database, use of the system and restart/recovery) and seeing that they are followed in the operation of the database.
- Coordinating with the vendor of the DBMS, assessing new releases of the DBMS and their relative impact on the entity, and ensuring that appropriate training is provided.

Application Development

The primary function of the DBMS is to handle all aspects of data definition and to provide data stored on the physical storage devices to the application programs, thereby relieving the application programs of this task. The application programs are left with the task of logically manipulating the data once they have been provided by the DBMS.

Almost all DBMSs provide the users with an inquiry capability (meaning a query language, usually QBE), which is independent of the application programs developed for the database. A number of DBMSs include programming capabilities for the end users. See chapter 3, "End User Computing."

Factors Affecting the Acquisition of Database Management Systems

Database packages for microcomputer environments may cost only a few hundred dollars and often do not require the development of application programs or the services of a DBA. On the other hand, mainframe DBMSs may cost hundreds of thousands of dollars and many times that amount to install and implement.

Although the perceived cost savings may appear substantial to a potential user, the savings need to be evaluated against the additional cost for the DBMS software and specialized personnel such as the DBA. Clearly, thoughtful and careful planning is essential.

EFFECT ON THE AUDIT

Assessing Inherent Risk

This section discusses those inherent risk factors that may be relevant to the client's use of databases. In making an assessment of inherent risk as it relates to the financial statement assertions, the auditor would also consider other factors. See Statement on Auditing Standards (SAS) No. 47, *Audit Risk and Materiality in Conducting an Audit* (AICPA, *Professional Standards,* vol. 1, AU section 312).

The auditor may wish to consider the impact of the DBMS on inherent risk as it relates to a financial statement assertion. The use of a DBMS may suggest lower inherent risk factors such as the elimination of redundant or inconsistent data. A DBMS can also result in higher risk if it has been inadequately designed and/or poorly implemented. Characteristics of design and implementation that indicate higher risk include the following:

- Design of the database without standard policies
- Complexity of testing of the application programs that interface with the DBMS (meaning that, not only must the application programs be tested, but their impact on the DBMS must be evaluated)
- Lack of an independent DBA
- Concentration of data in a single file rather than being duplicated in several files (for example, duplicate employee data in the payroll and employee master files)
- Logical access weaknesses resulting from the ability of disparate users to access the same data

Although inherent risk is typically assessed at the assertion level, the pervasiveness of a DBMS may require it to be evaluated at an entity-wide level. The impact of a faulty DBMS could materially affect the cost of performing the audit even if no reduction in the assessed level of control risk is contemplated.

Understanding the Internal Control Structure

The auditor might consider using a *data element matrix* in addition to the usual documentation (for example, flowcharts and checklists). The primary use of a data matrix is to develop computer assisted audit techniques (CAATs). Still, the matrix also contains each *audit significant field* (data element) and the applications in which it is used, which is useful because the auditor needs to know which of the data elements are associated with the financial statement line items.

The data element matrix should indicate how the item is used (meaning, entered, modified, inquiry only, or deleted). Note that data elements may be generated by the DBMS rather than by programmed procedures in the application programs. For example, the accounts payable record may be generated by the DBMS as a result of pulling various data elements together (for example, the purchase order, receiving documents, and vendor invoice). Therefore, to obtain an understanding of the internal control structure sufficient to plan the audit, it may also be necessary to have a general understanding of the following:

- Data dictionary
- Logical and physical structures
- System-generated data

The auditor should also consider including a description of the access controls over the database. Because of the number of potential users for each field, access controls are important.

To gain an adequate understanding of the internal control structure of database systems, auditors may wish to consider using the services of electronic data processing (EDP) audit specialists or other persons who are familiar with such systems.

Assessing Control Risk

Control Policies and Procedures

Use of a DBMS permits significant integration of programmed controls into the automated environment. The client's use of database systems may have a number of effects.

Segregation of functions. Database system access control features can be used to restrict the functions and data available to specific database users. Since a database system simplifies user access to data, it may also provide an environment that permits unauthorized access to the database in the absence of appropriate access controls. A separate DBA function can assist in preventing or detecting misstatements by independently applying control procedures over data access. This function would generally not be found in smaller entities.

Potential for increased management supervision. Database systems maintain the consistency of data usage by avoiding the storage of redundant data elements. This feature can be an important tool for management to ensure that transactions are consistently executed and recorded. However, most microcomputers contain programs (for example, editors such as EDLIN) which can easily access and modify microcomputer-based database files.

Initiation of transactions by computer. Database systems may contain functions relating to storing, editing, retrieving, and processing that are similar to functions contained in computer programs. As a result, the DBMS, rather than an application program, may be used to initiate new transactions.

Potential for errors and irregularities. A DBMS provides a common repository for computer readable data and, therefore, restricts the potential for human observation of the results of processing activities. Errors or irregularities in a database system may affect all like transactions uniformly but may remain undetected for long periods of time. Therefore, effective control may require the use of computer-based procedures to evaluate the results of processing activity and to detect potential misstatements in the database.

Transaction trails. Database system transaction trails often contain complex cross-references and data storage formats, requiring both specialized technical expertise and the software to use them. Tracing of transactions may also require the reconstruction of the database contents and changes to the database contents during the period covered by the audit. For example, an accounts payable open-item record may not exist as a single record, but be made up of fields located in the purchase order, receiving, inventory, and vendor records. It may be necessary to use specialized auditing or 4GL languages to rebuild the transaction trails.

Uniform processing of transactions. Information describing the relationships of data elements can be changed by use of the DDL with effects similar

to changing programs in batch and on-line computer systems. Therefore, auditors may wish to consider controls over changes to the database by use of the DDL. See chapter 3, "End User Computing."

Tests of Controls

Tests of controls can often be performed simultaneously with gaining an understanding of the internal control structure. This is usually the most efficient approach and involves a combination of inquiry, observation, reperformance, and inspection of documentary evidence. Specific procedures may include extended walk-throughs of applications, parallel simulation, or processing of test data. Inquiry alone is typically not sufficient evidence to reduce control risk below maximum.

The hardware (for example, mainframe versus microcomputer) may influence how far the auditor should go to gain the necessary understanding. For example, in a microcomputer environment, the auditor probably need not consider the impact of the DBMS. In a minicomputer or mainframe environment, however, DBMS can impact the effectiveness of many application controls, and the auditor may wish to obtain a more detailed understanding of the internal control structure.

Designing Substantive Audit Procedures

The nature, timing, and extent of substantive audit procedures that should be applied to significant financial statement assertions depends on the inherent and control risk assessments for those assertions. For assertions affected by database activities, the use of CAATs may be required in order to obtain audit evidence by substantive procedures. The auditor may obtain sufficient evidential matter without directly testing the database applications. That is, the auditor may obtain the evidence from other sources. For example, although the maintenance of inventory purchase records in a database may provide data used for testing the accuracy and ownership of the inventory, evidential matter will likely come from observation, vouching, and confirmation.

The auditor may also use a combination of the following:

- Recreation of the results with software written by the auditor (for example, the aging of the accounts receivable open items)
- Detailed testing of the results using a sampling plan
- High assurance substantive analysis techniques using independent data

For example, if the allowance for uncollectible accounts receivable accounts is determined based on results of database activities, the auditor might consider a combination of the assumptions used and reperform the computations. These procedures usually obviate the need to consider a review of the program code that created the results. In rare circumstances, it might also be necessary to review the program code to determine the proper aging of accounts.

The complexities of the database structure may make it inefficient to do a totally substantive audit. Under this circumstance, the auditor should

consider performing tests of the programmed control procedures in order to improve audit efficiency. In addition, extensive testing of the general computer control procedures may be appropriate.

AUDITOR'S RECOMMENDATIONS TO CLIENTS

The auditor reviewing DBMS may wish to consider the entity's planning, organization, and policies and procedures to determine how well this resource is managed.

Management should have and review, at least annually, a comprehensive management information system (MIS) plan that addresses all hardware platforms—including mainframes, minicomputers, microcomputers, and other office systems. One of the most critical elements for success is the organization's continued commitment to supporting the DBMS. This will provide for the proper maintenance of standards in hardware, software, and operating systems. Disaster recovery is especially critical because so much is tied up in database environments. The recovery process for DBMS may result in undetected misstatements since data recovered from backup files are rarely subjected to the same editing controls originally used to validate the data. The process has to be carefully planned and implemented and frequently tested to insure the integrity of the restored database.

The auditor is in an excellent position to help an entity identify risks and develop strategies for addressing them as part of the overall plan. All risks are not critical and should not be treated as such. As in any other system, there is a need for a reasonable—not absolute—level of control.

Chapter 5

Telecommunications

Telecommunications has become a pervasive part of business for organizations large and small. In many situations, it is an integral part of vital business activities such as order entry and acknowledgment, inventory releases and shipping notices, and invoicing and payment. It is often a factor in strategic and competitive systems. This chapter provides a discussion of various aspects of telecommunications, summarizes issues related to its effect on the business, and describes how a client's use of telecommunications might affect the auditor's assessment of inherent risk and control risk, and the design of substantive audit procedures.

DEFINITION AND DESCRIPTION OF TECHNOLOGY

The auditor is likely to encounter financially related uses of telecommunications by clients—if not today, then very soon. Although the use of telecommunications, in and of itself, is not likely to change the basic nature of substantive audit procedures to be followed, this technology may well affect the auditor's assessments of inherent and control risk. The auditor may need to consider the specific nature of the telecommunications application and the information involved, along with all other relevant factors, in arriving at these assessments.

Definition

Telecommunications is the electronic transmission of information by radio, wire, fiber optics, microwave, laser, or any other electromagnetic system. The information transmitted may be voice, data, video, facsimile, or other media. A telecommunications system comprises physical hardware and software. The hardware may include computers for communications control and switching; modems to provide compatibility of format, speed, and other factors; and transmission facilities and media such as copper wire, fiber optic cables, microwave stations, and communications satellites. The software controls and monitors the functions of the hardware, formats information, and adds appropriate control information, performs

switching operations, provides security, and supports the management of communications.

Scope of This Chapter

The focus of this chapter is data communications, which are most likely to transmit information that may have an effect on the financial statement audit. Thus, voice and other forms of communications will be referred to only as necessary in examples that involve audits. Appendixes C and D offer some additional discussion and definitions of common terms relating to communications hardware and software. This chapter will not attempt to address local area networks (LANs). For a discussion of LANs, see chapter 2, "Local Area Networks."

EFFECT ON THE BUSINESS

Telecommunications is not an end in itself; it is an enabling technology. Telecommunications enables organizations to implement applications and achieve benefits that would not otherwise be possible. Although telecommunications is not an inexpensive technology to implement, the combination of new technical breakthroughs and creative business services makes it available to small and large organizations. The auditor may find it useful to be aware of the variety of roles that telecommunications may play in business, and some of the more important issues that influence the use of this technology.

Telecommunications Applications

Telecommunications offers significant opportunities for new business applications. An entity can enhance its relationships with its customers, suppliers, bankers, agents, and strategic partners. It can achieve better coordination of geographically dispersed operations. It can gain the benefits of telecommunications services offered by communications vendors (value-added networks, or VANs) without the substantial front-end investment that would otherwise be needed. Examples of high-impact business applications follow.

Electronic Data Interchange

Telecommunications can be used to accelerate the exchange of business transactions between organizations through electronic data interchange (EDI), with benefits in the elimination of document handling and postage costs and the ability to reduce inventory levels and accelerate cash flow cycles. Databases shared among EDI trading partners, which are important to advanced users of EDI, would be impossible without telecommunications. The use of EDI is likely to have a profound effect on the entity and its auditors.

Electronic Funds Transfer

This application was developed and widely used in the banking industry. Other entities may use electronic funds transfer (EFT) for cash management

and employee payrolls. EDI applications often include the use of EFT for vendor payments. There is a clear trend toward replacing paper checks with EFT transactions.

Point of Sale Systems

Used extensively in the retail industry, point of sale (POS) systems link sales registers with store-based minicomputers that are, in turn, linked to central, entity-wide computers. The store-based computers provide the registers with current prices (eliminating the costs of labeling individual items and reducing clerical errors in sales transactions) and collect sales details from the registers. Details are then relayed to the central computers in the form of stock movement statistics and restock orders. Typically, POS systems are a major source of operational and financial data.

Commercial On-Line Databases

These databases offer current information in computer format to subscribers, accessible via telecommunications. The range of financial news and information available is wide—from published corporate financial statements through credit ratings to stock, bond, and commodity market data. Users, aided by extensive indexing and sophisticated search techniques, gain access on demand to meet information needs that would otherwise require long-time delays or prohibitive costs.

Airline Reservation Systems

Current databases of seat availability (meaning, inventory) are maintained for thousands of domestic and international flights. Telecommunications enables ticket agents around the world to confirm availability, reserve a seat, and issue a ticket in seconds. As reservations systems grow, consumers will be able to place reservations with the airlines' strategic partners in the hotel and car rental businesses.

Current Developments in Telecommunications

The current growth of telecommunications seems to have begun in the 1980s. In the United States, deregulation forced AT&T to divide into regional operating companies and opened the door to competition and innovative new services. In many other countries, government-run post, telephone, and telegraph agencies are providing new products and services that have made international communications more accessible. The open systems interconnection standards (OSI), an international standard for communication, has gained wide acceptance and will make international information exchange easier as these standards are established in the United States. The rapid maturation of telecommunications technology has created the ability to transmit ever-larger volumes of information over longer distances. The feasibility of services such as video conferencing, high-resolution facsimile, and high-volume data uploads and downloads for database backup and recovery are the result of new technologies that include the following.

Digital Transmission Services

Traditional, voice-oriented analog facilities are being replaced by digital services. Digital services provide much higher transmission speeds with lower error rates; are able to mix data, voice, and images on the same circuit; and can build more intelligence into a network.

Fiber Optic Cable

In a number of situations, copper cable is being replaced by fiber optic cable, which carries data by light waves rather than electricity. Fiber optics are less bulky than copper cable, and provide a capacity that is several orders of magnitude greater. In addition, fiber optics are free of the problems caused by noise and electromagnetic interface and less susceptible to wiretapping.

Communications Satellites

Satellites provide very high-volume transmission worldwide, without the limitations of surface lines. By comparison, lines with limited capacity and outdated facilities create excessive transmission interference (noise). The delay inherent in sending signals 20,000 miles into space and back again to earth makes satellite communications unsatisfactory for many interactive uses. Nevertheless, for a number of applications, this is very attractive technology.

Very Small Aperture Terminal Services

Satellites initially had another limitation, because the ground-based transmission and receiving facilities (dishes) were large and expensive, and thus located only in high-use areas, near large cities. Very small aperture terminal (VSAT) services now enable organizations to install small dishes in any location, providing economical access to satellite communications.

Cost and Complexity of Telecommunications

Through the public telephone network, even the smallest businesses have access to affordable telecommunications equipment and long-distance services. Nevertheless, at higher levels of usage, for example, for very high volumes of data, telecommunications can become expensive.

In order to avoid unanticipated expenses, the development of an application that entails extensive telecommunications must include a plan to adequately fill the entity's communications needs, an examination of the alternatives, and a cost/benefit analysis. This precaution is advisable whether the entity uses purchased public network services or entity-owned facilities. A number of carriers may have different tariffs (price schedules) for the same basic service, according to whether the use is for voice or data. The simple act of plugging a microcomputer modem into a telephone jack can, at least in principle, incur a different tariff than for voice service, and thus increase the cost of the line. As needs grow, some level of ongoing telecommunications network management and technical support may be needed to control costs, monitor the use of services, and maintain network availability. Even if the entity relies on a service provider for all telecommunications services and support, it is prudent to provide competent oversight for this arrangement.

Backup Considerations

Entities are becoming more aware of the importance of backing up their computer systems. Still, there is generally less awareness of the importance of telecommunications contingency planning for vital business activities, and there are fewer alternatives available to entities that have recognized their exposure. Generally, redundant facilities are prohibitively expensive. The entity needs to assess its risks and select appropriate alternatives for each major component of its networks. The components to be considered include the equipment used at various locations and each segment of the communications path between locations.

Accessibility of Information and Systems

Telecommunications increase the accessibility of information systems for both authorized and, unfortunately, unauthorized users. If employees, customers, or others can remotely access their systems through public networks, hackers may be able to enter the same way. A novice hacker may cause system crashes, erase data and program files, or overload processing resources, slowing system productivity. A malicious hacker may introduce a computer virus that could repeatedly cause any of these problems. A sophisticated hacker can copy proprietary software and information, fraudulently change data files, or make personal use of an entity's computer and communications systems. (There are growing numbers of reports of entities that incur thousands of dollars in telephone costs because hackers have gained access to their Private Branch Exchange and placed expensive calls.) The entity will need to implement and maintain security measures that provide appropriate protection against such threats and the ability to recover if they materialize.

If the entity transmits sensitive data (for example, confidential or proprietary information) to remote locations, it may also be vulnerable to wiretapping or other forms of eavesdropping. Such situations should be assessed to determine the need for other security measures, such as increased physical security over the lines entering the remote location or encryption of data transmissions.

EFFECT ON THE AUDIT

The potential audit implications of telecommunications will depend on the significance of telecommunications-based application systems to the client's financial statements. For those systems that the auditor considers significant, the topics addressed in the following sections may be considered.

Assessing Inherent Risk

This section discusses the possible relevance of inherent risk factors to the client's use of telecommunications. In assessing inherent risk as it relates to the financial statement assertions, the auditor would also consider other factors. See Statement on Auditing Standards (SAS) No. 47, *Audit Risk and Materiality in Conducting an Audit* (AICPA, *Professional Standards,* vol. 1, AU Section 312).

Telecommunications is a necessary component of distributed systems, in which portions of systems and data reside at remote locations. The scenarios included in appendix C provide examples of distributed systems. Systems that involve the distribution of functionality to remote locations are likely to introduce processing complexities beyond those found in wholly centralized systems and that may cause the auditor to assess inherent risk at a higher level.

The distribution of systems and data to remote locations leaves them unprotected by whatever physical and logical security is provided for the central computer. At remote locations, unauthorized and undetected changes may be made to programs or to data. Under these circumstances, even well-intended changes can threaten the integrity of systems and data if there is a lack of testing disciplines, quality assurance, and appropriate levels of management oversight.

In addition, it is possible that mandated changes to hardware or software may be implemented properly in some locations but be delayed or incorrectly implemented in others. The integrity of the system and the data processed may be affected, and thus the level at which the auditor assesses inherent risk increases.

Telecommunications often requires linking hardware and software components from assorted vendors. A number of these components may be relatively new and their ability to work together may be unproven. Subtle differences in the protocols and capabilities implemented by different vendors may result in sporadic errors (perhaps even the loss of transactions) that may be difficult to detect. It is often difficult to determine and correct such errors. As a result, data integrity may be a serious problem.

In a number of situations, telecommunications may add a processing step that allows personnel to modify transactions or introduce fraudulent transactions, as has occurred in the wire transfer rooms of a number of banks. (A wire transfer room is a telecommunications facility used to send and receive monetary transactions with other banks and a number of bank customers.) A client's use of electronic funds transfers may be a consideration in the auditor's assessment of inherent risk.

Telecommunications provides the entryway for hackers. Most of the risks created by hackers may be business risks. Nevertheless, the auditor may want to consider the kind of financial information involved and the client's past experience with hackers in deciding whether to include this as a factor material to overall inherent risk.

Although most transmission facilities used in applications today are likely to include built-in controls to ensure that transactions are not lost or distorted in transmission, errors can occur. This risk increases with the use of homegrown or new and unproven hardware or software in telecommunications.

Regardless of the facilities used, disruptions or failures in communication can and do occur. One result may be that the network is unable to recover transactions lost in transit. Procedures are needed to ensure that lost transactions can be identified and retransmitted after communications are restored. The auditor may want to consider the potential for loss of transactions in his or her assessment of inherent risk.

The use of telecommunications may also reduce some aspects of inherent risk. For example, remote entry of data may reduce the number of data entry errors and the potential loss of paper documents in transit between initiating locations and the central data entry function.

Understanding the Internal Control Structure

In the process of gaining an understanding of a client's internal control structure, the auditor would ordinarily become aware of telecommunications use that has financial and audit significance. Discussions with appropriate personnel or other means may disclose to the auditor the information appropriate to his or her needs. Examples of useful documentation might include listings of remote communications locations; summary network diagrams, annotated to show the nature, volume, and value of financial transactions that are transmitted; and descriptions of the processing performed at each remote location that relate to material financial statement accounts. Based on this information, the auditor ordinarily would assess whether each situation is significant to the audit. This assessment may affect the audit plan.

If the auditor determines that telecommunications has little or no audit significance, no further work is required in this area.

Assessing Control Risk

Internal controls over telecommunications may be pervasive (for example, network management; see appendix A "Local Area Network Technology and Terms") or specific. The auditor must determine which controls are relevant to the assessment of control risk for those systems in light of their impact on the financial statements and the auditor's assessment of inherent risk. The auditor may wish to consider the adequacy of the following controls.

System Integrity at Remote Sites

What controls exist to protect programs and data at remote sites from unauthorized modification or misuse? Such controls might include restrictions over physical access to terminals and the computer and communication systems, the use of individual user IDs and confidential passwords, and protected program libraries.

Data Entry and Update

Are controls such as batching, logging, and supervisory review in place to ensure that data are entered accurately and completely, and that only authorized updates are posted to databases or master files? Are input data at remote locations logged and retained until the receiving site confirms that they have been accurately received?

Application

Application controls include input validation, independent reconciliation, and check digits on selected important data fields. Are programmed and

manual controls over application transactions and databases sufficient to detect inaccurate, invalid, or fraudulent data received from remote locations via telecommunications?

Central Computer Security

Does the client make effective use of access control software (for example, RACF) or access control facilities of the operating system, as appropriate? This software should support user authentication, definition of authorization for individual users by resource and type of access (for example, read, write, execute), and reporting of unauthorized access attempts, which can then be monitored and resolved in a regular and timely fashion. The auditor should consider the complexity of the communications environment when testing access controls. If users not uniquely known to the system can enter through outside networks, the difficulty of providing appropriate security is increased.

Dial-in Security

Does the client protect dial-in access through a dial-back system or equivalent means (for example, operator intervention)? Are access privileges and telephone numbers added, maintained, and deleted on a current basis? Systems that allow users to dial-in over the telephone network are vulnerable to outsiders, including hackers, who may be able to discover the telephone number and thus attempt to gain unauthorized access to the system. For systems with low levels of activity, protection may be provided by having an operator or attendant answer all calls and establish the caller's identification. Identification could be established through an exchange of code words or a similar procedure (or, less effectively, through simple personal recognition). The operator can then connect the user to the computer system or, preferably, call the user back at a predesignated telephone number.

For high-use systems in which such manual intervention is not practical, specialized communications computers (dial-back devices) are available that—

- Answer incoming calls to the system.
- Request the entry of a user identifier (which can be entered by the caller's computer or terminal, or with a touch-tone telephone).
- Terminate the connection (meaning that it "hangs up" the call).
- Authenticate the user via a programmed database of authorized users.
- Return the call (using the telephone number precoded in the database).

The user is then connected to the system.

Transmission Accuracy and Completeness

Hardware, software, and services components of the telecommunications system typically include line quality control and error detection and correction features. The auditor might inquire as to the effectiveness of these control features, particularly if the client's telecommunications facilities include components that are unproven products. Regardless of the quality of the telecommunications facilities, a number of failures are almost inevitable.

If transactions are being transmitted when a failure occurs, they may be lost. Manual or programmed control procedures should be in place for such occurrences. Do procedures allow for the identification and resubmission of transactions lost in the event of a line failure or other disruption?

Physical Security Over Telecommunications Facilities

Is access to the computer facility appropriately restricted? Are communications wiring cabinets located in secure areas or locked to prevent physical access to communications lines? Security issues may not be of great concern to the auditor. He or she may, however, perceive that transactions transmitted by telecommunications are susceptible to manipulation that could, for example, lead to the misappropriation of assets.

Tests of Controls

If the auditor determines that tests of controls over telecommunications are needed to support the audit plan, the following tests may be considered.

Access to Programs and Data Stored at Remote Sites

Review the policies and procedures that are in operation at remote sites relating to access to programs and data stored at these sites. Determine that access is limited to an appropriate number of authorized individuals. Determine, through discussion with client personnel and review of appropriate documentation, that there is adherence to these policies and procedures.

General Security at Remote Sites

Review the policies and procedures in place at remote sites relating to general security over computer facilities, including, for example, prohibition of the use of software downloaded from electronic bulletin boards or obtained from other uncontrolled sources. Determine, through discussion with client personnel and review of appropriate documentation, that there is adherence to these policies and procedures.

Data Entry at Remote Sites

Review procedures and controls relating to data entry at remote sites. Assess whether these procedures and controls provide reasonable assurance that all transactions are entered properly at these sites. Determine, through discussion with client personnel and review of appropriate documentation, that there is adherence to these procedures and controls.

Data Received

Review application controls over data received via telecommunications. Assess whether these controls provide reasonable assurance that all data entered locally and at remote sites is properly received and entered into processing. Determine, through discussion, observation, or other tests, that these controls are operating effectively.

Access to the Central Computer and Dial-In Lines

Review policies and procedures related to access control in the central computer and dial-in lines. In particular, determine whether authorized users are added, maintained, and deleted on a timely basis; the system requires passwords to be changed on a regular basis; access authorization is defined at a meaningful level of detail; and unauthorized access attempts and other exception conditions are recorded, investigated, and resolved on a timely basis. For sensitive transactions, the auditor may want to give in-depth attention to the specific authorization rules defined within the system, and consider whether these provide an adequate level of segregation of duties.

Transmission

Review evidence of hardware and software transmission controls. Such evidence may include vendor specification sheets and documentation that such controls were considered by competent personnel when these systems were acquired.

System Logs

Determine whether system logs (system-generated records of the date, time, and nature of key activities such as message receipt or transmission) are captured and archived long enough to provide an audit trail for resolving problems.

Problem Logs

Determine whether persons responsible for the telecommunications systems maintain a problem log to document network failures, equipment malfunctions, and other problems. Determine whether these logs are used to monitor and investigate problems, address recurring problems, and initiate corrective action.

Designing Substantive Audit Procedures

The auditor's assessment of control risk related to the telecommunications aspects of financially significant systems may affect the nature, extent, and timing of substantive audit procedures. At the same time, however, it is unlikely that telecommunications alone will substantially change the audit procedures while the basic information and documents that are needed remain available.

The auditor should use his or her knowledge of the client's telecommunications to evaluate the risk of material misstatements in the financial statements. The auditor should consider the kinds of potential misstatements that might be attributable to telecommunications usage, as well as design appropriate substantive tests.

For example, the auditor may determine that the quality of the client's communications facilities is questionable, and that, therefore, the inherent risk of losing transactions (due to line failures, etc.) is high. The auditor may also conclude that the controls in place to detect losses are inadequate, and may thus assess that the control risk is also high.

In such a case, the substantive procedures designed by the auditor would include examining the risks in terms of the completeness and accuracy of the account or accounts that would be affected. Such procedures would be tailored to and appropriate for the accounts and the risks; they would neither focus on nor directly involve the telecommunications system itself.

AUDITOR'S RECOMMENDATIONS TO CLIENTS

If the client has not coordinated the purchase and use of telecommunications systems and services, the auditor can suggest that a coordinator with an adequate level of authority be identified. For a larger entity with extensive communication requirements, it may be advantageous to consider developing an entity-wide plan for the integration of voice and data telecommunications.

As the client's use of telecommunications grows, so does the importance of a full-function network management capability which is fully described in appendix A, "Local Area Networks Technology and Terms," in the section, "Network Management." This capability would ordinarily include the following:

- Fault management
- Configuration management
- Performance monitoring
- Security management
- Accounting management

The auditor could suggest that the client consider appointing an individual or group to provide this capability.

If the client has not formally considered the critical nature of telecommunications-supported systems and activities, the auditor could suggest that the client conduct an impact analysis of the potential loss of services for extended periods and develop backup strategies as needed.

If the client has not implemented effective mainframe and dial-in security, the auditor can suggest appropriate measures. If microcomputers are connected to the mainframe (or minicomputer), the auditor can suggest a survey to determine the number of microcomputers equipped with modems that are left in an automatic answering mode during nonworking hours. Often, management is unaware of this practice, making it an unrecognized vulnerability. See also related guidance on local area networks in chapter 1, "Microcomputers."

Transmissions of proprietary or sensitive information may be vulnerable to wiretaps or some other form of electronic eavesdropping, a possibility that is growing with the increasing use of land-based and satellite microwave communications. If the auditor perceives this to be an important consideration, he or she can suggest data encryption for at least selected portions of the transmissions. Data encryption encodes the data transmission for anyone except the intended receiver. This process can also make it difficult to alter the data or insert fraudulent transactions during transmission. It can even protect against the disclosure or unauthorized modification of data

stored on computer disks or tapes. Hardware devices or software packages are commercially available to provide encryption. The cost of encryption and the value of the information are both major factors in determining whether encryption is appropriate.

Data transmissions may be subject to laws that restrict or regulate the flow of information. A number of nations, particularly in Europe, impose trans-border data flow regulations or international information flow regulations. The auditor can suggest an assessment of the impact of these laws for clients who transmit information internationally.

The data privacy and protection laws in effect in a number of countries are a related issue, though not necessarily involving telecommunications. These laws regulate the collection, storage, and use of information inside a country's borders. Clients who have operations in other countries may be advised by the auditor to assess the impact of these regulations on information maintained in foreign locations.

Appendix A

Local Area Network Technology and Terms

SERVERS

Servers can be configured as either dedicated or nondedicated. A dedicated server is only used to serve the network and does not have any other functions. A nondedicated server can also be used as a workstation.

Common server functions include network, file, print, and communications services. Depending on the network configuration, server functions may be run on one or more computers or other hardware devices.

Network Server

The network server manages access to the network and serves the needs of the network. The configuration differs according to the topology selected. In a ring topology network, control may be distributed and each workstation on the network is responsible for forwarding messages not addressed to it, based on logic built into the network interface cards. The other topologies make use of a centralized network server to control and route the network traffic.

File Server

The primary function of the file server is to provide shared storage space for files and give multiple users access to the files. The server controls concurrent access to files, enforces access rights and restrictions, and provides directory structures that recognize file names and support the grouping of files.

Print Server

A print server permits all workstations on a LAN to share a common printer. Input/output requests from workstations are accepted by the server and redirected to a fast disk (print spool). The requests are then retrieved from the disk and printed, one at a time and, generally, in sequence.

Communications Server

A communications server manages access to the communications devices on the local area network (LAN). These servers are needed only to interconnect with remote LANs, other types of computers, or other networks. The server generally attaches to what the other communicating device views as a gateway.

HARDWARE COMPONENTS

Workstations

The term *workstation* includes previously installed PCs as well as microprocessors that have been specially configured to run on the network. The workstations can be from the same or different vendors. Each can be configured with different disk capacities, memory, and other add-ons.

Peripherals

Peripherals are input/output devices such as printers, magnetic tapes, disks, optical scanners, facsimile boards, and modems that provide or support data entry, data storage, and data output. The shared use of peripherals is a primary benefit of using a LAN. For example, all users on the network can access one laser printer if it is linked to the LAN.

Transmission Media

The physical path that connects the different components of the LAN is the transmission medium. There are two categories of LAN media: terrestrial and free space. Terrestrial media include twisted-pair wiring, coaxial cable, and fiber optic cable. Free space media, for use in highly specialized situations, include digital microwave radio and infrared light wave radio and infrared light beam transmission. Each medium has its own transmission speed, cost, number of devices that can be attached, maximum span, noise immunity, and availability. Currently, terrestrial media are most commonly used.

Network Interface Cards

The network interface card (NIC) connects the workstation and the transmission media. The NIC is installed in the computer in parallel with the processor board and disk drives. It is the connection point between the transmission media and the workstation and is recognized by the local processor as a local device.

DIFFERENTIATING LOCAL AREA NETWORKS

The four key factors that commonly differentiate one LAN from another are network topology, transmission media, service protocols, and transmission technique. Transmission media have been addressed previously, while the other three are addressed in the following.

Topologies

The topology of a LAN refers to the pattern formed by the physical links of the network. The common topologies are star, bus/tree, ring or a combination thereof.

- *Star.* In a star topology, communications processing control is performed by a central processing hub. All data pass from the sending station through a central point and on to the receiving stations.
- *Bus/Tree.* In a bus topology, links may follow a back-and-forth route. A transmission moves from one station to the next, turns around at the end of the line, and passes the same stations again in reverse order. Tree is used to describe a branched LAN whose limbs are all bus-topology networks.
- *Ring.* In a ring topology the data pass from one station to the next. Data generally move around a ring network in one direction.

Service Protocols

A service protocol is used to coordinate access to the transmission medium so that participants are not attempting to transmit simultaneously. The service protocol used is constrained by the topology and is a trade-off among competing factors such as cost, performance, and complexity.

There are two broad categories of service protocols, contention and in turn. The most commonly used contention service protocol is carrier sense multiple access/collision detection (CSMA/CD). In turn service protocols are token-passing, slotted access, and station polling.

CSMA/CD

With CSMA/CD, a station wanting to transmit first "listens" to the medium to determine whether another transmission is in progress. If the medium is idle, the station may transmit; if the medium is busy, the station will continue to listen until the channel is idle, and then transmit. If two or more stations attempt to transmit at the same time, the collision detection facility will cease transmission. Before retransmission is attempted, all prior steps of this communication technique are repeated.

Token Passing

In a token passing network a token (bit signal) is passed from node to node. A station that wants to transmit "takes" the token in its turn but does not pass the token to the next station until after its own message has been sent. The token is attached to the message, which moves from station to station. Even a long message will not be broken into shorter segments. Token passing is associated with ring and bus topology networks, which provide terminology such as "token bus" and "token ring."

Slotted Access

In a slotted-access system, data-packets (*slots*) circulate to be filled with data from transmitting stations. Each slot is preceded by a flag, which, like the

token, is changed from free to busy status by the using station. All the slots are of similar size. Messages that are too long for a slot must be broken into shorter segments or packets for transmission. Slotted access is most often used in ring topology, giving a slotted ring.

Station Polling

Station polling resembles token passing in its effect. Each station gets the opportunity to transmit, in turn, and may transmit a message of any length before relinquishing control. This opportunity is offered to each station by the host, rather than passing from station to station.

Transmission Techniques

Transmission techniques refer to the number of channels that the medium of the LAN has to transfer data. The terms used to describe the different transmission options are *baseband* and *broadband.*

Baseband

Baseband provides only a single channel for sending digital signals in a half duplex mode (send, then receive). Baseband transmission is bidirectional, that is, a signal inserted at any point on the medium propagates in both directions to the ends, where it is absorbed. Baseband systems usually require a bus topology. Baseband has the advantages of simplicity and low cost. The disadvantages include limitations in capacity and distance.

Broadband

Broadband consists of a broad bandwidth that provides many channels operating in full duplex mode (some sending and some receiving). It requires the use of a modem because it uses analog signaling. Unlike digital signaling, in which the entire frequency spectrum of the medium is used to produce the signal, analog signaling allows frequency-division multiplexing (FDM). With FDM, the frequency spectrum on the cable is divided into channels or sections of band width; separate channels can support data traffic, television, and radio signals. Broadband is a unidirectional medium; signals inserted on a medium propagate in one direction only, which means that only "downstream" stations can receive its signals.

NETWORK MANAGEMENT

Network management has become an increasingly important issue as networks become larger and more complex. In addition to technical complexity, networks of networks create administrative and organizational problems that are often unforeseen by the network software designers.

Network management covers a number of areas: fault, configuration, performance, security, and accounting management.

Fault Management

The most important function of network management is to maintain the high availability of network services and resources. For this purpose, it is necessary

to monitor the network for faults (error conditions or device failures), isolate the faults, and recover from them.

Configuration Management

The resources of the network must be initialized and the intended relationships established for proper network operation. Configuration management provides messages to describe active connections and equipment.

Performance Monitoring

To provide efficient service with acceptable response times and throughput, it is necessary to monitor the performance of the network. Performance management includes counting things like packets, disk-access requests, and the number of times specific programs are used.

Security Management

There is a need to define and regulate access to network resources via authentication, authorization, and encryption. Also, changes to files and programs need to be monitored.

Accounting Management

Costs for the LAN should be determined, and charges should be established for the use of managed objects to enable the allocation of expenses.

EXTENDED FEATURES AND OPTIONS

There are extended features and options that can be incorporated in a LAN to enhance its capabilities. The extended features and options include expanded communications and enhanced services.

Expanded Communications

There are a number of options available for connecting LANs to one another. The major categories of LAN connectivity equipment are: repeaters, routers/bridges, and gateways.

Repeaters

Repeaters pick up a signal on one LAN segment and repeat it onto another segment. Repeaters are not used to link LANs with different protocols; they simply strengthen the signal from node to node but do not interpret or translate. They extend the geographical reach of the LAN.

Routers/Bridges

Routers/bridges direct traffic from one LAN or LAN segment to another. In the absence of a protocol conversion feature, they can link only LANs or segments of a LAN utilizing the same protocol. Though there is significant inconsistency in the use of the two terms, generally routers are more complex, richer in function, and more expensive. Whether a particular device stores

configuration information or experience based on past successful transmissions must be determined from its technical documentation rather than its label as a bridge or a router.

Gateways

Gateways are the most versatile of the LAN connectivity equipment. They can connect any two systems that do not share a common routing protocol. In addition to routing, protocol conversion, and translation, they also provide application support functions to manipulate data before they are passed to the receiving network.

Enhanced Services

The enhanced services discussed here are database servers, computer-based message systems, and the client server model.

Database Servers

Database servers take a more active role in processing on a LAN than do file servers. Database servers are divided into two functions: the front-end client application seen by the user and the back-end database engine (server) that performs computation and data management.

The database server is useful to lessen network load by centralizing record manipulation at the server, and sending only the data needed for the client application. Users can obtain specific data segments from the database server through a query instead of filling microcomputer random-access memory (RAM) with large chunks of unsifted data.

Although database servers are more expensive than file servers, they can bring the capabilities of mid-range computers to a localized personal computer. They can also be either free standing or gateway access facilities for a host database.

Computer-Based Message Systems

Computer-based message systems (CBMS), which are services permitting the electronic transmission and storage of messages, are available as LAN applications. They come in different forms such as telex, facsimile, and electronic mail systems. Broadcast facilities are also available to automatically transmit to multiple recipients. The privacy and security of information associated with CBMS is at risk due to the loss of physical control.

Client Server Model

Also called distributed processing or client server architecture, the client server model is a movement of some user tasks from centralized locations to desktop machines while retaining data storage, processing, and management on a backend system or server, whether a high-end microcomputer, minicomputer, or mainframe. Basically, it is the division of applications systems into discrete programming tasks that execute in parallel on various nodes of a network. In effect, with the right kind of networking software, all of the personal computers, workstations, minicomputers, and mainframes on a local area or even a wide area network can work together in parallel to deliver performance equivalent to that of a supercomputer.

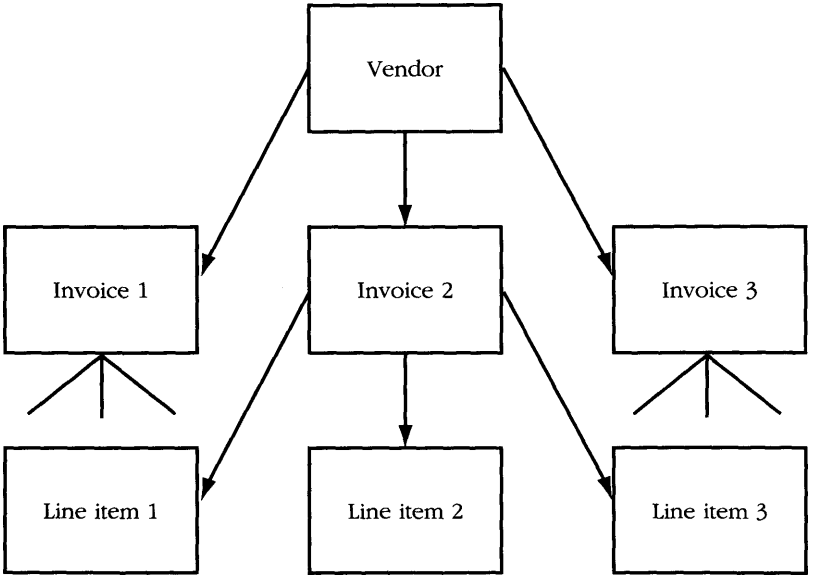
Appendix B

A Primer on Database Structures

The following is provided for those wishing to know more about the different types of logical file organizations used in database systems.

HIERARCHICAL MODELS

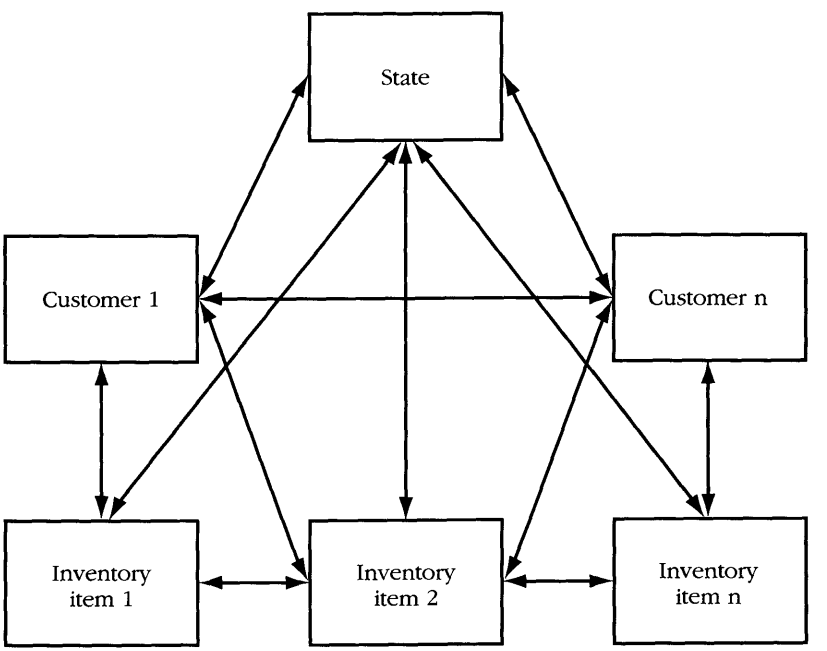
Exhibit B.1
The Hierarchical Model



The organizational chart shown in Exhibit B.1 symbolizes the logical structure of the hierarchical database. At the top of the structure is the *root node.* Extending downward out of the root node are branches. Each branch ends in a node. As a result, each node is connected by a branch to the node before it and to the node after it. In effect, there are two basic levels, the parent and the children; these relationships remain even though there can be a number of levels. The parent can communicate with its children and vice versa; however, parents cannot communicate with each other. The same is true for the children, who can communicate with each other only through its parent. This amounts to a one-to-many relationship (for example, each parent can communicate with its own children). Every vendor record has to be searched to accumulate data about a specific product.

NETWORK MODELS

Exhibit B.2
The Networked Model



Network models were developed to overcome the possible need to accumulate data by searching all records. In a networked database, such as the one shown in Exhibit B.2, any child can communicate directly with any other child or parent. This capacity is achieved through the extensive use of *pointers* (meaning, indices that disclose the item's location). The network model is a many-to-many model instead of a one-to-many relation. The parent-child relationship is also less narrowly defined. For example, a child can have more than one parent. Networked models are more efficient than hierarchical ones, but they are also more complicated.

RELATIONAL MODELS

Relational models, such as the one shown in Exhibit B.3, follow the logic of spreadsheets; each row is a record and each column is a field within the record. Thus, the relational model has the appearance of a flat file, although it is much more sophisticated. Instead of keeping all data in one file, the relational database may be broken into two or more files (in effect, two or more spreadsheets), or relations, within the database. For example, one relation (file) may contain vendor master data, another holds accounts payable details, while a third holds product data.

Both hierarchical and network databases require entry at the root. Relational models can be entered at any point. Data can be extracted from rows, columns, or combinations thereof. Very powerful commands (operators) can be used to extract data from a single relation or from multiple relations at the same time. New relations data can be made from parts of one or many relations. The three most common commands are *project, select,* and *join.* The project and select commands are used to extract data from a single relation; project takes data from rows, while select takes it from columns. The join command is used to develop a new relation from two or more existing relations.

Relational databases are known for their ease of use by end users. For example, the following questions are typical of the types used:

- Which vendors charge the lowest prices for product X?
- Which products are within 10 percent of their reorder points?
- From which vendors did we order product Y?

Relational databases can be used to simplify data structures. For example, relational databases may use redundancies instead of attempting to eliminate them. Instead of having a single database file for all customer invoices, several relations could be used, as follows.

- The *Customer master* contains all invoice numbers, salesperson codes, and all other relevant customer master data (for example, name, address, credit limit).

Exhibit B.3

The relational database, in which each row represents a record; each column a field. The "Open Items" file contains only the Customer Number, thereby minimizing redundancy.

Customer Master

Customer Number	Address	Credit Limit	Salesperson	Miscellaneous
12376	223 Anywhere	1000	a023	
12377	37 Somewhere	5000	a023	
12378	46 Homeplace	Hold	b071	
12379	10-07 Wherever	2000	a094	
12380	307 Anywhere	10000	b001	
12381	17 Elsewhere	500	a000	

Open Items

Customer Number	Invoice Number	Date Issued	Invoice Total	Freight	Tax
12376	10177	01/23/XX	203.12	2.06	12.19
12376	10247	04/06/XX	1367.44	13.63	54.70
12376	10252	04/12/XX	55.12	1.10	0.00
12381	09654	02/22/XX	66.21	.99	0.00
12382	10011	02/22/XX	703.12	7.40	35.16
12382	10264	03/23/XX	3074.22	22.10	0.00

Salesperson's Master

Salesperson's Number	Salesperson's Name	Territory Number	Commission Rate
a023	Smith, John	Northeast	.45
a024	Jones, Mary	New York	.040
a025	Wilson, Tom	Middle Atlantic	.040
a026	Brown, Harry	Southeast	.042
a027	Salesman, Super	Midwest	.044
a028	Brotherinlaw, Boss's	California	.060

- The *Invoice master* contains everything relating to the invoice except detailed product descriptions. This master uses the product numbers to link to the relation, which contains the product descriptions.
- The *Salesperson master* contains both the salesperson code and name, as well as all other pertinent data.

The relational database would automatically link all of the relations as needed and allow access to each via any of the others. For example, a list of all customers handled by a given salesperson could be obtained.

Appendix C

Telecommunications Scenarios

The purpose of the following scenarios is to present examples of three of the more common telecommunications architectures and identify applicable security and integrity issues.

CENTRALIZED TELECOMMUNICATIONS

ABC is a small, Chicago-based manufacturer and distributor of specialty food products. It has one manufacturing facility, located with its corporate offices, and eight outlets; one is local and the others are in neighboring states. A mainframe computer system in Chicago supports all corporate systems and communications via the public telephone network (meaning, dial-in lines) to a microcomputer in each of the outlets. The outlets transmit information to the corporate mainframe, including daily sales summaries, restock requirements, and monthly operating expense. The corporate computer, in return, sends shipping notices and month-end financial statements to the outlets. There is no particular need for communications between outlets.

This is typically referred to as a centralized or hierarchical network. The mainframe carries most of the processing workload and is the repository for corporate systems and data. The company is able to provide a relatively high level of information security and system integrity through mainframe access control software and a dial-back security system. The dial-back system maintains a list of outlet locations and telephone numbers; when a location calls, it identifies itself to the system and is disconnected. The dial-back system looks up the authorized telephone number and calls back to establish the data upload and download session. If operations grow to the extent that it becomes economical to install leased lines between the mainframe and some or all of the outlets, the dial-in/dial-back procedure to provide security will no longer be needed at those outlets.

CENTRALIZED AND PEER-TO-PEER TELECOMMUNICATIONS

DEF is a retail chain's subsidiary that provides data processing services and credit authorization to the member stores. The stores are concentrated in

the three geographic regions of the Midwest, the Northeast and the West Coast. Each region is supported by a data center that maintains the account information needed for credit authorizations for all cards issued in the region. Stores simply dial-in to the data center for authorizations. Most sales using the chain's proprietary charge card tend to occur in the region in which the card was issued. The chain's charge card is accepted at any of its stores, regardless of region. Therefore, a data center may not have the account information needed to authorize a sale. In this case, the information in the account number is used to determine the origin of the account and the request for authorization is automatically forwarded to the appropriate data center. The diagram shows that there is no direct link between the West Coast and the Northeast. The Midwest data center serves as switch for requests between those two regions. The authorization (or denial) is sent back to the originating data center and relayed back to the store. The added time required to obtain authorization from another region is not noticeable.

The most significant concerns surrounding this use of the telecommunications network are network availability and disaster recovery. Security and integrity issues are less critical in this case because the information that is transmitted is minimal and not especially susceptible to interception and misuse.

DEF is, however, considering adding a third line that would directly connect the Northwest and the West Coast. This redundancy would ensure that one of the three lines could be interrupted without disrupting communication among the three centers. DEF would have to evaluate the cost of the additional line in terms of other business considerations such as the potential cost of accepting uncollectible charges (or turning away customers).

DISTRIBUTED NETWORK

GHI is a specialty recruiting and business services firm that operates a number of small, geographically dispersed offices. Each office maintains its own data processing resources, typically a minicomputer and/or several microcomputers connected within the office by one or more local area networks (LANs). Interoffice communications comprise daily operational and informational messages, and weekly financial data for consolidation at the home office. The volume of transmissions may be relatively significant and tends to be largest among offices located in the same area. The firm has established a leased network connecting the clustered offices, and each cluster to the others. A message received by an office may have originated in any other office, and may have passed through one or more other offices before reaching its final destination.

It is not feasible to impose centrally administered security over the systems and data in each office; the offices are guided by firm-wide policies, but are responsible for assessing their own level of risk and implementing appropriate security measures on their LANs and computers. In this environment there are exposures to lost or misrouted messages and unauthorized access from within the network or from external hackers.

Appendix D

Selected Telecommunications Concepts and Terminology

The electronic transfer of information is quickly replacing the traditional flow of paperwork in the modern business environment. In fact, data communications—digitally coded information sent over a transmission facility—is the fastest growing field in telecommunications.

The purpose of this appendix is to define and discuss selected telecommunications concepts and terminology. This information may not have direct, specific, audit impact; rather, it is intended to assist the auditor in gaining an understanding of the following major topics in telecommunications:

- Communications hardware
- Communications media
- Interfaces, protocols, and standards
- Network architectures
- Communications facilities
- Network management
- Advanced technologies

The reader is also referred to chapter 2, "Local Area Networks," for related information.

COMMUNICATIONS HARDWARE

In addition to mainframes, terminals, and minicomputers, there are other components that constitute the physical network. Modems, multiplexers, front-end processors, and cluster controllers are found in most large data communications networks.

A large percentage of today's data transmission is being sent over analog lines. Analog lines were designed primarily for voice transmission and carry information in continuous electromagnetic waves. Computer data, however, are stored in digital form. This presents a problem. To be transmitted, the digital data need to be transformed into analog waves. This is done with a device called a modem, which is essentially a digital-to-analog

and analog-to-digital converter. Modems function by accepting digital data, transforming them into analog signals and sending the signals through a medium to another modem. The receiving modem then retransforms the signals into digital data. Analog lines are gradually being replaced by digital lines, which carry information in pulses and do not require the transformation of digital data.

Other telecommunications components help make efficient use of network resources. The high cost of communications lines and the fact that a single terminal cannot usually use the full capacity of a line have encouraged the development of devices that combine data streams from many individual low-speed channels and transmit the combined data over a higher-speed communications link. These devices are called multiplexers. Multiplexers operate in pairs—one combines the signals for transmission and one receives and separates them.

Communications network operations require intensive computer interaction, and can place a considerable amount of overhead on a host computer. To alleviate this burden, many vendors use front-end processors (FEPs) to perform network processing tasks, freeing valuable central processing unit (CPU) resources. An FEP is essentially a small computer that is linked to the host by a high-speed channel. It manages data being transmitted in both directions. Management tasks include polling and keeping track of network performance. Polling is used to determine whether a terminal is ready to transmit or receive data. If more sophisticated software is used, the FEP can translate code, perform protocol conversion, and help with error detection and correction.

A cluster controller is designed to support several terminals or printing devices and interface them with the host computer. The basic tasks performed by a cluster controller are to act as a buffer (temporary storage) for data being transmitted to and from the host, to perform basic error detection and correction, and to poll terminals. A cluster controller has buffer space for every attached terminal. Data sent by a user to the host for processing first go to the controller buffer. The host then polls the controller, rather than the terminals, and the controller sends the data.

Facsimile and telex use hardware components that transmit pictures or text over the network. They are used extensively in businesses where it is essential to transmit documents over distance. Facsimile is the reproduction and transmission of an image over a distance by electronic means. Telex is the general name for international teleprinter subscriber services. Telex transmits textual information. It is rapidly being replaced by facsimile.

COMMUNICATIONS MEDIA

Transmission between a sender and receiver travels over a physical path called a medium. The following are the most common media.

Twisted-pair wiring is simply a two- or four-strand copper wire that is twisted to minimize signal distortion. It is inexpensive and used to transmit both voice and data messages.

Coaxial cable is used for data, voice, and video. Coaxial cable consists of one or two central transmission wires surrounded by an insulating layer, a shielding layer, and an outer jacket. Coaxial is used for both long- and short-distance communications needs and is very common in image transmission.

Fiber optic cable uses light pulses rather than electricity to transmit a message. It consists of a glass core surrounded by two layers of glass or plastic insulation. It has a very high capacity and can be used to carry both voice and data.

Microwave transmissions are high-frequency radio waves, relayed through the atmosphere between towers. Because microwave signals travel in a straight line, the transmitter and receiver must be in each other's line of sight.

Satellite transmissions are also microwaves, but are relayed by satellite instead of between towers. Signals are transmitted from a sending earth station up to a satellite where they are rebroadcast to one or more receiving earth stations. Satellites are used for all types of transmission—voice, video, and data.

INTERFACES, PROTOCOLS, AND STANDARDS

Before two network devices can communicate, both devices must adhere to common, predetermined specifications. The specifications applicable to any special linking of two devices is generally referred to as an interface. The interface is the specific functional boundary between the two devices, where the electrical signals, connectors, timing, and handshaking take place. Interface also refers to the procedures, codes, and protocols that enable two entities to interact for a meaningful exchange of information. A protocol is the set of rules governing the transmission of information across communication lines. It provides rules on the following:

- The format of the message
- Which node is sending or receiving information at any given time
- The contingency plan in case of an error in transmission

The numerous protocol specifications in existence all have the same function of providing a structured format for communication. This structured format reduces transmission inefficiencies. Protocols address areas such as physical links, pin voltage levels, connections plug specifications, and the formats of data messages. The same protocol must be observed by both the sending and receiving devices.

Protocols can be established by computer or telecommunications vendors or by standards organizations. Vendor protocols are typically proprietary, compatible only with that vendor's equipment. Protocols set by an organization may become so widely used that they become standards. These protocols are defined by standards organizations and are voluntarily adhered to by manufacturers.

Standards committees are formed specifically to evaluate recommendations from private and public organizations, such as telephone carriers,

hardware vendors, European Post, Telephone and Telegraph (PTTs) agencies, and to use the best recommendations to create a standard. The committee is usually an authorized body within a larger organization, such as a technical society, a government agency, or an international consortium. The following are some of these organizations.

American National Standards Institute. This organization, also known as ANSI, is the principal standards-forming body in the United States. It is also the U.S. representative to the International Standards Organization (ISO).

Electronics Industries Association. This is a trade organization that represents a large number of U.S. electronics manufacturers. The Electronics Industries Association (EIA) standards are hardware-oriented.

Institute of Electrical and Electronic Engineers. In recent years, this American organization has become one of the leaders in establishing standards to advance the market. The Institute of Electrical and Electronic Engineers (IEEE) has become known for its standards work in local area networks (LANs).

International Organization for Standardization. The International Organization for Standardization (ISO) is an international organization made up of ninety nations. ISO has been the front-runner in establishing a comprehensive data link protocol used by most vendors of new data equipment.

International Telegraph and Telephone Consultative Committee. This is an international body composed of representatives from telephone companies around the world. Many of its recommendations are being implemented worldwide, especially in Europe. The International Telegraph and Telephone Consultative Committee (CCITT) is best known for its X.25 packet switching protocol.

NETWORK ARCHITECTURES

Vendors have developed proprietary specifications that provide a framework for constructing communications networks using their equipment. These overall specifications are called communications architectures. They define the logical structure of the types of networks that the vendor supports and how the vendor's various equipment and software products link together in a network.

Although proprietary architectures help solve communications problems within a vendor's product lines, they are not "open" enough to address heterogeneous networks. Today's growing demand for interconnecting multivendor systems and networks has called for open system standards. Perhaps the most visible of these efforts is represented by the ISO's Open Systems Interconnect Model.

The Open Systems Interconnect Model

Open Systems Interconnect (OSI) standards are intended to allow a computer connected to a network to communicate with any other computer on the same network or a different network, regardless of the manufacturer. These standards are based on a seven-layer reference model. This model provides a framework that defines the functions required in a communications transmission and the relationship between them. Two different computers fully implementing the OSI standards for communication would have software and hardware that correspond to each layer of the OSI model. A message sent from one computer to the other would pass "downward" through all seven layers from the application layer to the physical layer in the first computer. It would then travel through the network and enter the second computer, rising "upward" through the seven layers in that machine. This process is reversed when the receiving computer responds. The seven layers in the model are the following.

1. The *physical layer,* the lowest in the hierarchy, establishes the physical connection between the computer equipment and the network.
2. The *data link layer* packages the data for transmission and unpackages it on receipt. It also directs and handles errors in transmission.
3. The *network layer* determines what route the data will take through the network.
4. The *transport layer* controls the quality of the transmission and ensures that the network facilities are used effectively.
5. The *session layer* sets up, manages and disconnects the transmission. It interacts with another session layer to establish and control the dialogue between the two systems.
6. The *presentation layer* translates the message to and from the format used on the network so that it is comprehensible to the sending and receiving programs.
7. The *application layer* is responsible for receiving the message from the sending program in the first computer and handing it over to the receiving program in the second computer. Services provided by this layer can include sending a message, transmitting a file, and accessing a remote database.

Communications Facilities

There are a number of facilities that allow a user to establish communications between two or more locations. Network facilities can be dedicated or switched, public or private. Among the more common network facilities are two kinds of facilities that are used to transmit data from one point to another point. Data communications links can be either dedicated or switched. These basic facilities are similar to those in the voice network, providing either a permanent or a switched (temporary) link between two points. As with voice communications, data in a switched network may be sent over any number of alternative routes depending on the availability of lines. The chosen connection remains open until the end of the conversation, at which time the path is made available to the next user.

A variety of switched transmission services are appropriate for data transmission. For example, data can be transmitted over a switched service such as the public telephone network. Since the telephone company cannot guarantee which path or switching equipment will be used for the connection, the quality of a switched connection varies.

There are also a number of switched digital services that are used strictly for the transmission of data. Such services offer high speed (56 Kilobytes per second (Kbps) or more) transmission over switched, high-capacity digital lines. In all cases, this kind of switched data transmission uses the full capacity of the allocated path or circuit for the duration of the call. For this reason, it is frequently referred to as circuit switching.

An alternative form of switched data transmission is packet-switched networks (PSNs). These networks route blocks or packets of data from multiple users through a collection of circuits and switches. They are often called X.25 networks because of the standard developed by the CCITT for the interface between terminals and computer equipment connected to a packet switching network. X.25 devices can issue packets themselves, so they are directly connected to the local switch node. Packet network users are generally charged for network access, connect time, and the volume of data transmitted. In addition, the monthly charge will usually incorporate a minimum fee.

Packet switching networks are sometimes referred to as value-added networks (VANs), because they offer the user more than just a communications link. VANs can broadly be defined as any publicly available communications network that provides basic transmission facilities plus enhanced services. The enhanced transmission services VANs may provide are encryption, facilitating conversion of data, or enabling incompatible systems to be interconnected by providing protocol conversion. Most VANs are used for data traffic at rates up to 56 Kbps.

A dedicated line network is another data communications alternative. This communications network provides the user with permanent access to a dedicated line that links two or more points. These lines, like those for voice communication, can be leased from a communication company or they can be privately owned and operated. The decision to select a switched or dedicated network can be based on an analysis of costs, message volumes, and service requirements. The break-even point is a function of distance, average connect time, and the urgency of the communication.

Businesses that obtain circuit-switched or PSN services are billed according to usage, similar to standard telephone usage. Organizations that lease dedicated lines are billed at a fixed monthly rate.

Communications facilities can also be divided into public and private networks. Communications networks on which anybody can buy, rent, or lease access are considered public. The most common public networks are the telephone networks and PSNs. The telephone networks are public because every telephone has access to every other one. Private communications facilities are dedicated to a single user or a limited group of users. Examples of private facilities are digital data services and satellite channels. The components of a virtual private network are owned by the organization,

yet communications lines between network locations are managed by a carrier. Neither size nor technology dictates whether a network is public or private.

A variation of the private switched communications network is the software defined network (SDN). An SDN provides the appearance and most of the capabilities of a private network without incurring the large capital outlay or lease costs associated with private network equipment. The capabilities of an SDN are provided through the use of shared facilities under software control located on the carrier's premises, rather than facilities dedicated to individual users. This means that an SDN allows users to build their own networks with the public switched domain. An SDN is composed of dedicated or switched access lines connected to trunks provided by the carrier.

Managed networks are provided to large corporations by third-party vendors who offer computing services such as problem-solving tools, peak-load production/backup, and systems development/testing; information services such as access to financial markets and other financial databases; and application services such as electronic mail, electronic data interchange (EDI), and electronic bulletin boards and catalogs.

Network Management

Organizations that rely heavily on the efficient and continuous functioning of their telecommunications network must commit adequate skilled resources to the management of this network. The basic functions of network management are fault, configuration, performance, security, and accounting management.

Fault Management

The most important function of network management is to maintain the high availability of network services and resources. For this purpose, it is necessary to monitor the network for faults, isolate the faults, and recover from the faults.

Configuration Management

The resources of the network must be initialized and the intended relationships established for proper network operations. Configuration management includes change management as users and locations are added or removed and equipment and requirements change.

Performance Monitoring

To provide efficient service with acceptable response times and throughput, it is necessary to monitor the performance of the network. Performance management may often need to respond immediately to dynamic shifts in network use and transmission volumes.

Security Management

There is a need to define and regulate access to network resources via authentication, authorization, and encryption. Changes to telecommunications related files and programs also need to be monitored.

Accounting Management

The cost of telecommunications facilities and services should be determined, and charges should be established for the use of managed objects to enable the allocation of expenses.

Automated network management systems have become key components in a network due to the growing importance of networks to the user's business and the growing complexity of network operation. These systems enable the organization to monitor network performance and pinpoint malfunctions quickly. Network management systems that are currently available gather network statistics as well as monitor and control the network.

Satellite Technology

Satellites are used to carry voice, data, and video transmissions between locations in the United States and foreign countries. Communications satellites circle the earth in a geosynchronous orbit 22,300 miles above the equator. The orbit is designed such that the satellite stays in the same position relative to the earth. If not for satellites, a large portion of today's communications with remote regions of the United States and distant countries would not be economically feasible. The high transmission rates and wide bandwidth of satellite communications channels allow them to send and receive voice, data, and video signals.

A satellite communications channel starts at the host computer, which is connected to the central office of the satellite communications vendor. The data from this and other local loops are multiplexed into a fiber optic or microwave signal and sent to the satellite vendor's earth station. This signal becomes part of a composite signal that is sent by the earth station to the satellite and then transmitted by the satellite to the receiving earth stations. The satellite uses a transponder (a device that receives radio signals at one frequency and converts them to another frequency for transmission) to transfer the composite signal from one earth station to another. At the receiving earth station, the data are transferred by a fiber optic or microwave link to the satellite vendor's central office. From there, it is broken down into separate communications channels and transmitted over local telephone facilities to the receiving terminals.

Very Small Aperture Terminal

Very small aperture terminal (VSAT) technology provides satellite communications through small economical earth stations that are located on the user's premises. VSATs transmit and receive information directly to and from the satellite, and virtually eliminate dependence on the terrestrial communications links, and local and public-switched network access. VSATs offer companies a rapid and economical method of communicating with remote offices.

Glossary

Advanced peer-to-peer network (APPN). This is an IBM telecommunications network architecture for distributed systems. *Peer-to-peer* refers to the ability of workstations to communicate directly with other workstations. This can be contrasted to IBM's older hierarchical systems network architecture (SNA), which required all communications to go through the host/server computer. APPN is supported on all of IBM's major systems platforms.

Algorithms. These mathematical formulas are used to create check digits, electronic signatures, and encryption of computer data. In most cases, the computer data themselves are a factor in the mathematical formula that creates the check digits, signatures, or encrypted data.

Back-end processors. These special-purpose computers handle the data storage and retrieval functions of the DBMS. This allows the host computer to devote its resources to the application programs. Also known as database machines.

Check digit. This series of characters, usually numerical, is the result of an algorithm or encryption formula if the formula is applied to an associated group of computer data.

Communications protocol. These are the rules or standard procedures to be followed by two nodes in order to establish successful communications. Typically, a protocol defines specific control characters and their meaning, the action to be taken on receipt of each control character and the beginning and conclusion of transmission, the sequence of transmissions, etc. A number of protocols have been defined to meet specific needs, such as to enable faster movement through intermediate nodes (connections) in a network to support error detection and correction over low-quality transmission media and to support special address requirements. Protocols are designed to implement specific layers in the communications architecture. (See appendix D, "Selected Telecommunications Concepts and Terminology," the sections entitled, "Network Architectures," and "The Open Systems Interconnect Model.") Thus, two or more protocols will often be used together to define the complete architecture for a network.

Computer assisted audit technique (CAAT). This program is written by an auditor to manipulate computer data for the purpose of proving an audit objective.

Database administrator (DBA). The person responsible for managing the database as a firm-wide resource.

Database management system (DBMS). Programs and hardware that serve as an interface between the application programs and the physical files.

Data control language (DCL). Part of the database software that defines how the database data elements are to be protected and their integrity maintained.

Data definition language (DDL). Part of the database software that defines the database data elements used in the application programs.

Data dictionary. A catalog of the data elements, their meanings and attributes, and their interrelationships.

Data element. The smallest piece of data that has meaning, typically a field within a record.

Data element matrix. This is a table that shows the relationship of the data elements (fields) to each of the application programs.

Data independence. This is the term for the condition that results if the structure of the database is independent of the application programs that process the data. Thus, the definition and/or layout of the database can be changed without changing the application programs.

Data integrity. The validity of the data.

Data manipulation language (DML). This is the part of the database software that is used by the application programs to store, modify (meaning add, modify, or delete data or relationships), or retrieve data from the database.

Data redundancy. This is the presence of identical data in other application data files.

Direct access storage device (DASD). This computer storage device, typically a disk or diskette, permits direct access to specified data records. In contrast, a serial access device, such as a magnetic tape reel or cassette, requires reading/skipping through all prior records to access the record needed.

Encryption. This is the process of completely coding a set of data by applying a complex formula with a key to the data. The receiver of the data can decode the data by applying the same complex formula and key.

End user computing (EUC). This is a type of information processing whereby an end user is responsible for the development and execution of the EDP application that generates the information employed by that same end user; the MIS department is removed from the process.

File. This comprises the data stored on a storage device, which has been given a name.

Flat file system. The files in this system are defined by the application programs that use them.

Fourth generation languages (4GLs). These higher level programming languages are closer to English in style. 4GLs are user-friendly and nonprocedural—users code *what* is to be accomplished, not *how* to accomplish it, and often do not require a *professional programmer* to perform the coding.

Hierarchical database. In this database file structure, the data elements at one level own the data elements at the next lower level.

Hot site. This backup facility for a computer center contains most of the equipment contained in the original computer center.

Integrated services digital network (ISDN). This communications services architecture permits voice, data, and video communications to be combined and transmitted in a common transmission stream. ISDN is intended to eliminate the need for separate transmission facilities for each type of communications, and to achieve significant economies of scale by moving these over integrated, high-capacity digital transmission channels.

Log file. This computer file is the record of an electronic message that has just been received or sent via telecommunications.

Logical structure. This is the data structure in the database as perceived by the user.

Network. This is a collection of microcomputers, minicomputers, or mainframes, or any combination thereof, connected together in order to share data, peripheral devices (such as printers or disk drives), or other systems resources (such as application programs).

Networked database. This is a database file structure in which each data element can have several owners and can own several other elements. It can support many-to-many relationships as well as one-to-one and one-to-many.

Operating system security. This comprises security facilities to control access to computer resources, which are built into the computer's operating system.

Physical structure. This is the actual structure of the database as it is stored on the computer DASD.

Pointers. Databases use pointers to direct the DBMS to the location of the desired record. These pointers, or chains, point to the next record. Backwards pointers point to the previous record.

Processing control procedures. These control procedures are applied by an auditor to provide assurance that a CAAT processed on a client's computer has not been interfered with.

Protocol. A standard used for the telecommunication of electronic messages defines, for instance, the format of the header and trailer records, technical transmission characteristics and techniques, and addressing schemes.

Query language. A programming language employing plain English commands the query language and provides users with the ability to select and analyze the data in a database.

Recovery/restart. This is the ability of a system to restart after an abnormal termination without the loss of data.

Relational database. A database with the logical structure of a spreadsheet means rows and columns. Each row represents a record, which is an accumulation of all of the fields related to the same identifier or key; each column represents a field common to all of the records.

Root node. This is the highest level data element in a hierarchical database.

Schema. A database schema specifies the name and other characteristics (for example, character type and length of each field) of the data elements and their relationships to each other.

Security software. This software package is used to control access to the resources and data in a computer system.

Software. Any program that runs on a computer is software.

T-Carrier. The T-Carrier system is the North American telephone industry standard for high capacity digital transmission, usually expressed as T-1, T-2, etc., to indicate the capacity of the service provided.

Telecommunications protocol/internet protocol (TCP/IP). This is a widely used communications protocol that was originally developed by the United States government for the Internet network. A major strength of TCP/IP is that it supports communications between workstations and other devices independently of the vendor and type of equipment (in contrast to many proprietary protocols, which typically are designed to support one vendor's systems).

Bibliography

Davis, William S. *Computing Fundamentals—Concepts.* New York: Addison-Wesley Publishing Co., 1991.

Donne, Florence, and CAL Industries. *Local Area Networks—Developing Your System for Business.* New York: John Wiley & Sons Inc, 1989.

EDPAF. "Distributed Data Processing and Network Operations Controls," *Control Objectives.* Carol Springs, IL: EDP Auditors Foundation, 1990.

EDPAF. *Introduction to Telecommunications.* Carol Springs, IL: EDP Auditors Foundation, 1990.

Fitzgerald, Jerry, and Tom Eason. *Fundamentals of Data Communications.* New York: John Wiley & Sons, 1978.

Fortier, Paul J. *Handbook of LAN Technology.* New York: Intertext Publications, McGraw-Hill Inc, 1989.

Gallegos, Frederick, Dana R. Richardson and A. Faye Borthick. *Audit and Control of Information Systems.* Carlsbad, CA: South-Western Publishing Co., 1987.

Haynes, Colin. *Portable Computing—Work on the Go.* New York: American Management Association, 1991.

Hickman, James R. *Management Advisory Services: Expanding Your Accounting Practice.* Colorado Springs: Shepherd's McGraw-Hill, Inc., 1987.

____ . "How To Prevent Computer Losses," *Independent Banker,* Independent Bankers Association (October 1984): 39–43.

____ . "Using Those PC Databases," *ABA Banking Journal,* American Bankers Association (May 1986): 106–108.

IIA. "Telecommunications," *Systems Auditability and Controls,* Second Edition. Altamonte Springs, FL: Institute of Internal Auditors, 1991.

KPMG Peat Marwick Thorne. *Auditing EDP Systems.* Toronto: KPMG Peat Marwick Thorne, 1989.

Martin, James, and Kathleen Kavanagh. *Local Area Networks Architectures and Implementations.* Englewood Cliffs, NJ: Prentice-Hall, 1989.

Martin, James. *Fourth-Generation Languages.* Englewood Cliffs, NJ: Prentice-Hall, Inc., 1985.

McWilliams, Peter. *The Personal Computer Book.* Los Angeles: Prelude Press, 1990.

Medick, James. "Controls in the Design of End-User Systems—Part One." *edpacs: The EDP Audit, Control and Security Newsletter* (February 1989): 1–11.

_____ . "Controls in the Design of End-User Systems—Part Two." *edpacs: The EDP Audit, Control and Security Newsletter* (April 1989): 7–11.

Moeller, Robert R. *Computer Audit, Control, and Security.* New York: John Wiley & Sons, 1989.

Moeller, Robert R., et al. *EDP Auditing.* Boston: Warren, Gorham and Lamont, 1990.

Murphy, Michael A., and Xenia Ley Parker. *Handbook of EDP Auditing.* Boston: Warren, Gorham and Lamont, 1989.

Murphy, Michael A., and Xenia Ley Parker. *Handbook of EDP Auditing.* Boston: Warren, Gorham and Lamont, 1990.

Murphy, Michael A., and Xenia Ley Parker. *Handbook of EDP Auditing.* Second Edition and 1990 Supplement. Boston: Warren, Gorham & Lamont, 1989 and 1990.

Pearson, Olen R., *Personal Computer Buying Guide.* Mount Vernon, NY: Consumers Unions, 1990.

Perry, William E. *Ensuring Database Integrity.* New York: John Wiley & Sons, Inc., 1983.

Ronney, Marshall B., and James V. Hansen. *Data Communications Concepts and Controls.* Altamonte Springs, FL: Institute of Internal Auditors, 1986.

Sheldon, Tom. *Novelle Netware—The Complete Reference.* Berkeley: Osborne McGraw-Hill, 1990.

Schatt, Stan. *Understanding Local Area Networks.* 2nd edition. Carmel, IN: Howard W. Sams Company, 1990.

Schmitt, Thomas. "Recognizing and Controlling the Development of Distributed Programming." *edpacs: The EDP Audit, Control and Security Newsletter* (October 1988): 1–7.

Stoll, Clifford. *The Cuckoo's Egg.* New York: Doubleday, 1989.

"The Auditor and Data Base Management," *Data Processing Management.* Livermore, CA: Auerbach Publishers.

Townsend, Carl. *Networking with the IBM Token-Ring.* 1st edition. Blue Ridge Summit: TAB Books Inc., 1987.

Wang, W.E., and Kraynak, Joe. *The First Book of Personal Computing.* Carmel, IN: Howard Sams & Co., 1990.

Weber, Ron. *EDP Auditing Conceptual Foundation and Practice.* 2nd edition. New York: McGraw-Hill Book Company, 1988.

Wilkinson, Joseph W. *Accounting and Information Systems.* 2nd edition. New York: John Wiley & Sons, 1983.