APPENDIX 9A:

UNDERSTANDING INFORMATION SYSTEMS AND TECHNOLOGY FOR RISK AND CONTROL ASSESSMENT

This appendix expands on the auditor's internal control work by discussing control issues related to the auditee's information systems and use of technology to generate financial statements. It provides further detail on how the auditor's understanding of the auditee's business, information systems, technology, and controls plays a role in control evaluation and audit planning.

INTERNAL CONTROL, INFORMATION SYSTEMS, AND THE AUDIT PLAN

LEARNING OBJECTIVE

1 Explain why an auditor must understand the organization's information systems and technology to plan a financial statement audit.

All aspects of the business world and management have been affected by the rapid evolution of the Internet and by information technology (IT). Auditors are mainly concerned with IT processing, especially as it relates to the accuracy and reliability of the accounting processes and financial reporting. At an overview level, it is useful to look at IT in terms of its

a. business processes—operations of the business in which IT is used

b. applications—application software used by the IT

c. infrastructure—all the technical resources necessary for the operation of the IT system, for example, hardware, operating system software and communications facilities to support internal and external networks

One part of the internal control system is the IT control system, which maintains control over how these elements operate together to achieve their objectives while at the same time reducing risk to a tolerable level. All auditors should be familiar enough with computer processing and controls so that they can complete the audit of simple systems and work with IT experts. An auditor's IT experts are members of the audit team who understand computer technology and are aware of basic audit purposes. They are called in when there is a need for their skills, such as when the transaction automation is very complex.

Rapid and radical changes in IT can be risk factors to a business in many different ways. They can expose the organization to control risks such as unauthorized access to proprietary or confidential information. The auditor considers whether the entity has implemented effective general IT controls and application controls that respond adequately to the risks arising from IT. Controls over IT systems are considered effective if they maintain the integrity of information and the security of the data processed (CAS 315). This is another reason for audit teams to include IT experts who are up-to-date on the latest IT developments.

Internal control evaluation and control risk assessment are essential components of every financial statement audit and must be considered in planning the audit work. Internal control and the controls relevant to the audit are emphasized in the generally accepted auditing standards. When controls are a source of audit evidence, they should be tested for sufficient appropriate evidence that they corroborate the control assessment. The standards specify the extent of audit work necessary to understand the auditee's controls related to significant risks and to assess the risk of material misstatement. If the auditor is to lower the assessed risk of material misstatement because relevant controls are in place, and substantive audit procedures alone cannot provide sufficient appropriate audit evidence, the effectiveness of these controls must be tested.

The Accounting Information System and Control

An accounting system processes transactions, records them in journals and ledgers (either computerized or manual), and produces financial statements without necessarily guaranteeing their accuracy. Nevertheless, the accounting policies and procedures often contain important

elements of control. The accounting instruction of "Prepare sales invoices only when shipment has been made," is a control so long as the people performing the work follow the instruction. The control part of this policy could be expressed as, "Prepare sales invoices and record them only when a shipping document is matched."

All accounting systems do, however, whether computerized or manual, consist of four essential functions—data preparation, data entry, transaction processing, and report production and distribution.

Data preparation is the analysis of transactions and their "capture" for accounting purposes. Transactions themselves are recorded either manually or automatically by programmed procedures. The "capture" is the creation of source documents, such as sales invoices, credit memos, cash receipts listings, purchase orders, receiving reports, negotiable cheques, and the like, which provide the information for data entry. In some computerized accounting systems, however, the paper source documents are not produced first, and transactions are instead entered directly on a keyboard or captured by electronic equipment. For example, your long-distance telephone charges are initially captured by the telephone company's information system using your telephone number, the location called, and the duration of the call.

Data entry often consists of accounting personnel entering transaction information from source documents into an accounting software program. This process may produce a "book of original entry," another name for a journal, such as the sales journal, purchases journal, cash receipts journal, cash disbursements journal, general journal, and others. In advanced paperless systems, electronic equipment may directly enter the accounting information without producing an intermediate journal. For example, your long-distance telephone call is directly entered into the telephone company's revenue and receivable accounts, which later produces your monthly telephone bill.

Transaction processing usually refers to posting the journals to the general ledger accounts, using the debits and credits you learned in other accounting courses. The posting operation updates the account balances, and processing by automated or manual procedures involves editing and validation, calculation, measurement, valuation, summarization, and reconciliation, which support financial statement assertions. When all data are entered and processed, the account balances are ready for placement in reports.

Report production and distribution is the object of the accounting system. Internal management reports and external financial statements display account balances and are useful to management for measuring and reviewing the entity's financial performance, and other functions. The internal reports are management's feedback for monitoring, and for control of operations. The external reports are the financial information for outside investors, creditors, and others.

The accounting system produces a trail of accounting operations, from transaction analyses to reports, often called the **audit trail.** Auditors might follow this trail forwards from source documents to reports to determine that everything that happened (transactions) got recorded in the accounts and reported in the financial statements. Or they might follow it backwards from the financial reports to the source documents to determine whether everything in the financial reports is supported by appropriate source documents.

Accounting controls are entity procedures (both computerized and manual) imposed on the accounting system to prevent, detect, and correct errors and irregularities that might enter and flow through to the financial statements. For example, a control procedure related to the accounting policy cited at the beginning of this section would be, "At the end of each day, the billing supervisor reviews all the sales invoices to see that the file copy has a bill of lading copy attached."

A good control-oriented accounting system will include at minimum a chart of accounts and written definitions and instructions about measuring and classifying transactions. This material is incorporated in computer systems documentation, computer program documentation, systems and procedures manuals, flowcharts of transaction processing, and various paper forms in most organizations. A company's internal auditors and systems staff often review and evaluate this documentation, and independent auditors may review and study that work instead of doing the same tasks over again.

The objective of accounting is to produce correct statements of existence or occurrence, completeness, valuation, rights and obligations, and presentation and disclosure. The overriding objective of an accounting system, therefore, is to produce financial statement assertions that are correct. An accounting system cannot accomplish this objective without an integrated set of control procedures. Statements of objectives, policies, and procedures to that end should be given in the accounting manuals. Management should approve statements of specific accounting and control objectives and ensure that appropriate procedures are used to accomplish them.

REVIEW CHECKPOINTS

1 Where can an auditor find a auditee's documentation of the accounting system?
2 How do managers monitor control effectiveness? Why are controls monitored?
3 What are the key functions of the accounting system?
4 What is the audit trail? What is its use in the audit?

Understanding the Role of Systems in Control Assessment

This section explains how the auditor's understanding of the auditee's business, information systems, technology, and controls plays a role in control evaluation and audit planning. When planning an audit of financial statements, auditors apply their knowledge of the auditee's business, risks, systems, and controls in understanding the impact of how the financial information is produced by the organization. The information systems and IT used influence the nature, timing, and extent of audit procedures in significant accounting processes. Significant accounting processes are those that can materially affect the financial statements. The extent, complexity, and organizational structure of IT use, availability of data, use of CAATs, and the need for specialized skills are all important matters to consider. These issues are explained in detail in the following sections.

Extent of IT Use

Many types of integrated IT systems are available to enterprises ranging from small, local businesses to global, multi-divisional corporations. The extent of IT use in each of a company's significant accounting processes needs to be considered in planning the nature, timing, and extent of audit procedures. Significant IT use in the accounting applications means that the audit team needs IT skills to understand the flow of these transactions. The level of computer use may also affect the nature, timing, and extent of audit procedures. Historically, accounting applications such as payroll, accounts receivable, accounts payable, and inventory were the first processes to be computerized. Now virtually every business transaction is automated, and, in fact, the accounting applications may be a relatively small component of the enterprise's overall information system.

Complexity of IT Operations

The auditor should consider his or her training and experience with the information processing methods used by the auditee when assessing the complexity of computer processing. The complexity of the auditee's IT operations refers to things such as the hardware configuration in place and the degree to which various systems share common files or are otherwise integrated. Another consideration is the availability of transaction trails, as these may only cover short periods and be available only in a very complex or computer-readable form. It may be necessary to coordinate audit procedures with service organization auditors if significant accounting applications are processed at outside service centres. (Refer to Chapter 16 for a discussion of service organization auditors.) These factors affect the type and timing of audit evidence gathering activities, and need to be considered in audit planning.

Organizational Structure of IT

Organizations can differ greatly in the design of their information systems. The main variable might be the degree of centralization within organizational structures. In a highly centralized organizational structure, all significant computer processing activities are controlled and supervised at a central location. The control environment, hardware, and operating systems would be uniform throughout the company. Visiting the central location will give auditors most of the necessary knowledge about information systems and processing. At the other extreme, a highly decentralized organizational structure will allow departments, divisions, subsidiaries, or geographical locations to develop, control, and supervise information systems autonomously. Auditors will need to visit many locations to obtain the necessary audit information. Within an organization, the number of people involved in operating the information systems and their level of relevant IT knowledge are both important audit considerations for assessing segregation of functions and control risk.

Availability of Data

Input data, system-generated files, and other data required by the audit team may exist only for short periods or only in computer-readable form. In some systems, hardcopy input documents may not exist at all because information is entered directly. The data retention policies adopted by an auditee may require auditors to arrange for certain information to be retained for audit purposes. Also, auditors may need to plan to perform certain audit procedures at an interim date while the information is still available.

Certain information generated by the computer system for management's internal purposes may allow the auditors to perform analytical procedures. For example, the information system may report sales information by month, by product, and by salesperson. These details can be analyzed to determine whether the income statement amounts are reasonable and to identify risk areas in the business operations. These procedures can be included in the audit program and provide audit evidence if the reliability of the details can be verified.

Use of Computer-Assisted Audit Techniques (CAATs)

CAATs may be used to increase the efficiency of certain audit procedures and also to enable auditors to apply certain procedures to an entire population of accounts or transactions. There are two main categories of CAATs: (1) audit software and (2) test data. The use of these techniques requires advance planning and may require individuals with specialized IT skills as members of the audit team. These techniques are explained further later in this chapter.

Need for Specialized Skills

To determine the need for specialized IT skills, all aspects of an auditee's computer processing should be considered. In planning the engagement, the audit manager may conclude that certain specialized skills are needed to determine the effect of computer processing on the audit, to understand the flow of transactions, or to design and perform audit procedures. For example, specialized skills relating to various methods of data processing, programming languages, software packages, or CAATs may be needed. Audit team members should possess sufficient IT knowledge in order to know when to call on IT experts, and to understand and supervise their work.

REVIEW CHECKPOINTS

5 How does the extent to which information systems are computerized affect audit planning?

6 What impact does it have on the audit if the transaction trails in an auditee's system are only available in machine-readable form for a limited period?

7 How does the auditee's use of an outside service organization to process accounting information affect planned audit procedures?

8 List several aspects of the auditee's information systems and IT that indicate the need for an IT specialist on the audit team.

9 If an auditee has organized its information systems in a decentralized structure, what impact will this have on performing the audit?

10 What factors in the auditee's systems indicate audit work may need to be performed at an interim date?

BASIC IT-BASED ACCOUNTING INFORMATION SYSTEMS: CHARACTERISTICS AND CONTROL CONSIDERATIONS

LEARNING OBJECTIVE

2 Describe the characteristics and control risks in basic IT-based accounting information systems.

As a basis for developing your understanding of information systems in general and the risks presented by IT use, this section describes the characteristics of simple accounting information systems and their controls. One example of a simple type of system is a **local area network (LAN).** A second one might use a stand-alone **personal computer (PC),** a family of computers that includes small business computers, laptops, and intelligent terminals as are often used by smaller businesses. These small computers can have any or all of the characteristics of advanced systems.

Characteristics of a Simple IT-Based Information System

In a simple LAN-based system, processing occurs at a central network server computer, and several other PCs at that location are connected to the network, which, in turn, is connected to the Internet. The business system connections are usually cable, but wireless networks are also common. Several LANs at different office locations can be combined to a wide area network (WAN). Simple LAN system operations usually involve a small number of people.

A system's central processing facility may use **batch processing** (also called **serial** or **sequential processing**), which means that all records to be processed are collected into groups (batches) of like transactions. Each group can then be processed using the same programs and master files. For example, all payroll records are run at one time, from input in the form of employees' identification numbers and hours worked to employee master file data for pay rate and deduction information. The programs edit and validate the input and then process it to compute the payroll, print cheques, update year-to-date records, and summarize payroll information for management. After completing the run, the programs and data files are saved to storage media such as a magnetic disk, and checking and report output is distributed. Batches can be collected either at a central computer or at other locations. Input transactions may be entered via online terminals and stored on magnetic disks for processing.

Many systems now have online processing capability that was traditionally associated with advanced systems. Data processing is considered **online** (direct access or random) where users can access data and programs directly from terminal devices such as personal computers or **personal digital assistants (PDAs).**

Regardless of where it is done, batch processing is done using the same programs. The master data files take the place of subsidiary and general ledgers in manual systems, and the batches of transactions are similar to journals in a manual system. All transactions in a batch may be listed in printed output, but the transaction detail is usually not printed and, rather than the familiar journal, summary entries are prepared for updating general ledger master files.

Master files contain records with two types of fields: **static fields**, such as employee number and pay rate, and **dynamic fields**, such as year-to-date gross pay and account balances. Most computer processing of accounting data involves changing these fields in

the master file records. The dynamic fields are changed in **update** processing, as was described for batch processing of payroll. The static fields are changed by **file maintenance** processing, which will add or delete entire records (e.g., new employee) or change fields (e.g., new pay rate). Both types of changes, the authorization and control of them, are things that auditors are concerned with.

IT Controls

Control procedures in IT-based accounting system may be classified into two types: general controls and application controls. **General IT controls** relate to any computerized accounting activity, such as controls over access to computer programs and data files. **Application controls** relate to individual accounting applications; for example, programmed validation controls for verifying customers' account numbers and credit limits. The general controls are usually considered early in the audit so will be presented first here.

General IT controls

Organization and Physical Access The proper segregation of functional responsibilities—authority to authorize transactions, custody of assets, recordkeeping, and periodic reconciliation—is as important in computer systems as it is in manual systems. However, computer systems also involve such unique functions as systems analysis, programming, data conversion, library functions, and machine operations. Further separation of duties is, therefore, recommended.

The physical security of computer equipment and limited access to both computer program files and data files are as important as segregation of technical responsibilities. Access controls help prevent improper use or manipulation of data files, unauthorized or incorrect use of computer programs, and improper use of the computer equipment.

The librarian function, or librarian software, should control access to systems documentation and to program and data files through a checkout log (a record of entry and use) or password that records use. Anyone accessing both documentation and data files will have enough information to alter data and programs for his or her own purposes. Locked doors, security passes, passwords, and check-in logs (including those produced by the computer) limit physical access to the system hardware. Scheduled running of computer applications will also detect unauthorized access as the system software reports can be compared to the schedule for variations from the plan that might indicate unauthorized use of computer resources.

Weakness or absence of organizational and access controls decreases the overall integrity of the computer system. When there are deficiencies, the audit team should evaluate the impact on control risk. Auditors review and document the organization and access control of a computer facility through a series of questions, some of which are shown in the following box.

Organization and Physical Access: Selected Questionnaire Items

PRELIMINARY

Prepare or have the auditee prepare a "Computer Profile," which should include an organization chart, hardware and peripheral equipment, communication network, major application processes (batch or online), significant input and output files, software used, and a layout of the data centre.

ORGANIZATION

Are the following functions performed by different individuals so that proper segregation of duties exists?

a. Application programming, computer operation, and control of data files?

b. Application programming and control and reconciliation of input and output?

Are computer operators rotated periodically from shift to shift?

Are programmers and systems analysts rotated periodically from application to application?

DATA AND PROCEDURAL CONTROL

Is there a separate group within the computer department to perform control and balancing of input and output?

Are there written procedures for setting up input for processing?

Is there a formal procedure for distribution of output to user departments?

ACCESS CONTROL

Is access to the computer room restricted to authorized personnel?

Are operators restricted from access to program and application documentation?

Does access to online files require that specific passwords be entered to identify and validate the terminal user?

Online control issues:
viruses
hackers
firewalls

Documentation and Systems Development Documentation communicates the essential elements of the data processing system. It can provide information for the following uses:

- management review of proposed application systems
- application systems history and background and guidelines for developing new applications
- computer application operational data
- control evaluation
- operating instructions
- program revision through details of processing logic
- audit software planning and implementation, or other auditing techniques[1]

Auditors review the documentation to gain an understanding of the system and to determine if the documentation is adequate and whether systems development and documentation standards have been established by the auditee. This is difficult to do if no written standards exist. Standards should be set down by management in a **systems development and documentation standards manual** that covers (1) proper user involvement in the systems design and modification process, (2) review of the specifications of the system, (3) approval by user management and data processing management,

[1] Gordon B. Davis, Donald L. Adams, and Carol A Schaller, *Auditing and EDP, 2nd ed.* (New York: AICPA, 1983), p. 59.

and (4) controls and auditability. Examples of questionnaire items related to systems development documentation are shown in the following box.

Documentation and Systems Development: Selected Questionnaire Items

DEVELOPMENT

Does a written priority plan exist for development of new systems and changes to old systems?

Does the design and development of a new system involve the users as well as computer personnel?

Is there a formal review and approval process at the end of each significant phase in developing a new system?

DOCUMENTATION

Do written standards exist for documentation of new systems and for changing documentation when existing systems are revised?

Does the following documentation exist for each application?

- system flowchart
- record layouts
- program edit routines
- program source listing
- operator instructions
- approval and change record

In many modern, networked information systems, much of the operating system and application software is purchased "off the shelf" from software companies. For example, Windows-based operating systems are used in a majority of organizations, both in network servers and individual desktops. Systems documentation tends to be online, accessed over the Internet by the network technicians. The general control components provide a framework that can be adapted to the variety of computer operations structures that exist in organizations, each with its own specific system description. Since the development of systems and the documentation of the configurations for each may be ad hoc, it is important for auditors to focus on risks to financial reporting. An auditor needs to consider certain aspects when an auditee uses custom-built information systems for applications that are significant to the financial reports and where IT-related control weaknesses are likely to create a risk of material misstatement of the financial statements.

Auditors should review the manuals describing systems development standards to determine whether they are adequate. A review of the documentation will then determine whether the standards are being followed. This review is a test of controls audit of systems development standards (and controls) and it allows auditors to gain an understanding of how a particular system works. This kind of work may require the knowledge and skills of a computer audit specialist.

Auditors are interested in the following elements of the documentation of accounting applications: application description, problem definition , program description, acceptance testing records, computer operator instructions, user department manual, change and modification log, and listing of controls. For example, the **application description** usually contains system flowcharts, descriptions of all inputs and outputs, record formats, lists of computer codes, and control features. The application system flowcharts frequently can be

adapted to audit working paper flowcharts where the flow of transactions can be followed and control points noted. Copies of record formats of significant master files can be obtained for use in computer-assisted audit techniques (CAATs) described later.

The **program description** should contain a program flowchart, a listing of the program source code (such as C++ or Java), and a record of all program changes. Auditors should review this documentation to determine whether programmed controls such as input validations exist.

The **acceptance testing records** may contain test data that auditors can use to perform their own tests of controls audit procedures. The users' manual should indicate procedures and controls in the user departments that submit transactions and receive the output. The log of changes and modifications is important to auditors because it should provide assurance that the application systems have been operating as described for the period under review, and that all changes and modifications have been authorized.

The **controls documentation** is also very important as all the computer controls described in other sections are repeated here, along with manual controls affecting the application program. Reviewing this section provides auditors with an overview of both general controls and controls over transaction processing in a particular application.

Hardware Modern computer equipment is very reliable and machine malfunctions that go undetected are relatively rare. While you are not expected to be a computer systems engineer, you should be familiar with some of the hardware controls so that you can converse knowledgeably with computer personnel.

The most important hardware control in computers is a **parity check.** This ensures that the coding of the computer's internal data does not change when it is moved from one internal storage location to another. Another hardware control, an **echo check,** involves "echoing back" to the sending location a magnetic read after each magnetic write so that the results can be compared. Many computers also contain dual circuitry to perform arithmetic operations twice. Auditors (and management) cannot do much about the absence of these controls and should focus on operator procedures when errors do occur. In addition, many companies now rely on back-end database servers to do much of their processing. The server manages application tasks, handles storage and security, and provides scalability—linking up more PCs and expanding the firm's network. The front-end of the system handles the user interface such as PDAs and PCs. Servers increase the reliability of IT systems by building in redundancies in memory, disk drives, and power supply. Modern computers are largely self-diagnostic, but written procedures should exist for all computer malfunctions, and the causes and resolutions for all of these should be recorded.

Auditors are also interested in **preventive maintenance.** They should determine if maintenance is scheduled and whether the schedule is followed and documented. Frequently maintenance is under contract with the computer vendor, and in such cases auditors should review the contract as well as the record of regular maintenance work. Other general evidence on hardware reliability may be obtained from a review of operating reports and downtime logs.

Data File and Program Control and Security

Controls over physical access to the computer hardware were described previously as part of organization controls. Control over access, use, and security of the data files and programs is equally important and sensitive. Since magnetic storage media can be erased or written over, controls are necessary to ensure that the proper file is being used and that the files and programs are appropriately backed up. Backup involves a retention system for files, programs, and documentation so that master files can be reconstructed in case of accidental loss and processing can continue at another site if the computer centre is lost somehow. Thus, backup files must be stored offsite, away from the main computer. Some of the more important security and retention control techniques and procedures are covered next.

External Labels These are paper labels on the outside of a file (diskettes, cartridges, portable disk packs, or magnetic tapes). The label identifies the contents, such as "Accounts

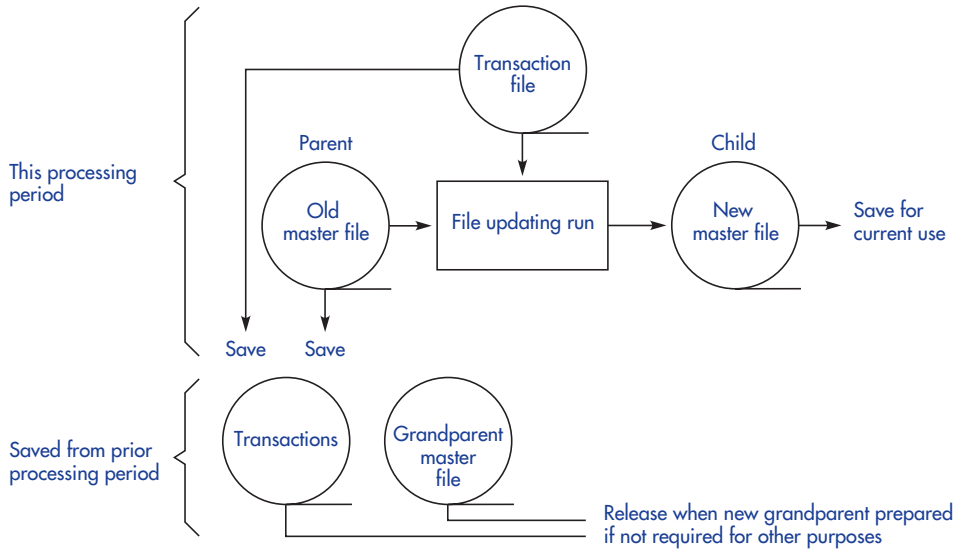
Receivable Master File," so the probability of using the file inappropriately (e.g., in the payroll run) is minimized.

Header and Trailer Labels These are special internal records on magnetic tapes and disks. Instead of containing data, they hold label information similar to the external label. Therefore, the header and trailer labels are sometimes called **internal labels.** Their function is to prevent use of the wrong file during processing. The header label will contain the name of the file and relevant identification codes. The trailer label gives a signal that the end of the file has been reached. They can also be designed to contain accumulated control totals as a check on loss of data during operation; for example, of the number of accounts and the total balance of an accounts receivable file.

File Security Security can be physically enhanced by storage in fireproof vaults, backup in remote locations, or storage in computer-readable, print, or microfilm forms. In the majority of cases, the risk of loss warrants insurance on program and data files.

File Retention Retention practices are related closely to file security and it may provide the first line of defence against relatively minor loss, while security itself consists of all measures taken to safeguard files against total loss. File retention allows reconstruction of damaged records and files through a popular method called the **grandparent-parent-child** concept. With this method, the current master file can be reconstructed using the current transaction file and the prior master file. Exhibit 9A–1 illustrates the file retention plan. Particularly important files may be retained to the great-grandparent generation if this is considered necessary.

EXHIBIT 9A–1 GRANDPARENT, PARENT, AND CHILD IN MAGNETIC TAPE FILES



Disk files are more difficult to reconstruct than tape files because the process of updating old records with new information is "destructive." The old or superseded data on a record are removed (destroyed) when new data are entered in the same place on a disk. One means of reconstruction is to have a disk file "dumped" onto tape or cartridge periodically (each

day or each week). This file copy, along with the related transaction file that is also retained, can serve as the parent to the current disk file (child).

IT Application Controls

Understanding the information system involves reviewing the accounting processes and applications that generate financial information. The designation "application controls" indicates that they are used in each "application"—sales and billing, purchasing, payroll and other specific accounting applications. IT application controls are organized under three categories: input controls, processing controls, and output controls.

Input Control Procedures These controls provide reasonable assurance that data received for processing by the information system have been authorized properly and converted into machine-sensible form, and that data have not been lost, suppressed, added, duplicated, or otherwise improperly changed. These controls also apply to corrected and resubmitted data initially rejected for errors. The following control areas are particularly important:

- **Input authorized and approved.** Only properly authorized and approved input should be accepted for processing in the information system. Authorization might involve a signature or stamp on a transaction document. Some may be general (e.g., a management policy of automatic approval for sales under $500), and some can be computer-controlled (e.g., automatic production of a purchase order when an inventory item reaches a predetermined reorder point). In many ecommerce applications, customers enter their own order information, and procedures validating their entries and ensuring they cannot repudiate their order after it is shipped are key procedures.
- **Check digits.** Numbers often are used in computer systems in lieu of customer names, vendor names, and so forth. One common number validation procedure is the calculation of a check digit. A check digit is an extra number, precisely calculated, that is tagged onto the end of a basic identification number, such as an employee number. The basic code with its check digit sometimes is called a self-checking number. An electronic device can be installed on a data input instrument or the calculation can be programmed to calculate the correct check digit and compare it to the one on the input data. When the digits do not match, the device indicates the error or prints out an input error report. Check digits are used only on identification numbers (not quantity or value fields) to detect coding errors or keying errors such as the transposition of digits (e.g., coding 387 as 837).[2]

Some typical questionnaire items that may be asked during a review of input controls are shown in the next box. These questions should be asked about each significant accounting application.

[2] One check digit algorithm is the "Modulus 11 Prime Number" method:

(a) Begin with a basic number: 814973.

(b) Multiply consecutive prime number weights of 19, 17, 13, 7, 5, 3 to each digit in the basic code number:

8	1	4	9	7	3	
×19	×17	×13	×7	×5	×3	
=152	+17	+52	+63	+35	+9	= 328

Note: the sequence of weights is the same for all codes in given system.

(c) Add the result of the multiplication = 328.

(d) Determine the next higher multiple of 11, which is 330.

(e) Subtract the sum of the multiplication (330 – 328 = 2). This is the check digit.

(f) New account number: 8149732.

Now if this number is entered incorrectly, say it is keypunched as 8419732, the check digit will not equal 2 and an error will be indicated. See J. G. Burch, Jr., F. R. Strater, Jr., and G. Grudniski, *Information Systems: Theory and Practice,* fifth edition (New York: John Wiley & Sons, 1989), pp. 191–93.

Input Control Procedures

SELECTED QUESTIONNAIRE ITEMS

Input controls are primarily preventive in nature, and with increasingly complex computer systems, auditors are placing increasing importance on the input controls. This follows from the garbage in, garbage out or GIGO philosophy that it is generally more cost-effective for a system to prevent misstatements than it is to detect and correct misstatements once they have entered the system. The input controls procedures include the following:

AUTHORIZATION OF TRANSACTIONS

Have procedures been established to ensure that only authorized transactions are accepted, such as (*a*) written approval on source documents, (*b*) general authorizations to process all of the user's transactions, and (*c*) use of identification numbers, security codes, and passwords for remote terminal users?

COMPLETENESS OF INPUT

Are control totals established by the user prior to submitting data for processing? Does someone verify that input data are received on a timely basis from the user and physically controlled in the computer centre?

DATA CONVERSION

Have procedures been established to exercise proper control over processing rejected transactions, including (*a*) positive identification of rejected records, (*b*) review of the cause of rejection, (*c*) correction of rejected records, (*d*) review and approval of the correction, and (*e*) prompt re-entry of the correction at a point where it will be subjected to the same input controls as the original data?

Data Conversion Many errors occur when data is converted into machine-sensible form. Control procedures include the following:

- **Record counts.** These are tallies of the number of transaction documents submitted for data conversion. The known number submitted can be compared to the count of records produced by the data-conversion device (e.g., the number of sales transactions or count of magnetic records coded). A count mismatch indicates a lost item or one converted twice. Record counts are used as batch control totals, during processing, and at the output stage—whenever the comparison of a known count can be made with a computer-generated count.
- **Batch financial totals.** These totals are used in the same way as record counts, except the batch total is the sum of some important quantity or amount (e.g., the total sales dollar in a batch of invoices). Batch totals are also useful during processing and at the output stage.
- **Batch hash totals.** These totals are similar to batch number totals, except the hash total is not meaningful for accounting records (e.g., the sum of all the invoice numbers on invoices submitted to the data input operator).

Edit or Validation Routines Various computer-programmed editing or validation routines can be used to detect data conversion errors. Some of these are listed following:

- **Valid character tests.** These tests are used to check input data fields to see if they contain numbers where there should be numbers and alphabetic letters where there should be letters.

- **Valid sign tests.** Sign tests check data fields for appropriate plus or minus signs.
- **Missing data tests.** These edit tests check data fields to see if any that must contain data for the record entry to be correct are left blank.
- **Sequence tests.** These test the input data for numerical sequence of documents when sequence is important for processing, as in batch processing. This validation routine also can check for missing documents in a prenumbered series.
- **Limit or reasonableness tests.** These tests are computerized checks to see whether data values exceed or fall below some predetermined limit. For example, a payroll application may have a limit test to flag and reject any weekly payroll time record of 50 or more hours. The limit tests are a computerized version of scanning, the general audit procedure of reviewing data for indication of anything unusual that might turn out to be an error.

Error Correction and Resubmission Errors should be subject to special controls. Usually the computer department itself is responsible only for correcting its own errors (data conversion errors, for example). Other kinds of errors, such as those due to improper coding, should be referred to and handled by the user departments. It is a good idea to have a control group log the contents of error reports in order to monitor the nature, disposition, and proper correction of rejected data. Unless properly supervised and monitored, the error-correction process itself can become a source of data input errors.

Processing Control Procedures These controls are designed to provide reasonable assurance that data processing has been performed as intended, without any omission or double-counting of transactions. Many processing controls are the same as input controls, but they are used in the processing phases rather than when input is checked. The following are some important controls in this group:

- **Run-to-run totals.** Movement of data from one department to another or one processing program to another can be controlled by run-to-run totals. Run-to-run refers to sequential processing operations—runs—on the same data. These totals may be batch record counts, financial totals, and/or hash totals obtained at the end of one processing run. The totals are passed to the next run and compared to corresponding totals produced at the end of the second run.
- **Control total reports.** Control totals—record counts, financial totals, hash totals and run-to-run totals—should be produced during processing operations and printed out on a report. Someone (the control group, for example) should compare and/or reconcile them to input totals or to totals from earlier processing runs. Loss or duplication of data thus may be detected. For example, the total of the balances in the accounts receivable master file from the last update run, plus the total of the credit sales from the current update transactions, should equal the total of the balances at the end of the current processing.
- **File and operator controls.** External and internal labels ensure that the proper files are used in applications. The systems software should produce a log identifying instructions entered by the operator and make a record of time and use statistics for application runs. These logs should be reviewed by supervisory personnel.
- **Limit and reasonableness tests.** These tests should be programmed to ensure that illogical conditions do not occur; for example, an asset is depreciated to below zero or a negative inventory quantity is calculated. These sorts of thing, and others considered important, should generate error reports for supervisory review. Other logic and validation checks, described previously under the heading of input edit checks, also can be used during processing.

Some typical processing control questionnaire items are shown in the following box.

Processing Control Procedures

SELECTED QUESTIONNAIRE ITEMS

Processing controls are primarily oriented to detecting misstatements. Processing control procedures enquiries are as follows:

COMPLETENESS

Are programmed control procedures (run-to-run totals) included in each job step during the processing cycle?

Do application programs test the terminal identification or password, or both, for access authorization to that specific program?

Are control totals maintained on all files, and are these verified by the update or file maintenance application program each time a file is used in processing?

FILE CONTROL

Do application programs check for internal header and trailer labels?

Are disk or cartridge files subjected to adequate onsite and offsite backup support?

Are test data files documented, up to date, and kept separate from live data files?

Output Control Procedures Output controls are the final check on the accuracy of the results of computer processing. These controls also should ensure that only authorized persons receive reports or have access to files produced by the system. Typical output control procedures include the following:

- **Control totals.** Output control totals should be compared and/or reconciled to input and run-to-run control totals produced during processing. An independent control group should review output control totals and investigate differences.
- **Master file changes.** Details of these changes should be reported back to the user department that the request for change came from, as an error can be pervasive. For example, changing selling prices incorrectly can cause all sales to be priced wrong. Computer-generated change reports should be compared to original source documents for assurance that the data are correct.
- **Output distribution.** Systems output should be distributed only to persons authorized to receive it, and only the number of reports needed should be produced. A distribution list should be maintained and used to deliver report copies.

Some typical questionnaire items are shown in the following box.

Output Control Procedures:

SELECTED QUESTIONNAIRE ITEMS

Are input control totals reconciled to output totals?

Are input changes to master files compared item by item to output reports of these changes?

Do written distribution lists exist for all output reports from each application?
Are all output files appropriately identified with internal and external labels?

IT System Conversion Controls

Similar input, processing, and output controls need to be in place whenever a system conversion occurs; that is, when one system is replaced by a new one. All the information is transferred from the old system to the new one, and there must be procedures in place to ensure the transfer is complete and accurate.

It is essential that there is an accurate cutoff between the two systems. The conversion process and controls must be documented so that the correctness and accuracy of the work can be assessed during an audit. The auditor often performs audit procedures at the time of the conversion, even if it is not year-end, as this can prevent errors from being carried forward into the year-end balances. These procedures would involve verifying the cutoff and testing the accuracy and completeness of the data transferred.

REVIEW CHECKPOINTS

11 What are the characteristics of IT-based information systems?

12 What general and application controls are used in IT-based systems?

13 Application controls in information systems relate to input, processing, and output. Which of these is mainly oriented to error detection? prevention? correction?

14 What is a self-checking number? Give your own example of one.

15 Describe five types of edit or validation controls and give an example of each for fields on a sales invoice form (e.g., customer name and number, dollar amount of the sale, shipping document number field).

16 What is the difference between an external label and an internal label in magnetic file media? What is the purpose of each?

17 What aspects of documentation, file security, and retention control procedures are unique to computer systems?

18 Describe the purposes of computer system documentation. Why should the auditor review the computer system documentation?

19 What does an auditor need to know about system conversion controls?

Control Risk Assessment in a Simple IT-Based Information System

Material weaknesses in manual and computer controls become a part of the independent auditor's assessment of control risk. Lack of input controls may lead to lost or double-counted data, and poor processing control can permit accounting calculation, allocation, and classification errors to occur. Poor output controls over distribution of reports and other output (negotiable cheques, for example) can lead to misstatements that could make financial statements materially misleading.

Apparent weakness in any of the input, processing, and output control procedures is a matter of concern. However, absence of a control at the input stage may be offset by other controls at later stages. For example, if check digits are not calculated when the input is prepared but transaction numbers are compared to master file numbers and non-matches are rejected and appear in an error report, the control is likely to be satisfactory and effective. Of course, it is more efficient to catch errors early rather than later, but control is still considered effective for the accounting records and financial statements. Internal auditors, however, may be very interested in when controls are applied, since they are concerned about the efficiency of computer operations.

The purpose of the review of internal control is to gain an understanding of the flow of transaction processing and to determine strengths (controls) and weaknesses (lack of controls) that need to be considered in planning substantive audit procedures. General control procedures and the controls of any application systems must be reviewed in a computer environment. The computer and manual controls audit documentation (working papers) are the basis of the audit manager's decision about whether processing is accurate and complete. The audit documentation may consist of questionnaires, such as those illustrated in this chapter, and flowcharts. The general control procedures and the controls in each application system may be subject to tests of controls auditing to determine whether the controls operate effectively. Generally, most auditors find it cost effective to evaluate general and environmental controls before evaluating the more specific application controls. This is because the more general ones have a pervasive impact, are more preventive in nature, and, thus, are more significant.

REVIEW CHECKPOINTS

20 How do control weaknesses affect the audit risk assessment?

21 What is a compensating control?

22 Why do auditors often evaluate environmental and general controls before application controls?

Special Considerations for Small, Stand-Alone IT-Based Information Systems

This section highlights the characteristics and control risks in stand-alone IT-based information systems, such as the PC systems often used in small businesses. While a PC may be used as stand-alone unit, it can also be connected to the Internet (by modem, cable, wireless, etc.) and thus even a simple system faces the risks associated with ecommerce activities. Also, simple PC subsystems are often found in larger organizations where they give more access flexibility and software choice than the main computing system offers. Sometimes significant accounting functions and analyses may be done on stand-alone PC workstations. These informal systems provide audit evidence produced under different, and often less rigorous, control conditions than that produced through the main system, and, therefore, different evaluation may be needed if it is relied on for audit purposes.

Computer activity involving PCs should be included in the assessment of control risk. Since the control objectives do not change, the internal control questionnaires illustrated in this chapter may have to be tailored to the PC installation. The following explanations are designed to assist you in appreciating how the questionnaires, flowcharts, and audit techniques may have to be modified by directing attention to potential problems and controls normally affecting PCs.

Characteristics of a PC-Based Information System

PCs may be elements of a business's distributed system or a stand-alone data processing system. The latter is considered here. It is the control environment and not the computer technology itself that is important to auditors. Small businesses might use any of these resources:

- *Utility programs*. Purchased utility programs are used to enter and change data.
- *Disks*. Magnetic and optical disks, such as DVDs, can be used for accounting file storage. Outboard hard drives or flash drives are useful for longer-term backup file storage.
- *Software packages*. Purchased software packages are often used rather than internally developed application software.
- *Documentation*. Available system, program, operation, and user documentation may be limited or even nonexistent.

In a PC installation, the most significant control weakness is a lack of segregation of duties. This potential weakness may be compounded by the lack of control procedures in the operating system and application programs. Simply turning on the PC might provide

access to all the files and programs, and generate no record of use. The next box highlights these control problems.

Control Problems in PC Environments

LACK OF SEGREGATION OF ACCOUNTING FUNCTIONS

People in user departments may initiate and authorize source documents, enter data, operate the computer, and distribute output reports.

LACK OF SEGREGATION OF COMPUTER FUNCTIONS

Small organizations may not separate the functions of programming and operating the computer. Programs and data are often resident on disk at all times and accessible by any operator.

LACK OF PHYSICAL COMPUTER SECURITY

The computer often is located in the user department instead of in a separate, secure area. Ease of access and use is desired, so access to hardware, programs, and data files may not be adequately restricted.

LACK OF COMPUTER KNOWLEDGE

Individuals responsible for data processing sometimes have limited knowledge of computers, relying instead on packaged software and utility programs with convenient user manuals. Computer professionals may be assigned to monitor mainframe systems but not the PCs.

PC Control Considerations

Most control problems can be traced to lack of both segregation of duties and computerized control procedures. It follows that most of the auditors' control considerations and procedures are designed to overcome these deficiencies. The entire control structure, including manual controls, should be assessed for control strengths that might offset apparent weaknesses. Following are various control considerations and techniques under headings similar to those of the general control procedures discussed previously—organizational, operation, processing, and systems development and modification.

Organizational Control Procedures

The environment in a PC installation is similar to the one-person bookkeeping department because the system analysis, design, and programming functions use off-the-shelf software, with one or two people doing rudimentary client set-up and modification. The main controls limit concentration of functions and establish proper supervision as much as is possible. Implementing the following control procedures will help offset control weaknesses caused by the lack of segregation of duties.

Operation Control Procedures

In PC installations, the most important controls are those over online data (accounting transactions) entry.

Restricting Access to Input Devices. Terminals may be physically locked and keys controlled. Various levels of passwords for accessing files, initiating changes, and invoking programs should be strictly followed.

Standard Screens and Computer Prompting. The computer can be programmed to produce a standard screen format when a particular function is called. All blanks must be completed as prompted by the computer, ensuring that transactions are complete before they are processed.

Online Editing and Sight Verification. The input edit and validation controls discussed previously can be programmed to occur at time of input. In some installations, the data on the screen are not released until they have been sight-verified and the operator signals the computer to accept the entire screen.

Processing Control Procedures

Processing can be controlled by creating files equivalent to those of the grandparent-parent-child retention concept used in batch systems. The following procedures ensure that data processed are in balance, an adequate audit trail is maintained, and recovery is possible:

Transaction Logs. Transactions entered through a terminal should be captured in a computerized log. These records (for each terminal or each class of terminals) should be summarized into the equivalent of batch totals (counts of transactions, financial totals, or hash totals).

Control Totals. Master files should contain cumulative records and financial totals. The control records should be updated automatically.

Balancing Input to Output. A summary of daily transactions and master file control totals should be balanced against manual control totals maintained by the accounting department. If this external balancing is not feasible, techniques similar to the auditor's analytical procedures can be employed to test for reasonableness.

Audit Trail. An audit trail and means for recovery is provided by the transaction logs and periodic dumps of master files. In addition, some PC installations have systems software that can provide a log of all files accessed and all jobs processed.

Systems Development and Modification

The control objectives and techniques in a PC installation are similar to those of a larger system, even though the environment is different. In both cases, many application programs are purchased from computer manufacturers or software vendors not completely familiar with control techniques. These should be reviewed carefully and tested before acquisition and implementation. However, once the auditor becomes familiar with widely used off-the-shelf accounting software packages such as QuickBooks or MYOB, this knowledge is useful in reviewing the systems of other auditees using the same software.

There are a variety of programming languages and application generators used in PC systems (C++, Java) and programming ability may develop within the user group. Most PCs have menu-type micro-instructions, which can be used without technical training. Also, the programming is in an interpretative language, which means it remains in the computer program library in source code form that is easy to change. Standards and authorizations for development and modification become even more important than in larger systems. Only authorized personnel should have the passwords necessary to access the programs for programming that is done through terminals.

EVALUATION APPROACHES FOR INFORMATION SYSTEMS

This section will compare and contrast the following approaches to auditing information systems: auditing around the computer, auditing through the computer with computer-assisted audit techniques (CAATs), and auditing with the computer using generalized audit

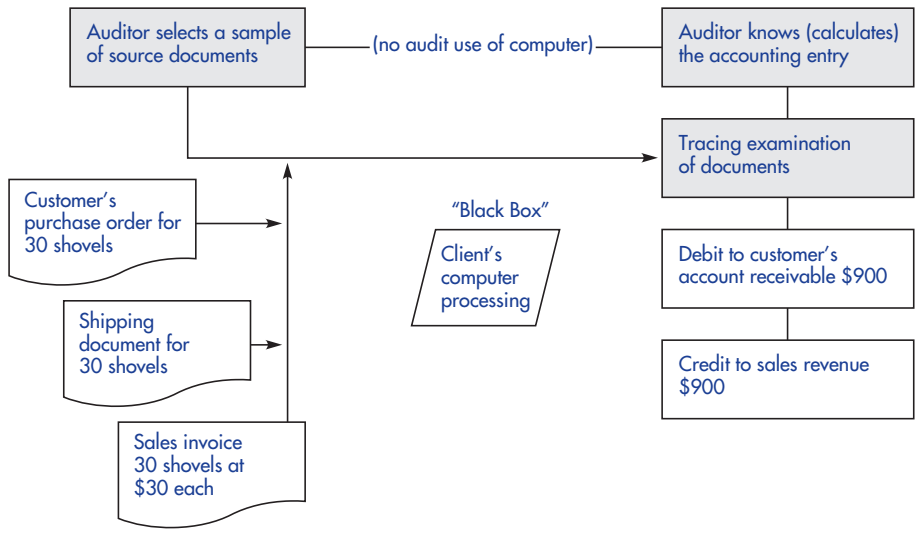
LEARNING OBJECTIVE

3 Describe the following approaches to auditing information systems: auditing around the computer, auditing through the computer with computer-assisted audit techniques (CAATs), and auditing with the computer using generalized audit software (GAS).

software (GAS). When businesses started using computers, two terms were coined to describe the nature of auditing work on computer systems. The first term, "auditing around the computer," came to refer to auditors' attempts to isolate the computer, to treat it like a "black box," and to find audit assurance by vouching data from output to source documents and by tracing from source documents to output. This method was generally considered adequate, as long as the computer was used as a speedy calculator. It may, in fact, be satisfactory today in a case where the information system provides all the physical documentation the auditor needs for sufficient appropriate audit evidence. But auditing around the computer is not always adequate and IT expertise is needed to determine the appropriate approach whenever the auditee's information systems involve IT-based processing.

Auditing around the computer is satisfactory if the controls and information system provide enough visible evidence, such as the input source data, machine-produced error listings, visible control points (e.g., use of batch totals), and detailed printed output. An example of auditing around the computer is offered in Exhibit 9A–2. For this, auditors select a sample of source documents and test the controls over recording transactions, such as sales, in a tracing procedure. The auditee's computer system processes the transactions but the auditor treats it like a "black box," interested only in how the input (customer's order, quantity shipped, and amount invoiced) corresponds to the output (debit to accounts receivable, credit to sales revenue). If sufficient evidence is obtained from the comparison, as in this case, it is not necessary to test the actual processing done by the computer.

EXHIBIT 9A–2 EXAMPLE OF AUDITING AROUND THE COMPUTER



The second term, "auditing through the computer," refers to an actual evaluation of the computer's hardware and software to determine the reliability of operations that cannot be viewed by the human eye. Auditing through has become more common because IT-based information systems often have significant built-in control procedures, and ignoring these would be ignoring important features of internal control.

Auditing through the computer can also mean using computer-assisted audit techniques (CAATs). CAATs refer to the following audit techniques:

- Tests of general IT controls: e.g., using test data to check access procedures to the programs and data.
- Compliance tests of IT application controls; e.g., using test data or an embedded audit program (continuous auditing) to test the functioning of programmed control procedures.

- Tests of details of transactions and balances; e.g., the use of auditor-created or auditor-tested software to verify all (or a sample) of the transaction processing in a system.
- Analytical review procedures; e.g., using audit software to identify unusual fluctuations in amount or volume of transactions.

A third approach, known as auditing with the computer, involves using general audit software (GAS) to perform various audit tests and analytical procedures and to prepare audit file documentation. Though some of the GAS techniques might also be viewed as types of CAATs, for study purposes we will discuss them separately.

REVIEW CHECKPOINTS

23 When would it be appropriate for the financial statement auditor to audit around the computer; that is, to treat the computer systems like a black box?

24 What are CAATs? What does auditing through the computer using CAATs refer to?

25 What is GAS used for?

Computer-Assisted Audit Techniques (CAATs)

In the simple information systems described above, the printed output and logs often show adequate evidence of control performance, making auditing around the computer possible. While internal auditors more frequently utilize this technique, external auditors sometimes must also use the computer as an audit tool to test the controls within the application programs of even simple systems. Thus, the following section explains how the computer can be used as an "auditor's assistant" in testing controls.

Two Approaches for Using the Computer in Control Testing

Auditing through the computer to test controls can be done by auditing the programmed processing controls either with simulated data or with live data reprocessed with an audit program. Auditing of programmed control procedures with simulated data generally is referred to as test data, while the reprocessing of live data to test program controls is called parallel simulation.

Test Data

The test data concept makes use of the fact that once a computer is programmed to handle transactions in a certain way, it will handle every transaction in exactly that same way. This is sometimes called the uniformity principle. Because of it, the audit team need only prepare a limited number of simulated transactions, some with "errors" and some without, to determine whether each control operates as described in the program documentation, the questionnaire responses, and program flowcharts.

The simulated test data will most likely be on a disk, and it may be entered into an online system through computer terminals. Test data is a sample of one of each possible combination of data fields that may be processed through the real system. The transactions may consist of abstractions from real transactions and of simulated transactions generated by the auditors' imagination.[3] The auditors must prepare a worksheet listing each transaction along with its predicted output, based on the program documentation. These must be converted to the normal, machine-sensed input form, and arrangements must be made to process the transactions with the actual program that would be used for real transactions.

To anticipate all data combinations that might exist as transaction input or that might be generated by processing, auditors must be very familiar with the nature of the business

[3] This is a simplification. IT-based information systems may have multiple controls that create thousands of error combinations and possible test transactions. Computerized test data generators are available to help auditors overcome the magnitude of the test data creation task.

and the logic of the programs. They must be able to assign degrees of audit importance to each error-checking control method. Further, they must ensure that the test data do not affect the actual master files.

For example, the objective of the test of sales transactions processing may be to check the controls over accuracy of input data. The set of transactions assembled must include important error conditions in order to determine whether the input and processing controls can detect them. The audit team could create hypothetical transactions with the following features:

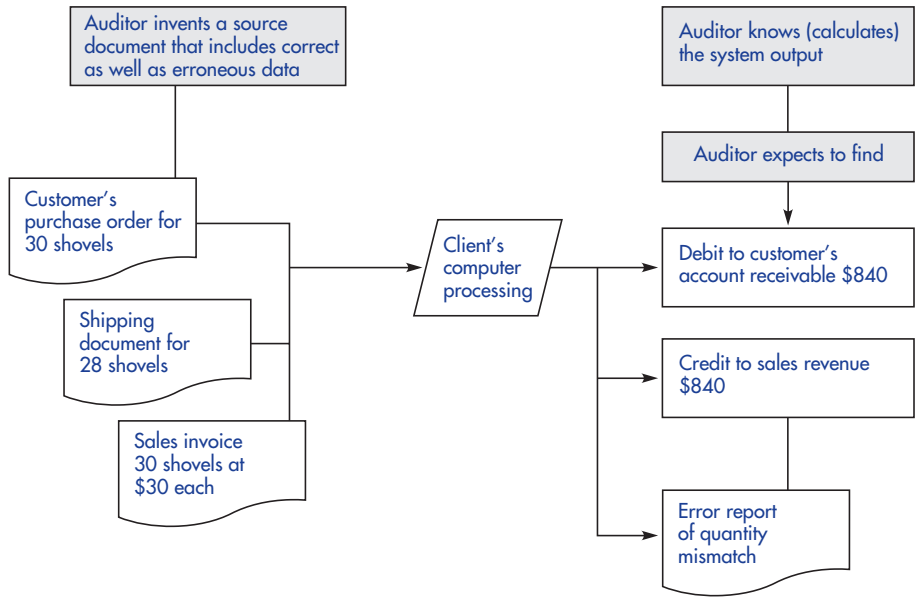
1. customer code number missing
2. customer code number invalid (wrong check digit)
3. bill of lading document number not entered
4. sales amount greater than $25,000
5. sales amount equal to zero
6. sales amount less than zero

The auditors know that transactions with any of those characteristics should produce an error message. Those with valid conditions should not. The auditors arrange to run these simulated transactions on the auditee's system to find out if the program controls operate as they should.

Test data are processed at a single point in time using the auditee program in use during the period under audit. After the analysis of test output, the auditor still must make an inference about processing throughout the entire period. To do so, he or she must also be satisfied, by a review of documentation, that any program changes were authorized and correctly made. Some auditors perform surprise test data procedures during the year. As real-time financial reporting on the Internet becomes more common, continuous auditing techniques will become more important (these are discussed in Appendix 9C on the Online Learning Centre).

Exhibit 9A–3 shows the schema of testing controls with test data. (Compare it to Exhibit 9A–2, the example of auditing around the computer.) In this example, the auditors created source document input containing a shipment of fewer units than the customer ordered. The auditors are looking for an error message indicating that the quantity shipped

EXHIBIT 9A–3 EXAMPLE OF AUDITING CONTROLS WITH TEST DATA (THROUGH THE COMPUTER)

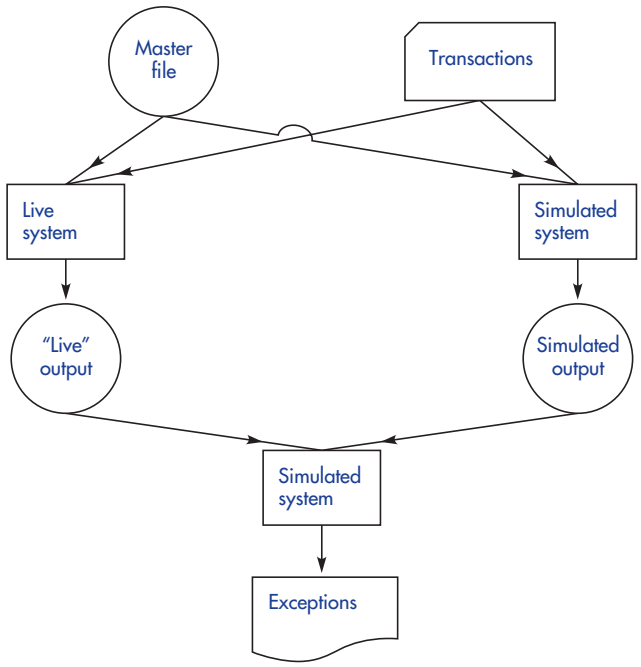


and the quantity billed do not match, perhaps with an accounting entry to charge the customer for the shipped quantity. If this result does not appear from processing this test data, the auditors can conclude that there is a deficiency in the processing control over accurate sales, as they are testing the control procedures embedded in the computer program and using the actual processing program for the test. Using test data in this way, the auditor can focus on unusual transactions or error conditions rather than on a large number of similar transactions. The reasoning is that if the program handles one transaction correctly, then it will handle other similar transactions the same way. However, test data provides a control test only at a specific point in time. In order to rely on the program controls for a period of time, the auditor will also need to obtain assurance that general controls such as controls over program changes are in place and operating over the same period.

Parallel Simulation

In parallel simulation the audit team prepares a computer program (utilizing generalized audit software described later in this chapter) designed to process auditee data properly. The result of the auditors' processing is compared with the result of data processed by the auditee's program. This method is illustrated in Exhibit 9A–4.

EXHIBIT 9A–4 SYSTEM CONCEPT OF PARALLEL SIMULATION



To test the computer program controls, auditors have the options of (1) using the auditee's real programs, (2) having auditee personnel write special programs, or (3) writing their own special programs to collect evidence that the controls work. The first option would be used in the test data technique described in the previous section. The second option requires close supervision and testing to ensure that the auditee's personnel have prepared the audit program correctly. The third option is parallel simulation, and it requires significant programming expertise of the audit staff or close liaison with expert independent programmers. The parallel simulation option is more feasible, however, with generalized audit software (GAS).

The generalized audit software programs consist of numerous prepackaged subroutines that can perform most tasks needed in auditing and business applications. The auditor's programming task consists of writing simple instructions that call up one or more of the

subroutines. Thus, there is no need to write complete, complex programs, and a short training course supplies the expertise needed to use the generalized software. (You will get a closer look at these generalized audit software programs and their capabilities later in this appendix.)

Using the generalized audit program capabilities, an auditor can construct a system of data processing that will accept the same input as the real program, use the same files, and attempt to produce the same results. This simulated system will contain all the controls the auditor believes appropriate, and the process is in this respect quite similar to that of preparing test data. The simulated-system output then is compared to the real-system output, providing audit evidence, just as using test data with the real program does, to arrive at conclusions about the error-detection capabilities of the real system.

A parallel system can also be created by conducting a thorough technical audit of the controls in the auditee's actual program, and then securing a copy of it in the auditors' files. Later this audited copy can be used to process actual auditee data (e.g., at times later in the year under audit or in the following-year audit). This allows comparisons of accounting output from the program the auditee currently uses with the output from the auditors' controlled copy of the program. This approach, often called **controlled reprocessing,** is a version of parallel simulation.

The first audit application of parallel simulation may be very costly, although it probably will be more efficient than auditing without the computer or than utilizing test data. Real economies are realized, however, in subsequent audits of the same auditee.

For the results of the parallel simulation to be valid and relevant to the audit, the audit team must take care to determine that the real transactions selected for processing are "representative." Thus, some exercises in randomly selecting and identifying important transactions must be done. The example of a parallel simulation in the following box is based on the sales accounts receivable system of the Kingston Company example used throughout the text.

PARALLEL SIMULATION

A parallel simulation of Kingston Company's sales invoice and accounts receivable processing system revealed that invoices showing no bill of lading or shipment reference were processed and charged to customers, with a corresponding credit to sales. Further audit of the exceptions showed that the real-data processing program did not contain a missing-data test and the missing shipping references did not trigger error messages. This finding led to (1) a more extensive test of the sales invoice population and comparison to shipping documents and (2) a more extensive audit of accounts receivable for customers who were charged with such sales.

As the example shows, the ultimate goal of using CAATs to test controls is to reach a conclusion about the actual operation of IT-based controls in an information system. This conclusion allows the audit team to assess the control risk and determine the nature, timing, and extent of substantive audit procedures for auditing the related account balances. Based on this control risk assessment, the auditor decides whether subsequent audit work may be performed using machine-readable files that are produced in the system. The data processing control over these files is important as they are used in computer-assisted work using generalized audit software.

REVIEW CHECKPOINTS

26 What is the difference between auditing through the computer and auditing with the computer?

27 What is the difference between test data and parallel simulation, the two approaches used to audit through the computer using computer-assisted audit techniques?

28 What types of control evidence can be provided using CAATs?

29 What role do CAATs play in the overall audit plan?

30 Why does the test data approach only provide evidence that the control operated at a point in time?

31 Why is it important that data selected for parallel simulation tests are representative? How can the audit team determine if the data are representative?

Generalized Audit Software (GAS)

Generalized audit software (GAS) programs are a set of functions used to read, compute, and operate on machine-readable records. Audit software provides audit evidence that is otherwise unavailable or too costly to be feasible. The controls tests covered in this appendix and the IT concepts and terminology introduced in the text are built on in this part of the appendix covering GAS tools. The tools are those used to test controls and gather substantive evidence about transaction details and account balances.

You need to know about GAS because it is used in most audits of accounting records based on computer or database files. There are many different generalized audit software packages in use, and this material does not attempt to prepare you to use any particular one. Instead, it provides you with an understanding of what GAS can accomplish and, most important, where an IT specialist auditor needs to be involved.

Features of GAS

The audit challenges in assessing control risk in a computer environment are (a) gaining access to machine-readable detail records, (b) selecting samples of items for manual or computer audit procedures, (c) performing calculations and analyses of entire data files, and (d) producing audit working papers of the work performed. GAS packages were first developed by CA firms in the mid-1960s for specific audit engagements, and they have been improved and adapted with the changes in technology. The essential advantages of a GAS package are as follows:

- Original programming is not required.
- Designing tests is easy. Many GAS packages are PC based and menu driven so they operate much like commonly used spreadsheet programs.
- For special-purpose analysis of data files, GAS is more efficient than programs written from scratch as less time is spent writing instructions for specific appropriate functions of the software.
- The same software can be used on various auditees' computer systems. Control and specific tailoring are achieved through the auditors' own ability to program and operate the system.

Audit Procedures Performed by GAS

Computer accounting applications capture and generate voluminous amounts of data that usually are available only on machine-readable records. GAS can be used to access the data and organize it into a format useful to the audit team. Audit software can be used to perform the following basic audit techniques.[4]

1. *Recalculation.* Verification of calculations can be done by the computer with more speed and accuracy than by hand. The audit software can be used to test the accuracy of auditee computations and to perform analytical procedures to evaluate the reasonableness of account balances. Examples of this use are to (*a*) recalculate

[4] CICA, *Application of Computer-Assisted Audit Techniques Using Microcomputers* (Toronto: CICA, 1994), p. 16.

depreciation expense, (*b*) recalculate extensions on inventory items, (*c*) compute file totals, and (*d*) compare budgeted, standard, and prior-year data with current-year data.

2. *Confirmation.* Auditors can program statistical or judgmental criteria for selecting customers' accounts receivables, loans, and other receivables for confirmation. The GAS can be used to print the confirmations and prepare them for mailing. It can do everything except carry them to the post office!

3a. *Inspection.* GAS can efficiently compare company records to audit evidence from other sources. The audit evidence must be converted to machine-readable form before it can be compared to the company computer files. Examples are comparing (*a*) inventory test counts with perpetual records, (*b*) adjusted balances on confirmed accounts receivable to the book balances, and (*c*) vendor statement amounts to the company's record of accounts payable.

3b. *Inspection.* Auditors can use GAS to examine records for quality, completeness, consistency, and correctness. This is the computer version of scanning the records for exceptions to the auditors' criteria. For example, GAS can scan (*a*) accounts receivable balances for amounts over the credit limit, (*b*) inventory quantities for negative or unreasonably large balances, (*c*) payroll files for terminated employees, and (*d*) loan files for loans with negative balances.

4a. *Analysis.* Comparing data on separate files can be accomplished by GAS to determine whether compatible information agrees. Differences can be printed out, investigated, and reconciled. Examples are comparisons of (*a*) payroll details with personnel records, (*b*) current and prior inventory to details of purchases and sales, (*c*) paid vouchers to check disbursements, and (*d*) current and prior-year fixed asset records to identify dispositions.

4b. *Analysis.* GAS can summarize and sort data in a variety of ways. For example (*a*) preparing general ledger trial balances, (*b*) sorting inventory items by location to facilitate observations, and (*c*) summarizing inventory turnover statistics for obsolescence analysis.

With enhanced PC processing capabilities, GAS has been further expanded to include expert system modules that incorporate the knowledge of human experts in various domains. Thus, audit expert systems have been developed to provide advice on various technical issues such as internal control evaluation, risk analysis, materiality assessment, and management fraud.

Using Generalized Audit Software

For the most part, the widely used GAS packages are very similar. Regardless of the particular GAS used, five distinct phases are involved in developing a GAS application: (1) define audit objectives, (2) plan the application, (3) design the application, (4) test the application, and (5) process the application and evaluate the results.

1. Define the Audit Objective

The first step in applying GAS is determining specific audit objectives. GAS should be viewed as a tool for accomplishing audit objectives, not as an objective in itself. For example, the general audit objectives might be to audit management's assertions that the accounts receivable balance represents detail accounts which exist, are complete, and are valued correctly. Based on these general objectives, specific procedures may include footing the accounts subsidiary ledger master file, selecting a sample of accounts for confirmation, preparing an aged trial balance, and investigating accounts with overdue balances.

2. Feasibility and Planning

Feasibility should be considered in three ways: (1) Is the use of audit software technically feasible? (2) Are there alternative ways to accomplish the audit task? (3) Which of the

alternatives is the most practical and economical? If the use of GAS is technically feasible, other considerations listed in the following box must be weighed.

Feasibility Considerations

Cost-effectiveness of hardware and software.
Technical complexity including access to auditee data.
Availability of qualified audit software staff.
Other issues including auditee concern about data security.

Source: *Application of Computer-Assisted Audit Techniques Using Microcomputers* (Toronto: CICA, 1994), p. 20.

Audit software may be the most practical way to achieve the audit objective, but it is seldom the only way. Audit resources (qualified people and their time) must be allocated carefully for efficient and effective results. Using GAS requires considerable investment in time and effort and it may be efficient only when repeated use is anticipated on return engagements. Obviously, the data must be available; some files, especially detailed transaction files, often are retained only for a short time. The availability of data files and the degree of auditee cooperation are normally determined during the general and application controls review. The auditee's level of cooperation could be affected by such issues as their concerns over the security of confidential or sensitive data, including the risk of auditors introducing viruses into auditee computers.

After determining the feasibility of using GAS, the audit manager should decide specifically how it will be used, establish control procedures for all subsequent steps, and arrange the logistics with the data centre. Specific planning steps are listed in the following box.

GAS Planning Steps

Set GAS application objectives that are clearly limited to audit objectives.
Determine content and accessibility of the auditee's files.
Determine hardware and software needs.
Define transactions to test procedures and output requirements.
Identify auditee personnel to provide technical assistance.
Prepare application budgets and timetables.
Execute application.
Evaluate the test results.

The planning phase is also the time to define the workpapers that will document the GAS application. The audit manager, not the IT specialist, should determine what computer output representing the GAS application should be retained in the workpapers. The computer output may be in the form of computer-readable workpapers, such as audit files on disk.

3. Application Design

Developing a GAS application is much like the auditee's procedures for developing a new application system. Most GAS packages have an extensive repertoire of powerful instructions to facilitate processing data files and preparing audit output. A complete description of the application phase is beyond the scope of this appendix. Application design involves selecting the sequence of instructions to implement the required test and is something that

should be undertaken only by specially trained audit staff. The documentation of the application design phase may include the GAS application system flowchart, logic descriptions, detailed report layouts, list of control points and procedures, record formats, and a test plan. Frequently, the auditor must obtain a computer dump of a few records of each auditee file to ensure that the design is based on accurate information.

4. Testing

The logic of the application design must be tested with sample auditee data or simulated data until the auditor is confident that the GAS application works as desired. Testing is very similar to the test data approach used in CAATs, as described earlier in this chapter. A copy, not the original, of the auditee's files should be used for testing. The test plan should be extensive enough to test each logic path and anticipate all variations of auditee data. The application design, tests, and results should all be documented.

5. Processing and Evaluation

The foregoing phases are usually accomplished during interim work, before the year-end so that everything is tested and ready for processing of the year-end balances. The processing phase involves (1) verifying that the status of the auditee file has not changed, (2) obtaining a copy of the auditee file, (3) processing the GAS application against the copy of the auditee's file(s), and (4) reviewing results, updating working papers, and retaining audit files. The audit team should carefully monitor and control the actual processing and the output. Control procedures established during the design phase should be followed. Control working papers should have a record of the totals logged on and planned totals compared to results. The audit manager should review the output for reasonableness and clarity. Finally, the documentation workpapers of the application must be completed and filed. There should be adequate documentation for use on a repeat engagement. (In a sense, this documentation is the "audit trail.") The working papers might contain a list of suggested modifications for next year's audit.

In summary, following the feasibility and planning phase, a GAS application should be designed to achieve specific audit objectives. The reliability of general application computer controls, the availability of auditee files, access to the computer and technical assistance, and estimated costs as well as the availability of GAS-trained audit staff must be evaluated. If IT specialists are involved, the non-IT auditor should be actively involved in defining audit objectives and the application plan. Results of testing should be reviewed by the audit manager. The whole GAS process, including copying auditee files and printing out audit results, needs to be run under control of the audit team.

Planning and testing are the most critical tasks in the development of a GAS application. If planning is not adequate, the audit objectives may not be achieved. Problems are likely to occur in subsequent phases and require excessive time and effort to correct. Testing must be adequate or the probability of success is low. It is extremely difficult to correct errors and deficiencies once processing begins after year-end.

Many larger companies have internal auditors skilled in using GAS. Independent (external) auditors may utilize the internal auditors to develop and run the GAS application under the supervision and review of the external audit manager.

GAS Limitations

Notwithstanding the powers of the computer, several good auditing procedures are outside its reach. The computer can compare auditor-made counts to computer records but it cannot observe and count physical things (inventory, for example). The computer cannot examine external and internal documentation; thus, it cannot vouch accounting output to sources of basic evidence. An exception would be an advanced computer system that stored the basic source documents on magnetic or optical media. The auditor would have to test the controls over creation of the files but then would have no choice but to treat the file as a basic "document" source. When manual vouching is involved, computer-assisted selection of sample items is a great efficiency. Probably the biggest problem auditors encounter in using CAATs is obtaining the data in a format that can be used on their computers. Issues

that must be addressed in advance include compatibility of the auditee's with the auditor's system, data structures in the auditee's system, and availability of auditee staff to download the data for use by the auditor.[5] Finally, the computer cannot conduct an enquiry in the limited sense that the enquiry procedure refers to questionnaires and conversations.

Using the Personal Computer as an Audit Tool

The PC is widely used in audit practice. You probably already use PC spreadsheet software like Excel to prepare accounting schedules and word processing software like MS Word to prepare written class assignments. The audit PC software makes use of these same PC software tools to prepare auditing working papers, audit programs, and audit memos. There also are several GAS programs that have been designed for use on PCs; some common ones are Caseware, ACL, and IDEA. These are used internationally and are relatively easy to use since little or no programming is required.[6]

The PC is used regularly in small and large public accounting firms to perform such clerical steps as preparing the working trial balance, posting adjusting entries, grouping accounts that represent one line item on the financial statement into lead schedules, computing comparative financial statements and common ratios for analytical review, preparing supporting workpaper schedules, and producing draft financial statements. Audit firms also use PCs to assess control risk, perform sophisticated analytical functions on individual accounts, access public and firm databases for analysis of unusual accounting and auditing problems, and utilize decision support software in making complex evaluations.

The trend in auditing is towards using highly integrated PC-based processes to control and document the audit from the engagement letter to the audit report. The preliminary audit program will be generated automatically following answers to internal control questionnaires and other programmed audit risk evaluators. The accounting data for the trial balance will be entered into the PC workpapers automatically, and all lead schedules and supporting workpapers will be generated. Related analytical procedure workpapers will be produced using not only auditee data but also related industry data downloaded from the Internet and audit firm Intranets, with suggestions made to update the preliminary audit program. Virtually every element of this integrated PC audit is currently in use or being developed. The integration and the degree of sophistication will develop further uses of the PC as an audit tool. In particular, the availability of audit software enables the auditor to

- simulate all or part of the process by which the data supporting management's assertions were compiled;
- extract information for substantive tests and tests of controls, based on the auditee's data supporting the subject matter of the engagement; and
- prepare information directly relevant to high inherent and control risk items (e.g., approvals of limits for high risk customers).[7]

REVIEW CHECKPOINTS

32 What are some advantages of using GAS?

33 What are five audit procedures that can be performed with GAS?

34 What are some limitations of using GAS?

[5] G. Trites, *Audit of a Small Business* (Toronto: CICA, 1994), pp. 50–51.

[6] Ibid., p. 50.

[7] CICA, *Application of Computer-Assisted Audit Techniques Using Microcomputers* (Toronto: CICA, 1994), p. 17.