CHAPTER 8

Consideration of Internal Control in an Information Technology Environment

Review Questions

8–1 System software monitors and controls hardware and provides other support to application programs. The computer's operating system and utility programs are important components of system software. Application software consists of programs that perform specific tasks, such as updating the accounts receivable master file.

8–2 End user computing makes the user responsible for the development and execution of the IT application that generates the information employed by that same user. In end user computing a user frequently uses off-the-shelf software on a personal computer (work station). A distributed data processing network uses communication links to share centralized data and programs among various users in remote locations throughout the organization.

8–3 A local area network interconnects computers within a limited area, typically a building or a small cluster of buildings.

8–4 User control activities are procedures applied by users to test the accuracy and reasonableness of computer output. Manual application control activities typically involve information system employee follow-up of items listed on computer exception reports.

8–5 Internal labels are machine-readable messages at the beginning and end of a tape or disk file. The header label, at the beginning, identifies the file and its creation date, and the trailer label marks the end of the file and usually includes one or more control totals. External labels are gummed paper labels placed on the outside of a tape or disk pack to identify its contents. Both internal and external labels are designed to prevent computer operators from processing the wrong files.

8–6 The term general control activities is used to describe controls that apply to all or many IT systems in an organization. General control activities include controls over the development of programs and systems, controls over changes to programs and systems, controls over computer operations, and controls over access to programs and data. Application control activities are controls that apply to specific computer accounting tasks, such as the updating of accounts receivable. This category includes programmed controls embedded in computer programs and manual follow-up activities consisting of follow-up procedures on computer exception reports.
8–7 No. While it is true that many duties that might be separated in a manual system are combined in an information systems department, separation of duties is still an important means of achieving internal control. The separation of duties in an information systems department follows a somewhat different pattern than in a manual system. In the latter, duties are separated to enable independent records to be maintained and reconciled. In an information systems department, many records can be maintained and reconciled by computer. However, separation of duties is necessary so that no one employee is in a position to make unauthorized changes in programs or data files. This is accomplished largely through separation of responsibilities for programming, computer operations, and custody of programs and files.

Several traditional separations of duties are also applicable to IT systems. Since the computer performs largely a recordkeeping function, information systems personnel should not have custody of, or control over, assets. Also, information systems personnel should not authorize or initiate transactions. When transactions are initiated elsewhere in the organization, an independent record is usually created that establishes control over the information systems department.

8–8 An online, real-time system is one in which input devices are in direct (online) communication with the computer and all relevant files are instantaneously updated (real-time) by input data.

8–9 Documentation in an information systems department consists of an orderly description of the system and procedures used in all data processing tasks, so that a complete historical record exists of the use of documents, program changes, and so on.

One important form of documentation is system documentation, describing an overall processing system. System documentation includes system flowcharts and descriptions of the nature of input, output, and operations controls. System documentation in the user's manual describes the procedures for entering data, reviewing output, and reprocessing erroneous data.

The details of application programs should be described by program documentation, including such elements as a description of the purpose of the program, program flowcharts, operating instructions for processing the programs, and control sheets for approving programs and changes in programs. Computer operators are provided with the operations manual, consisting of one type of program documentation—the operating instructions for processing the program.

Auditors use the client's documentation in obtaining an understanding of internal control, and in planning audit procedures that make use of the client's computer such as generalized audit programs. Good documentation provides the auditors with much of the background necessary to develop effective test data.

8–10 The minimum amount of segregation of duties in an information systems department requires that programming be separate from the functions of operating the computer and controlling input to the computer. Also, computer operators should not have custody or detailed knowledge of computer programs.

8–11 The data control group is concerned with the day-to-day operation of controls, such as preparing batch control totals, reviewing computer activity logs, reprocessing errors, and distributing output. Internal auditors, on the other hand, do not usually perform routine control activities. Rather, they test and evaluate the effectiveness of existing controls with the purpose of making recommendations for improving the system. Internal auditors often participate in the design of internal controls and subsequently monitor all aspects of the system, including administrative controls and the activities of the data control group.
8–12  

**a.** Record counts are totals that indicate the number of documents or transactions processed; the record counts are compared with totals determined before processing. The purpose of the record count control is to compare the computer-developed totals with the predetermined totals to detect the loss or omission of transactions or records during processing. Unauthorized transactions may also be detected by record counts.

**b.** The limit test control in the computer program compares the result of computer processing against a minimum or maximum amount. The purpose of the limit test is to determine whether certain predetermined limits have been exceeded. Violations are usually printed out for follow-up action.

**c.** A validity test involves the comparison of data against a master file or table for accuracy. For example, employee numbers may be compared with a master file of all valid employees. The purpose of validity tests is to determine that only legitimate data is processed.

**d.** Hash totals are sums of data that would ordinarily not be added, such as unit prices, invoice numbers, and so on. These items are added before processing for later comparison with a total of the same items accumulated by the computer. The purpose of the hash total control is to provide assurance that all, and only authorized, records were processed.

8–13 A system flowchart is an overall graphic representation of the flow of documents and operations in the entire data processing application. A program flowchart, in contrast, is a representation of the major steps and logic of a single computer program.

8–14 Data transmission controls include (only three required):

1. **Parity checks**—A redundant bit added to data that may be used to verify the integrity of the information as it is processed or transmitted.

2. **Data encryption**—A coding of data to make it difficult for unauthorized individuals to read the information.

3. **Message acknowledgment techniques**—Techniques to help ensure that the receiving device receives a complete message. One such technique is an echo check in which the receiving device sends a message that verifies a transmission back to the sending device.

4. **Private lines**—Telephone lines that are owned or leased by an organization and are secure.

8–15 There is an increased risk of unauthorized use of workstations because the machines are located in user work areas. To reduce this risk, system software should maintain a log of computer activities for management review. Also, the workstation's operating system should require authorization codes to be entered to gain access to menus that control specific programs and files. Use after business hours may be prevented by locking away critical programs or replacing the computer operating switch with a key lock.

8–16 Telecommunications is the electronic transmission of information by radio, wire, fiber optics, microwave, laser, and other electromagnetic systems. (For example, owners of two computers may transmit information through the use of their computers, modems, and fiber optics.)
8–17 In distributed data processing systems small business computers, located throughout the company, are linked to a main computer. Users may access programs and files in the main computer and perform limited data processing activities in their own departments.

8–18 Electronic data interchange is a system in which data are exchanged electronically between the computers of different companies. The audit trail is affected in that "hard copy" source documents (e.g., invoices, purchase orders, checks, bills of lading) are replaced with electronic transactions created in a standard format.

8–19 While it is technically possible for an IT system to operate without leaving an audit trail, it is improbable that this will ever occur in an actual system used by a business entity. Valid business reasons exist for the deliberate inclusion of an adequate audit trail in even the most sophisticated IT system. One reason is the practical need for a "management trail," equivalent to an audit trail, which enables management to determine the status and effects of individual transactions. In addition, the Internal Revenue Service and other government agencies require businesses to maintain an audit trail permitting individual transactions to be traced back to their source or forward to the summary totals. Also, businesses that are audited annually usually are anxious to accommodate the needs of their independent auditors in order to reduce the time and cost of the audit.

8–20 The auditors usually begin their consideration of internal control over IT activities with a review of the general controls. This is an efficient approach since application control activities cannot be effective in the absence of general control activities over all IT activities. When the auditors discover that generally control activities are weak, they often decide it is unproductive to test specific application control activities.

8–21 When using the tagging and tracing technique, the auditors tag input transactions with an indicator before they are processed. A computer routine provides a printout of the steps used in processing the tagged transactions. The auditors may then review the printout for unauthorized processing steps.

Questions Requiring Analysis

8–22 The characteristics of a satisfactory plan of organization for an information systems department are as follows:

(1) The information systems department should have as much autonomy from major user departments as is reasonably possible. One means of achieving this autonomy is to have the information systems manager report directly to a vice president of information systems. If information systems are units within the accounting department, the controller should not have direct contact with computer operations.

(2) Within the data processing portion of the information systems department there should be physical and organizational separation of the computer processing unit, the library, and the systems and programming units. Duties of the programmers and the operators should be distinctly separated, and access to the computer center, programs and data should be restricted to authorized persons.

(3) A separate data control group should review the activities of the information systems department.
Batch processing refers to a system in which source documents are collected into "batches" for processing in sequence as one lot. Accumulation of batches means that processing takes place only periodically. Thus, records and files are only as current as the data in the last batch processed.

In an online, real-time system (OLRT), input terminals are in direct (online) electronic communication with the central processing unit. Data entered through these online terminals causes instantaneous (real-time) updating of all relevant files. In an OLRT system, the results of processing a transaction are immediately available and may even influence the completion of the transaction. For example, if a credit sale is entered through an online terminal, the computer would immediately notify the terminal user if that transaction caused the customer's account to exceed a predetermined credit limit. In a batch processing system, the fact that the customer's credit limit had been exceeded would not be known until the batch of credit sale documents containing that transaction had been processed.

Internal control over input is more easily attained in a batch processing system than in an OLRT system. The concept of a "batch" of input data permits such controls as accounting for the numerical sequence of source documents, control totals, hash totals, and item counts. These input controls provide substantial assurance that no data is omitted, added, transposed, or otherwise misstated between the original recording of the transaction and the completion of processing. In an OLRT system, these "batch controls" are no longer applicable. Also, if transaction data are entered directly into terminals, there may be no "hard-copy" source documents for later reference if a transaction is misprocessed.

As compensating controls in an OLRT system, access to terminals is limited to authorized users, and the operating system should be programmed to maintain terminal activity logs to be reviewed for unauthorized use. Also, input validation checks, such as validity tests and limit tests, should be applied to data as it is entered. Still, these controls often are less effective than batch controls in preventing omissions, additions, or misstatements of input data.

In general, personal computers are less flexible, slower at processing data, and smaller in terms of storage capacity than larger computers.

Auditors are concerned with controls over personal computers whenever they are used by the client to process or access financial data. In those situations, use of the personal computers may affect the reliability of the client's financial information.

Other than test data, methods commonly used for testing processing controls in an IT system include using an integrated test facility, controlled programs, program analysis, tagging and tracing, and generalized audit software.

The integrated test facility approach uses a subsystem of dummy records and files built into the regular data processing system. The auditors monitor the processing of test data, studying the effects upon the dummy files, exception reports, and other output produced, and the follow-up of exceptions by the data control group.

Controlled programs involve the processing of current data by using a duplicate program that is held under the control of the auditors. The output is then compared to the output developed by the client's copy of the program.

The program analysis technique involves the use of software that generates a flowchart of the logic of the client's application programs that may then be reviewed by the auditors for unauthorized program steps.

The tagging and tracing of transactions approach involves the selection of certain transactions as they are entered into the system and using software to follow these transactions throughout the various processing steps, each of which if normally printed. Unauthorized processing steps may be detected by reviewing the listing.
Another approach to testing processing controls is processing selected input data using generalized audit software and comparing the results to those obtained by the client's programs. This approach, termed "parallel simulation," is similar to using controlled programs in that current or historical live data may be tested without placing reliance upon the client's equipment or IT personnel.

An inherent limitation in most of the testing methods described above is that agreement between the client's processing results and those obtained by the auditors provides no assurance that the client's system contains processing controls that would detect types of errors not present in the selected input data. For this reason, auditors may use test data in conjunction with the other testing methods.

Generalized audit software can be used to aid the auditor in examining accounts receivable in a fully computerized system by performing such tasks as:

a. **Examining records for quality, completeness, and valid conditions.** For instance, customer accounts might be scanned for account balances in excess of credit limits.

b. **Rearranging data and performing analyses useful to the auditors.** The audit software might be used to arrange the accounts receivable file in the form of an aged trial balance to assist in the evaluation of the allowance for doubtful accounts.

c. **Selecting and printing confirmation requests.** The program can include instructions to select a sample of accounts receivable using any quantifiable selection criteria including a statistical sample. Also, considerable time can be saved by having the computer print the confirmation requests.

d. **Comparing duplicate data maintained in separate files.** For example, the changes in accounts receivable during a given time period can be compared with the detail of credit sales and cash receipts transactions files.

e. **Comparing confirmation information with company records.** For example, the computer can be used to compare payment dates indicated on customer confirmations with client cash receipts records.

An integrated test facility (ITF) is a testing subsystem that is built into the client's processing system. The major advantage of using the technique is that it allows continuous testing of the system. Also, test data is processed with actual data ensuring that the programs tested are the same as those actually used to process transactions.

One disadvantage of the ITF approach is the possibility that personnel may manipulate real data using the test system. Also, there is a risk that the client's real financial records may be contaminated with the test data.

When a service center processes a company's records, the company should establish controls to test the accuracy of the center's activities. Control totals should be developed for input transactions and later reconciled to the center's output. In addition, the company’s personnel should test a sample of the computations performed by the service center’s computer.

When information is not available from a service auditors' report, the auditors of a client using a service center may find it necessary to visit the center to consider the center's internal control. At the center, the auditors obtain an understanding of the internal control.
c. Service centers often engage their own auditors to review their processing controls and provide a report for the users of a center and the users' auditors. These reports are known as service auditors' reports.

d. The service auditors may provide a report on management’s description and design of its controls (Type 1 reports) or that plus operating effectiveness (Type 2 reports).

e. A Type 1 report provides the user auditors with an understanding of the prescribed controls at the service center. It provides no basis for reliance on service center controls, because it does not report the results of tests of controls. A Type 2 report may provide a basis for the user auditors' to reduce their assessments of control risk.

Objective Questions

8–29 Multiple Choice Questions

a. (2) LAN is the abbreviation for local area network, a network that interconnects computers within a limited area, typically a building or a small cluster of buildings.

b. (3) End user computing is most likely in a personal computer environment. End user computing involves environments in which a user department is responsible for developing and running an IT system with minimal or no support from the central information systems department.

c. (1) The exception report should be reviewed and followed up on by the data control group, which also tests input procedures, monitors IT processing, handles the reprocessing of exceptions, and reviews and distributes all computer output.

d. (1) A validity check compares data (for example, vendors or employees) against a master file for authenticity. Accordingly, a validity test will prevent the posting of a payable to a vendor not included in the online vendor master file.

e. (3) In an online, real-time system, users enter individual transactions from remote terminals and files are updated immediately. Therefore, it is important that control be established over computer files through a system of user identification numbers.

f. (3) A distributed data processing system is one in which communication links are used to share data and programs among various users in remote locations throughout the organization. Accordingly, access controls in such a system gain importance.

g. (3) The assessment of “computer control risk” is a vague term and ordinarily there is no assessment of “computer control risk.” Accordingly, it is least likely that auditors will use software to assess it.

h. (2) Auditors use utility programs to perform routine processing functions such as sorting and merging. Generalized audit software programs are utility programs.

i. (2) When deciding whether to engage an information technology specialist, it is doubtful that the auditor would consider the number of financial institutions at which the client has accounts as increases in that number itself doesn’t necessarily result in a
more complex computer application. The other replies all involve factors making such an application more complex.

j. (2) Generalized audit software allows the auditors to independently process their clients' records. The software is flexible and may be used on a variety of IT systems. These packages have not all been written in one language and their use should have no effect on the auditors' need to obtain an understanding of internal control, as indicated in answers (1) and (3). Generalized audit software is primarily used as a tool for performing substantive tests; the software is of limited value in tests of controls.

k. (2) User IDs and passwords for the various users may be used to restrict access to the computer in a manner so as to prevent unauthorized access to sensitive programs.

l. (3) The test data method is used to test controls contained within the program. The audit approach is that of identifying relevant controls within the computer program, and then preparing transactions to run through that program to determine whether the controls operate effectively.

8–30  
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>False</td>
<td>f</td>
</tr>
<tr>
<td>b</td>
<td>True</td>
<td>g</td>
</tr>
<tr>
<td>c</td>
<td>True</td>
<td>h</td>
</tr>
<tr>
<td>d</td>
<td>False</td>
<td>i</td>
</tr>
<tr>
<td>e</td>
<td>True</td>
<td></td>
</tr>
</tbody>
</table>

8–31 Definitions

a. 1 Auditing around the computer involves examining input into and outputs from the computer while ignoring the processing.

b. 6 Test data is a set of dummy transactions developed by the auditor and processed by the client’s computer programs to determine whether the controls that the auditor intends to rely upon are functioning as expected.

c. 3 An integrated test facility introduces dummy transactions into a system in the midst of live transactions and is often built into the system during the original design.

d. 3 An integrated test facility approach may incorporate a simulated division or subsidiary.

e. 4 Parallel simulation involves processing actual client data through the auditor’s software to determine whether the output equals that obtained when the client processed the data.

8–32 Definitions

a. 2 Data warehouse

b. 1 Batch processing

c. 5 End user computing

d. 3 Database system

e. 4 Decentralized processing system

Problems

8–33 SOLUTION: Ultimate Life Insurance Company (Estimated time: 25 minutes)

a. A database is an integrated set of data elements that is shared by two or more application programs.
b. The fundamental advantage of a database is the elimination of data redundancy, which (1) reduces data storage costs, and (2) avoids the problem of data inconsistencies. Also, a database provides management with direct access to large amounts of data for decision making.

c. The integrity of the database may be safeguarded by limiting access to terminals, through the use of locks or user identification codes. A system of authorization (i.e., passwords) may be established to assure that only authorized personnel have access to specific elements of the database. To prevent access after business hours, terminals may be disabled during those hours. In addition, improper use of the terminals may be detected by reviewing computer generated logs of terminal activity.

8–34 SOLUTION: IT Auditing Approaches (Estimated time: 30 minutes)

a. Auditing "around" the computer is an audit approach to testing the reliability of computer processing without the auditors actually making use of the computer. The auditors manually process samples of transaction input data, compare their results with those obtained by the client's computer processing, and investigate any material discrepancies. This approach to the audit of IT-based systems is often contrasted with auditing "through" the computer. In the latter approach, the auditors make use of computer-assisted techniques in performing their testing procedures.

b. CPA's may decide to audit "through" the computer instead of "around" it (1) when the IT applications become complex, (2) when the audit trail becomes partly obscured (as, for example, when transaction data are originally entered into an online terminal without the preparation of source documents), and (3) when it is more efficient than auditing around the computer.

Auditing "around" the computer will be inappropriate and ineffective when a major portion of the internal control is embodied in the computer and when accounting information is intermixed with operating information in a computer program that is too complex to permit ready identification of inputs and outputs. Auditing "around" the computer will also be ineffective if the sample of transactions selected for testing does not include unusual transactions that require special treatment.

Auditing "through" the computer can provide direct assurance as to the functioning of the system and affords the opportunity to test specific controls. This technique is necessary for assessing control risk in all but very simple IT systems.

c. (1) "Test data" is a set of data in some machine readable form (historically on punched cards) representing a full range of simulated transactions, some of which may be erroneous, to test the effectiveness of the control activities and to ascertain how transactions would be handled (accepted or rejected) and, if accepted, the effect they would have on the accumulated accounting data.

(2) CPAs may use test data to gain a better understanding of how the computer processes data. Test data may be used to test the accuracy of programming by comparing computer results with results predetermined manually. Test data may also be used to determine whether or not the system is capable of detecting various types of error conditions. Assurance is provided by the fact that, if one transaction of a given type passes a test, then all transactions containing the identical test characteristics will—if
the appropriate control features are functioning—pass the same test. Accordingly, the volume of test transactions of a given type is not important.

d. To obtain assurance about this matter, the CPAs should consider the client's general controls over IT operations, especially those related to the approval of changes in computer programs. The auditors may also observe the processing of data by the client. If the general control activities are weak the auditors might consider requesting the program on a surprise basis from the librarian and using it to process test data.

The CPAs may also request on a surprise basis that the program be left in the computer at the completion of processing so that they may use it to process test data. This procedure may reveal computer operator intervention as well as assuring that a current version of the program is being tested. This is an especially important consideration in newly organized IT systems undergoing many program changes.

8–35 SOLUTION: Norton Corporation (Estimated time: 25 minutes)

a. Whenever workstations are used for processing financial data, it is important that internal controls be established to help ensure the reliability of financial data.

b. Controls that should be established for the workstation include the following (five required):

- Programs and operating procedures should be fully documented.
- The computer operator should be well trained.
- Segregation of duties should be established to insure that the operator is not in a position to perpetrate errors or irregularities and prevent their detection.
- Critical software should be locked away after business hours.
- The computer's operating system should provide a log of workstation use that may be reviewed by an employee that does not operate the computer or authorize transactions.
- Back-up diskettes or tapes of records should be prepared and stored in a secure location.
- A system of authorization or a locking operating switch should be used to prevent unauthorized use of the workstation.

8–36 SOLUTION: Central Savings and Loan Association (Estimated Time: 25 minutes)

a. The internal controls pertaining to input of information that should be in effect because an online, real-time IT-based system is employed should include:

(1) A self-checking digit or some other redundant check should be used with every account number to prevent an entry to a wrong account.
(2) Input validation checks, such as validity tests and limit tests, should be applied to input data to test their accuracy and reasonableness.
(3) A daily record of all transaction inputs from each input terminal should be produced as a by-product of the computer processing so as to provide a supplemental record.
(4) A log of input transactions should be maintained at each terminal and reconciled on a daily basis (at least with respect to daily totals) with the record of transactions by the terminal maintained by the computer.
(5) Computer personnel should not initiate input to the computer except for testing purposes so that a proper segregation of duties is maintained. Any testing should be done after regular processing is completed and should be recorded in the computer log.
(6) Consideration should be given to establishing an integrated test facility of dummy accounts to enable the internal audit staff to include test data with the actual input.

(7) Computer file security should be provided to assure that entries are not made to the accounts except during normal processing periods.

b. The internal controls that should be in effect pertaining to matters other than information input are as follows:

(1) Account balances should be printed out or dumped on magnetic tape at regular intervals to provide for record reconstruction and testing.

(2) Limit tests should be included in the computer program to permit ready identification of obvious errors or irregularities (e.g., a withdrawal from an account should not exceed the balance on deposit in the account).

(3) The data control group should review terminal logs.

(4) The internal audit staff should have the responsibility for testing accounts and transactions.

(5) Account balance printouts and transaction records necessary to reconstruct the accounts should be maintained in a separate location from the computer file storage as a precaution against simultaneous destruction.

(6) There should be provision for continued operation to avoid a time loss in case of computer failure (e.g., each terminal should have mechanical registers in addition to the computer's electronic registers).

(7) Security should be provided at each terminal to assure that certain operations could be initiated only by authorized supervisory personnel (e.g., user identification numbers and passwords).

8–37 SOLUTION: Alexandria Corporation (Estimated time: 40 minutes)

<table>
<thead>
<tr>
<th>Weakness</th>
<th>Recommended Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>The function of systems analysis and design, programming, computer operations and control should be assigned to different employees. This also should improve efficiency since different levels of skill are involved.</td>
</tr>
<tr>
<td>(2)</td>
<td>In order to properly control usage of the computer, a usage log should be kept and reconciled with running times by the supervisor. The system also should provide for preparation of exception reports on the operator's terminal. These should be removable only by the supervisor or the control clerk independent of the computer operators.</td>
</tr>
<tr>
<td>(3)</td>
<td>Only operating employees should have access to the computer room. Programmers' usage should be limited to program testing and debugging.</td>
</tr>
<tr>
<td>(4)</td>
<td>The company should maintain up-to-date system and program flowcharts, record layouts,</td>
</tr>
</tbody>
</table>
adaptations made by the programmer or new programs.

program listings, and operator instructions. All changes in the system should be documented.
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(5)</td>
<td>Physical control over tape files and system documentation is not adequate. Materials are unguarded and readily available in the computer department. Environment control may not be satisfactory.</td>
<td>Programs and tape libraries should be carefully controlled in a separate location. Preferably a librarian who does not have access to the computer should control these materials and keep a record of usage. The company should consult with the computer company about necessary environmental controls.</td>
</tr>
<tr>
<td>(6)</td>
<td>The company has not made use of programmed controls.</td>
<td>Program controls should be used to supplement existing manual controls. Examples of programmed controls include data validity tests, check digits, limit and reasonableness tests, sequence checks, and error routines for unmatched items, erroneous data, and violations of limits.</td>
</tr>
<tr>
<td>(7)</td>
<td>Insertion of prices on shipping notices by the billing clerk is inefficient and subject to error.</td>
<td>The company's price list should be placed on a master file in the computer and matched with product numbers on the shipping notices to obtain appropriate prices.</td>
</tr>
<tr>
<td>(8)</td>
<td>Manual accounting for the numerical sequence of shipping notices is inefficient.</td>
<td>The computer should be programmed to review the numerical sequence of shipping notices and list missing notices.</td>
</tr>
<tr>
<td>(9)</td>
<td>Control over computer input is not effective. The computer operator has been given responsibility for verifying agreement of output with the control tapes. This is not an independent verification.</td>
<td>The billing clerk (or other designated control clerk) should retain the control tapes and compare them to the daily sales register. This independent test should be supplemented by programming the computer to check control totals and print exception reports where appropriate.</td>
</tr>
<tr>
<td>(10)</td>
<td>The billing clerk should not maintain accounts receivable detail records.</td>
<td>If receivable records are to be maintained manually, a receivable clerk who is independent of billing and cash collections should be designated. If the computer department updates the records, as recommended below, there still should be an independent review by the general accounting department.</td>
</tr>
<tr>
<td>(11)</td>
<td>Accounts receivable records are maintained manually in an open invoice file.</td>
<td>These records could be maintained more efficiently on magnetic disk.</td>
</tr>
<tr>
<td>(12)</td>
<td>The billing clerk should not receive or mail invoices.</td>
<td>Copies of invoices should be forwarded by the computer department to the customer (or to the mailroom) and distributed to other recipients in accordance with established procedures.</td>
</tr>
<tr>
<td>(13)</td>
<td>Maintaining a chronological file of invoices appears to be unnecessary.</td>
<td>This file's purpose may be fulfilled by the daily sales register.</td>
</tr>
</tbody>
</table>
Chapter 08 - Consideration of Internal Control in an Information Technology Environment

(14) Sending duplicate copies of invoices to the warehouse is inefficient.

The computer can be programmed to print a daily listing of invoices applicable to individual warehouses. This will eliminate the sorting of invoices.

In-Class Team Case

8–38 SOLUTION: Jenz Corporation (Estimated time: 45 minutes)

(1) M. Perform customer credit check—Customer credit file is being accessed, making it likely that a credit check is occurring.

(2) Z. Open order file—Processing to the right of #2 begins with "open orders," making this an open order file.

(3) L. Match customer purchase order with sales order—Two copies of the sales order are being combined with the customer purchase order through a manual operation (the trapezoid).

(4) B. Verify agreement of sales order and shipping document—Manual operation includes two copies of the shipping document being combined with the sales order.

(5) H. Release goods for shipment—Department is the warehouse and shipping department, and out of this operation is "shipping information," accordingly goods are being released for shipment.

(6) S. Master price file—The operation below #6 include entering price data; since the first two files being accessed are the accounts receivable master file and the shipping file, this third file must include prices.

(7) O. Prepare sales invoice—Since a document is being prepared through this computerized billing program, it is the sales invoice.

(8) U. Sales invoice—A sales invoice is normally sent to the customer.

(9) I. To accounts receivable department—Copy of the sale invoice informs accounts receivable that the sale has been processed and shipped.

(10) Q. General ledge master file—Because the processing step below includes updating of master files, this is the general ledge master file.

(11) N. Prepare sales journal—Sales transactions are being processed; therefore, a sales journal is prepared.

(12) T. Sales Journal—A sales journal was prepared; the accounting department will receive the sales journal.

(13) Y. Aged trial balance—An aged trial balance is prepared; the credit department will receive such a report.