CHAPTER 12

IMPLICATIONS OF INFORMATION TECHNOLOGY FOR THE AUDIT PROCESS

Just Because The Computer Did The Work Doesn't Mean It's Right

Allen, the senior auditor, is assigned to work on an audit of a subsidiary of an international UK financial institution, Robot Banks in Singapore. Robot recently merged with another Singapore subsidiary of another international UK financial institution, Apache Banks. Robot Banks decided to roll out a new system that consolidated all loan data onto one system.

During the audit planning phase, Allen overhead a conversation between two employees in Robot's office cafeteria. "How was your weekend?" one guy asked the other. "Terrible, I had to come in during the weekend to perform reconciliations between the old and the new trade systems. The worst thing is nobody knows why some figures were not captured in the new system. There are definitely a lot of issues!"

"Oh no," Allen thought to himself, "it means the audit on revenue recognition of loans will have to be tested extensively." Normally, the merger of two subsidiaries would mean more extensive testing of account balances. The addition of rolling out a new system would mean that Allan would not only have to ramp up the number of audit tests, but will be unlikely to rely on summary or computed data generated by the computer system. He would have to go back to the source documentation when performing his audit tests. "At least all the data from Robot is fully electronic, so I can perform audit analytics on the data from the two original systems," Allen thoughtfully said to himself. "Because audit analytics means I don't have to select samples above a pre-determined amount, I can review all transactions and weed out the 'odd' transactions. I'll then have to look into those 'odd' transactions. It'll be a little like putting students to a common test. For those who pass, no further work is needed. For those who fail, more probing will be needed to understand why they failed and how they can pass in the future."

LEARNING OBJECTIVES

After studying this chapter, you should be able to

- **12-1** Describe how IT improves internal control.
- **12-2** Identify risks to accounting systems specific to IT.
- **12-3** Explain how general controls and application controls reduce IT risks.
- **12-4** Describe how general controls affect the auditor's testing of application controls.
- **12-5** Use test data, parallel simulation, and embedded audit module approaches to test automated controls.
- **12-6** Identify issues for e-commerce systems and other specialized IT systems.

Auditors cannot rely on information just because it is generated by a computer. People often assume "the information is correct because the computer produced it." Unfortunately, auditors sometimes depend on the untested accuracy of computer-generated output because they forget that computers perform only as well as they are programmed. Before concluding that computer-generated information is reliable, auditors must understand and test computer-based controls.

This chapter builds on Chapter 10's coverage of internal control and how the auditor obtains an understanding of internal control, assesses control risk, and does tests of controls. We will examine how the client's integration of information technology (IT) into the accounting system affects risks and internal control.

The use of IT improves internal control by adding new control procedures done by the computer and by replacing manual controls subject to human error. At the same time, IT introduces risks, which the client can manage by using controls specific to IT systems. In this chapter, we highlight risks specific to IT systems, identify controls that can be implemented to address those risks, and explain how IT-related controls affect the audit.

HOW INFORMATION TECHNOLOGIES IMPROVE INTERNAL CONTROL

OBJECTIVE 12-1

Describe how IT improves internal control.

Virtually all entities, including small, family-owned businesses, rely on IT to record and process business transactions. As a result of explosive advancements in IT, even relatively small businesses use personal computers with commercial accounting software for their accounting. As businesses grow and have increased information needs, they typically upgrade their IT systems. The accounting function's use of complex IT networks, the Internet, and centralized IT functions is now commonplace.

There are several benefits to internal control that result from the continued integration of IT in accounting systems:

- *Computer controls replace manual controls.* The obvious benefit of IT is the ability to handle large amounts of complex business transactions cost-effectively. Because computers process information consistently, IT systems can potentially reduce misstatements by replacing manual procedures with automated controls that apply checks and balances to each processed transaction. This reduces the human errors that often occur in manually processed transactions.

  Computers now do many internal control activities that once were done by employees, including comparing customer and product numbers with master files and comparing sales transaction amounts with preprogrammed credit limits. Online security controls in applications, databases, and operating systems can improve separation of duties, which reduces opportunities for fraud.
- *Higher-quality information is available.* Complex IT activities are usually administered effectively because the complexity requires effective organization, procedures, and documentation. This typically results in providing management with more and higher-quality information, faster than most manual systems. Once management is confident that information produced by IT is reliable, management is likely to use the information for better management decisions.

ASSESSING RISKS OF INFORMATION TECHNOLOGY

OBJECTIVE 12-2

Identify risks to accounting systems specific to IT.

Although IT can improve a company's internal control, it can also affect the company's overall control risk. Many risks in manual systems are reduced and in some cases eliminated. However, there are risks specific to IT systems that can lead to substantial losses if ignored. If IT systems fail, organizations can be paralyzed by the inability to retrieve information or by the use of unreliable information caused by processing errors. These risks increase the likelihood of material misstatements in financial statements. Specific risks to IT systems include:

1. Risks to hardware and data
2. Reduced audit trail
3. Need for IT experience and separation of IT duties

Risks to Hardware and Data

Although IT provides significant processing benefits, it also creates unique risks in protecting hardware and data, as well as introducing potential for new types of errors. Specific risks include the following:

- *Reliance on the functioning capabilities of hardware and software.* Without proper physical protection, hardware or software may not function or may function improperly. Therefore, it is critical to physically protect hardware, software, and related data from physical damage that might result from inappropriate use, sabotage, or environmental damage (such as fire, heat, humidity, or water).
- *Systematic versus random errors.* When organizations replace manual procedures with technology-based procedures, the risk of random error from human involvement decreases. However, the risk of systematic error increases because once procedures are programmed into computer software, the computer processes information consistently for all transactions until the programmed procedures are changed. Unfortunately, flaws in software programming and changes to that software affect the reliability of computer processing, often resulting in many significant misstatements. This risk is increased if the system is not programmed to recognize and flag unusual transactions or when transaction audit trails are inadequate.
- *Unauthorized access.* IT-based accounting systems often allow online access to electronic data in master files, software, and other records. Because online access can occur from remote access points, including by external parties with remote access through the Internet, there is potential for illegitimate access. Without proper online restrictions such as passwords and user IDs, unauthorized activity may be initiated through the computer, resulting in improper changes in software programs and master files.
- *Loss of data.* Much of the data in an IT system are stored in centralized electronic files or off-site via cloud computing. This increases the risk of loss or destruction of entire data files. This has severe ramifications, with the potential for misstated financial statements and, in certain cases, serious interruptions of the entity's operations.

Reduced Audit Trail

Misstatements may not be detected with the increased use of IT due to the loss of a visible audit trail, as well as reduced human involvement. As accounting systems continue to embrace emerging technologies, automated procedures continue to replace traditional types of authorizations in many IT systems.

- *Visibility of audit trail.* Because much of the information is entered directly into the computer, the use of IT often reduces or even eliminates source documents and records that allow the organization to trace accounting information. These documents and records are called the audit trail. Because of the loss of the audit trail, other controls must be put into place to replace the traditional ability to compare output information with hard-copy data.
- *Reduced human involvement.* In many IT systems, employees who deal with the initial processing of transactions never see the final results. Therefore, they are less able to identify processing misstatements. Even if they see the final output, it is often difficult to recognize misstatements because underlying calculations are not visible and the results are often highly summarized. Also, employees tend to regard output generated through the use of technology as "correct" because a computer produced it.
- *Lack of traditional authorization.* Advanced IT systems can often initiate transactions automatically, such as calculating interest on savings accounts and ordering inventory when pre-specified order levels are reached. Therefore,

proper authorization depends on software procedures and accurate master files used to make the authorization decision.

Need for IT Experience and Separation of IT Duties

IT systems reduce the traditional separation of duties (authorization, record keeping, and custody) and create a need for additional IT experience.

- *Reduced separation of duties.* Computers do many duties that were traditionally segregated, such as authorization and record keeping. Combining activities from different parts of the organization into one IT function centralizes responsibilities that were traditionally divided. IT personnel with access to software and master files may be able to steal assets unless key duties are segregated within the IT function.
- *Need for IT experience.* Even when companies purchase simple off-the-shelf accounting software packages, it is important to have personnel with knowledge and experience to install, maintain, and use the system. As the use of IT systems increases, the need for qualified IT specialists increases. Many companies create an entire function of IT personnel, while other companies outsource the management of IT operations. The reliability of an IT system and the information it generates often depends on the ability of the organization to employ personnel or hire consultants with appropriate technology knowledge and experience.

INTERNAL CONTROLS SPECIFIC TO INFORMATION TECHNOLOGY

OBJECTIVE 12-3

Explain how general controls and application controls reduce IT risks.

To address many of the risks associated with reliance on IT, organizations often implement specific IT controls. Auditing standards describe two categories of controls for IT systems: general controls and application controls.

General controls apply to all aspects of the IT function, including IT administration; separation of IT duties; systems development; physical and online security over access to hardware, software, and related data; backup and contingency planning in the event of unexpected emergencies; and hardware controls. Because general controls often apply on an entity-wide basis and affect many different software applications, auditors evaluate general controls for the company as a whole.

Application controls typically operate at the business process level and apply to processing transactions, such as controls over the processing of sales or cash receipts. Auditors must evaluate application controls for every class of transactions or account in which the auditor plans to reduce assessed control risk because IT controls will be different across classes of transactions and accounts. Application controls are likely to be effective only when general controls are effective.

Figure 12-1 illustrates the relationship between general controls and application controls. The oval represents the general controls that provide assurance that all application controls are effective. Effective general controls reduce the types of risks identified in the boxes outside the general controls oval in Figure 12-1.

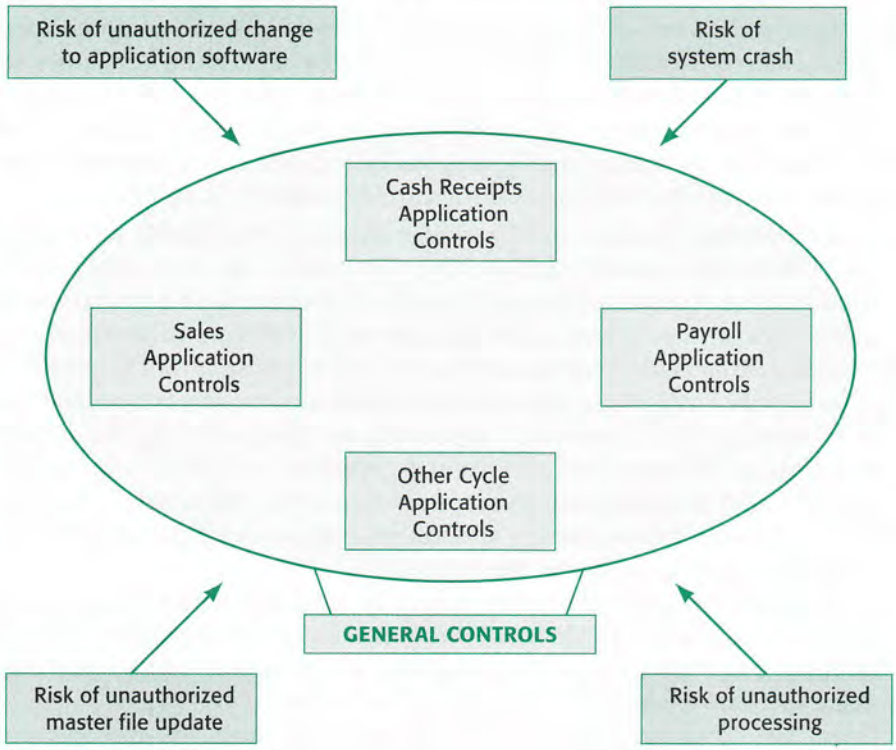
Table 12-1 describes six categories of general controls and three categories of application controls, with specific examples for each category. Let's examine these categories of general and application controls in more detail.

General Controls

Similar to the effect that the control environment has on other components of internal control discussed in Chapter 10, the six categories of general controls have an entity-wide effect on all IT functions. Auditors typically evaluate general controls early in the audit because of their impact on application controls.

Administration of the IT Function The board of directors' and senior management's attitude about IT affect the perceived importance of IT within an organization. Their oversight, resource allocation, and involvement in key IT decisions each signal

FIGURE 12-1 Relationship Between General and Application Controls



the importance of IT. In complex environments, management may establish IT steering committees to help monitor the organization's technology needs. In less complex organizations, the board may rely on regular reporting by a chief information officer (CIO) or other senior IT manager to keep management informed. In contrast, when management assigns technology issues exclusively to lower-level employees or outside

TABLE 12-1 Categories of General and Application Controls

Control Type	Category of Control	Example of Control
General controls	Administration of the IT function	Chief information officer or IT manager reports to senior management and board.
	Separation of IT duties	Responsibilities for programming, operations, and data control are separated.
	Systems development	Teams of users, systems analysts, and programmers develop and thoroughly test software.
	Physical and online security	Access to hardware is restricted, passwords and user IDs limit access to software and data files, and encryption and firewalls protect data and programs from external parties.
	Backup and contingency planning	Written backup plans are prepared and tested regularly throughout the year.
	Hardware controls	Memory failure or hard drive failure causes error messages on the monitor.
Application controls	Input controls	Preformatted screens prompt data input personnel for information to be entered.
	Processing controls	Reasonableness tests review unit-selling prices used to process a sale.
	Output controls	The sales department does postprocessing review of sales transactions.

consultants, an implied message is sent that IT is not a high priority. The result is often an understaffed, underfunded, and poorly controlled IT function.

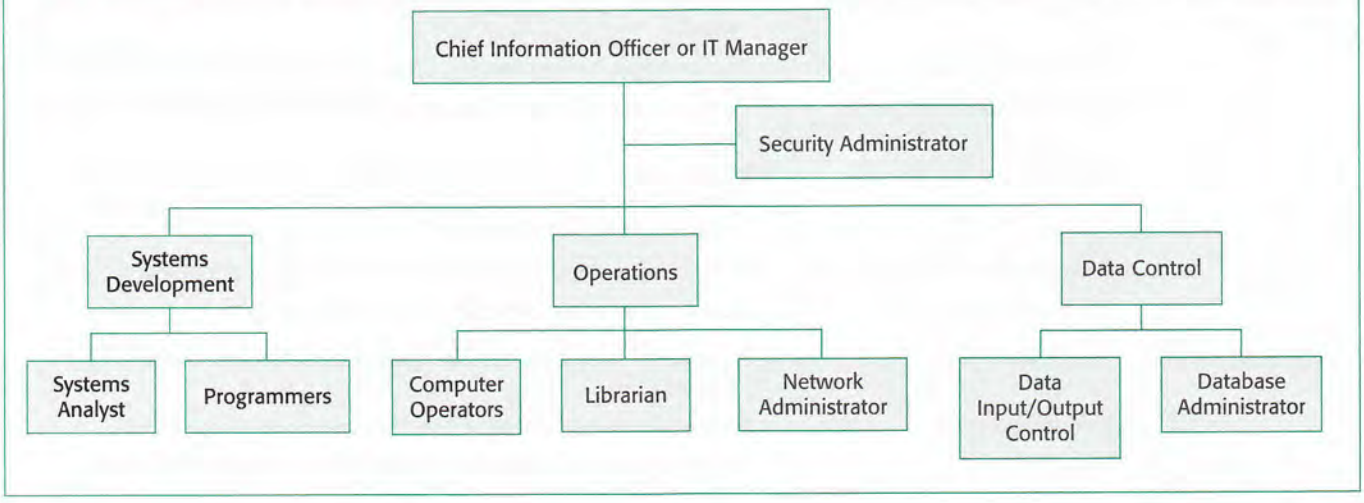
Separation of IT Duties To respond to the risk of combining traditional custody, authorization, and record-keeping responsibilities by having the computer perform those tasks, well-controlled organizations respond by separating key duties within IT. For example there should be separation of IT duties to prevent IT personnel from authorizing and recording transactions to cover the theft of assets. Figure 12-2 shows an ideal separation of duties. Ideally, responsibilities for IT management, systems development, operations, and data control should be separated as follows:

- *IT management.* The CIO or IT manager should be responsible for oversight of the IT function to ensure that activities are carried out consistent with the IT strategic plan. A security administrator should monitor both physical and online access to hardware, software, and data files and investigate all security breaches.
- *Systems development.* Systems analysts, who are responsible for the overall design of each application system, coordinate the development, acquisition, and changes to IT systems by IT personnel responsible for programming the application or acquiring software applications and personnel outside IT who will be the primary system users (such as accounts receivable personnel). Programmers develop flowcharts for each new application, prepare computer instructions, test the programs, and document the results.

  Programmers should not have access to input data or computer operations to avoid using their knowledge of the system for personal benefit. They should be allowed to work only with test copies of programs and data so they can only make software changes after proper authorization.
- *Operations.* Computer operators are responsible for the day-to-day operations of the computer following the schedule established by the CIO. They also monitor computer consoles for messages about computer efficiency and malfunctions.

  A librarian is responsible for controlling the use of computer programs, transaction files, and other computer records and documentation. The librarian releases them to operators only when authorized. For example, programs and transaction files are released to operators only when a job is scheduled to be processed. Similarly, the librarian releases a test copy to programmers only on approval by senior management. Network administrators also affect IT operations as they are responsible for planning, implementing, and maintaining operations of the network of servers that link users to various applications and data files.

FIGURE 12-2 **Segregation of IT Duties**



- *Data control.* Data input/output control personnel independently verify the quality of input and the reasonableness of output. For organizations that use databases to store information shared by accounting and other functions, database administrators are responsible for the operation and access security of shared databases.

Naturally, the extent of separation of duties depends on the organization's size and complexity. In many small companies, it is not practical to segregate the duties to the extent illustrated in Figure 12-2. For example, some entities acquire accounting systems from third-party vendors or they access applications through the Internet. As a result, they may have few staff dedicated to systems development or the librarian function.

Systems Development Systems development includes:

- Purchasing software or developing in-house software that meets the organization's needs. A key to implementing the right software is to involve a team of both IT and non-IT personnel, including key users of the software and internal auditors. This combination increases the likelihood that information needs as well as software design and implementation concerns are properly addressed. Involving users also results in better acceptance by key users.
- Testing all software to ensure that the new software is compatible with existing hardware and software and determine whether the hardware and software can handle the needed volume of transactions. Whether software is purchased or developed internally, extensive testing of all software with realistic data is critical. Companies typically use one or a combination of the following two test approaches:
  1. **Pilot testing**: A new system is implemented in one part of the organization while other locations continue to rely on the old system.
  2. **Parallel testing**: The old and new systems operate simultaneously in all locations.

Proper documentation of the system is required for all new and modified software. After the software has been successfully tested and documented, it is transferred to the librarian in a controlled manner to ensure only authorized software are ultimately accepted as the authorized version.

Physical and Online Security Physical controls over computers and restrictions to online software and related data files decrease the risk of unauthorized changes to programs and improper use of programs and data files. Security plans should be in writing and monitored. Security controls include both physical controls and online access controls.

- *Physical controls.* Proper physical controls over computer equipment restrict access to hardware, software, and backup data files on magnetic tapes or disks, hard drives, CDs, and external disks. Common examples to physically restrict unauthorized use include keypad entrances, badge-entry systems, security cameras, and security personnel. More sophisticated controls only allow physical and online access after employee fingerprints are read or employee retinas are scanned and matched with an approved database. Other physical controls include monitoring of cooling and humidity to ensure that the equipment functions properly and installing fire-extinguishing equipment to reduce fire damage.
- *Online access controls.* Proper user IDs and passwords control access to software and related data files, reducing the likelihood that unauthorized changes are made to software applications and data files. Separate add-on security software packages, such as firewall and encryption programs, can be installed to improve a system's security. (See page 406 for a description of firewall and encryption programs.)

Backup and Contingency Planning Power failures, fire, excessive heat or humidity, water damage, or even sabotage can have serious consequences to businesses using IT.

TECHNOLOGY GLITCHES BUNGLE FACEBOOK'S IPO

The buildup surrounding Facebook, Inc.'s May 18, 2012, initial public offering set expectations high; however, the opening days of trading led quickly to disappointment. Just days before its debut, the company's CFO decided to boost the number of shares to be offered by 25 percent and increased the opening offer price to $38 per share, believing demand would be high. On opening day, massive demand for the social networking's initial offering actually led to a 30-minute delay in the start of the trading of the stock on the NASDAQ Stock Market. The technology glitch left individual investors puzzled about whether their buy and sell orders had actually been executed when normally those acknowledgements are instantaneous. U.S. regulators, including the SEC, are examining the disruption with some noting that while the mishap is blamed on a computer malfunction, the underlying cause may be programmer failure in designing the systems to be robust enough to handle the volume of orders. NASDAQ has proposed a $40 million fund to repay brokerages that lost money during the botched IPO; however, news of the settlement offer has been met with criticism given that brokerages claim to have lost more than $100 million. Lawsuits are likely to follow.

Sources: 1. John McCrank and Jonathan Spicer, "Facebook Investors Left Guessing after NASDAQ Glitch," Reuters (May 21, 2012) (www.reuters.com); 2. Andrew Tangel, "NASDAQ Offers Brokerages $40 Million for Facebook Glitches," *Los Angeles Times*, (June 6, 2012) (www.articles.latimes.com); 3. Jacob Blunge, "Regulators Probe Role of 'Glitches' in Market Upheavals," NASDAQ News (June 27, 2012) (www.nasdaq.com).

To prevent data loss during power outages, many companies rely on battery backups or on-site generators. For more serious disasters, organizations need detailed backup and contingency plans such as off-site storage of critical software and data files or outsourcing to firms that specialize in secure data storage.

Backup and contingency plans should also identify alternative hardware that can be used to process company data. Companies with small IT systems can purchase replacement computers in an emergency and reprocess their accounting records by using backup copies of software and data files. Larger companies often contract with IT data centers that specialize in providing access to off-site computers and data storage and other IT services for use in the event of an IT disaster.

Hardware Controls **Hardware controls** are built into computer equipment by manufacturers to detect and report equipment failures. Auditors are more concerned with how the client handles errors identified by the hardware controls than with their adequacy. Regardless of the quality of hardware controls, output will be corrected only if the client has provided for handling machine errors.

Application Controls

Application controls are designed for each software application and are intended to help a company satisfy the six transaction-related audit objectives discussed in previous chapters. Although some application controls affect one or only a few transaction-related audit objectives, most controls prevent or detect several types of misstatements. Other application controls concern account balance and presentation and disclosure objectives.

Application controls may be done by computers or client personnel. When they are done by client personnel, they are called **manual controls**. The effectiveness of manual controls depends on both the competence of the people performing the controls and the care they exercise when doing them. For example, when credit department personnel review exception reports that identify credit sales exceeding a customer's authorized credit limit, the auditor may need to evaluate the person's ability to make the assessment and test the accuracy of the exception report. When controls are done by computers, they are called **automated controls**. Because of the nature of computer processing, automated controls, if properly designed, lead to consistent operation of the controls.

Application controls fall into three categories: input, processing, and output. Although the objectives for each category are the same, the procedures for meeting the objectives vary considerably. Let's examine each more closely.

Input Controls **Input controls** are designed to ensure that the information entered into the computer is authorized, accurate, and complete. They are critical because a large

TABLE 12-2	Batch Input Controls	
Control	**Definition**	**Examples**
Financial total	Summary total of field amounts for all records in a batch that represent a meaningful total such as dollars or amounts	The total of dollars of all vendor invoices to be paid
Hash total	Summary total of codes from all records in a batch that do not represent a meaningful total	The total of all vendor account numbers for vendor invoices to be paid
Record count	Summary total of physical records in a batch	The total number of vendor invoices to be processed

portion of errors in IT systems result from data entry errors and, of course, regardless of the quality of information processing, input errors result in output errors. Typical controls developed for manual systems are still important in IT systems, such as:

- Management's authorization of transactions
- Adequate preparation of input source documents
- Competent personnel

Controls specific to IT include:

- Adequately designed input screens with preformatted prompts for transaction information
- Pull-down menu lists of available software options
- Computer-performed validation tests of input accuracy, such as the validation of customer numbers against customer master files
- Online-based input controls for e-commerce applications where external parties, such as customers and suppliers, perform the initial part of the transaction inputting
- Immediate error correction procedures, to provide for early detection and correction of input errors
- Accumulation of errors in an error file for subsequent follow-up by data input personnel

For IT systems that group similar transactions together into batches, the use of financial batch totals, hash totals, and record count totals helps increase the accuracy and completeness of input. Batch input controls are described in Table 12-2. For example, the comparison of a record count calculated before data entry of the number of vendor invoices to be entered to the number of vendor invoices processed by the system would help determine if any invoices were omitted or entered more than once during data entry.

Processing Controls **Processing controls** prevent and detect errors while transaction data are processed. General controls, especially controls related to systems development and security, provide essential control for minimizing errors. Specific application processing controls are often programmed into software to prevent, detect, and correct processing errors. Examples of processing controls are illustrated in Table 12-3 (p. 398).

Output Controls **Output controls** focus on detecting errors after processing is completed, rather than on preventing errors. The most important output control is review of the data for reasonableness by someone knowledgeable about the output. Users can often identify errors because they know the approximate correct amounts. Several common controls for detecting errors in outputs include:

- Reconcile computer-produced output to manual control totals
- Compare the number of units processed to the number of units submitted for processing
- Compare a sample of transaction output to input source documents
- Verify dates and times of processing to identify any out-of-sequence processing

TABLE 12-3 Processing Controls

Type of Processing Control	Description	Example
Validation test	Ensures that a particular type of transaction is appropriate for processing	Does the transaction code for the processing of a recent purchase match predetermined inventory codes?
Sequence test	Determines that data submitted for processing are in the correct order	Has the file of payroll input transactions been sorted in departmental order before processing?
Arithmetic accuracy test	Checks the accuracy of processed data	Does the sum of net pay plus withholdings equal gross pay for the entire payroll?
Data reasonableness test	Determines whether data exceed prespecified amounts	Does employee's gross pay exceed 60 hours or $1,999 for the week?
Completeness test	Determines that every field in a record has been completed	Are employee number, name, number of regular hours, number of overtime hours, department number, etc., included for each employee?

For sensitive computer output, such as payroll checks, control can be improved by requiring employees to present employee identification before they receive their checks or by requiring the use of direct deposit into the employees' pre-approved bank accounts. Also, access to sensitive output stored in electronic files or transmitted across networks, including the Internet, is often restricted by requiring passwords, user IDs, and encryption techniques.

IMPACT OF INFORMATION TECHNOLOGY ON THE AUDIT PROCESS

OBJECTIVE 12-4

Describe how general controls affect the auditor's testing of application controls.

Because auditors are responsible for obtaining an understanding of internal control, they must be knowledgeable about general and application controls, whether the client's use of IT is simple or complex. Knowledge of general controls increases the auditor's ability to assess and rely on effective application controls to reduce control risk for related audit objectives. For public company auditors who must issue an opinion on internal control over financial reporting, knowledge of both general and application IT controls is essential.

Effect of General Controls on Control Risk

Auditors should evaluate the effectiveness of general controls before evaluating application controls. As illustrated in Figure 12-1 (p. 393), general controls have a pervasive effect on the effectiveness of application controls, so auditors should first evaluate those controls before concluding whether application controls are effective.

Effects of General Controls on System-wide Applications Ineffective general controls create the potential for material misstatements across all system applications, regardless of the quality of individual application controls. For example, if IT duties are inadequately separated such that computer operators also work as programmers and have access to computer programs and files, the auditor should be concerned about the potential for unauthorized software program or data file changes that might lead to fictitious transactions or unauthorized data and omissions in accounts such as sales, purchases, and salaries. Similarly, if the auditor observes that data files are inadequately safeguarded, the auditor may conclude that there is a significant risk of loss of data for every class of transaction that relies on that data to conduct application controls. In this situation, the auditor may need to expand audit testing in several areas such as cash receipts, cash disbursements, and sales to satisfy the completeness objective.

On the other hand, if general controls are effective, the auditor may be able to place greater reliance on application controls whose functionality is dependent on IT. Auditors can then test those application controls for operating effectiveness and rely on the results to reduce substantive testing.

Effect of General Controls on Software Changes Client changes to application software affect the auditor's reliance on automated controls. When the client changes the software, the auditor must evaluate whether additional testing is needed. If general controls are effective, the auditor can easily identify when software changes are made. But in companies where general controls are deficient, it may be difficult to identify software changes. As a result, auditors must consider doing tests of application controls that depend on IT throughout the current year audit.

Obtaining an Understanding of Client General Controls Auditors typically obtain information about general and application controls through the following ways:

- Interviews with IT personnel and key users
- Examination of system documentation such as flowcharts, user manuals, program change requests, and system testing results
- Reviews of detailed questionnaires completed by IT staff

In most cases, auditors should use several of these approaches because each offers different information. For example, interviews with the chief information officer and systems analysts provide useful information about the operation of the entire IT function, the extent of software development and hardware changes made to accounting application software, and an overview of any planned changes. Reviews of program change requests and system test results are useful to identify program changes in application software. Questionnaires help auditors identify specific internal controls.

Effect of IT Controls on Control Risk and Substantive Tests

The following discussion of control risk may seem familiar because auditors link IT controls to audit objectives following the same principles and approaches we covered in Chapter 10. You may recall that auditors relate controls and deficiencies in internal control to specific audit objectives. Based on those controls and deficiencies, the auditor assesses control risk for each related audit objective. The same approach is used when controls are done by IT.

Relating IT Controls to Transaction-Related Audit Objectives Auditors do not normally link controls and deficiencies in general controls to specific transaction-related audit objectives. Because general controls affect audit objectives in several cycles, if the general controls are ineffective, the auditor's ability to rely on IT-related application controls to reduce control risk in all cycles is reduced. Conversely, if general controls are effective, it increases the auditor's ability to rely on IT-based application controls for all cycles.

Auditors can use a control risk matrix, much like the one we discussed in Chapter 10, to help them identify both manual and automated application controls and control deficiencies for each related audit objective. For example, to prevent payments to fictitious employees, a computer comparison of inputted employee identification numbers with the employee master file might reduce control risk for the occurrence objective for payroll transactions. Auditors can identify manual and automated controls at the same time or separately, but they should not identify deficiencies or assess control risk until both types of controls have been identified.

Effect of IT Controls on Substantive Testing After identifying specific IT-based application controls that can be used to reduce control risk, auditors can reduce substantive testing. The systematic nature of automated application controls may allow auditors to reduce sample sizes used to test those controls in both an audit of financial statements and an audit of internal control over financial reporting. Auditors may also be able to rely on prior year testing of automated controls as described in

Chapter 10 when general controls are effective and the automated control has not been changed since testing by the auditor. Auditors often use their own software to test the controls. These factors, when combined, often lead to extremely effective and efficient audits.

The impact of general controls and application controls on audits is likely to vary depending on the level of complexity in the IT environment. We discuss that next.

Auditing in Less Complex IT Environments

Many organizations design and use accounting software to process business transactions so that source documents are retrievable in a readable form and can be traced easily through the accounting system to output. Such systems retain many of the traditional source documents such as customer purchase orders, shipping and receiving records, and sales and vendor invoices. The software also produces printed journals and ledgers that allow the auditor to trace transactions through the accounting records. Internal controls in these systems often include client personnel comparing computer-produced records with source documents.

In these situations, the use of IT does not significantly impact the audit trail. Typically, auditors obtain an understanding of internal control and do tests of controls, substantive tests of transactions, and account balance verification procedures in the same way they do when testing manual accounting systems. The auditor is still responsible for obtaining an understanding of general and application computer controls because such knowledge is useful in identifying risks that may affect the financial statements. But, the auditor typically does not test automated controls. This approach to auditing is often called **auditing around the computer** because the auditor is not using automated controls to reduce assessed control risk. Instead, the auditor uses manual controls to support a reduced control risk assessment.

Auditors in smaller companies often audit around the computer when general controls are less effective than in more complex IT environments. Often, smaller companies lack dedicated IT personnel, or they rely on periodic involvement of IT consultants to assist in installing and maintaining hardware and software. The responsibility of the IT function is often assigned to user departments, such as the accounting department, where the hardware physically resides. Auditing around the computer is effective because these systems often produce sufficient audit trails to permit auditors to compare source documents such as vendors' and sales invoices to output, and there may be manual controls over the input and output processes that operate effectively to prevent and detect material financial statement misstatements.

Many organizations with non-complex IT environments often heavily rely on desktop and networked servers to do accounting system functions. The use of computers creates the following unique audit considerations:

- *Limited reliance on automated controls.* Even in less sophisticated IT environments, automated controls can often be relied on. For example, software programs can be loaded on the computer's hard drive in a format that does not permit changes by client personnel, making the risk of unauthorized changes in the software low. Before relying on controls built into that software, auditors must be confident that the software vendor has a reputation for quality.
- *Access to master files.* When clients use desktop computers and servers, auditors should be concerned about access to master files by unauthorized people. Appropriate separation of duties between personnel with access to master files and responsibilities for processing is critical. Regular owner-manager review of transaction output improves internal control.
- *Risk of computer viruses.* Computer viruses can lead to the loss of data and programs. Certain viruses can damage electronic files or shut down an entire network of computers. Regularly updated virus protection software that screens for virus infections improves controls.

TABLE 12-4 Examples of Auditing Around and Through the Computer

Internal Control	Auditing Around the Computer Approach	Auditing Through the Computer Approach
Credit is approved for sales on account.	Select a sample of sales transactions from the sales journal and obtain the related customer sales order to determine that the credit manager's initials are present, indicating approval of sales on account.	Obtain a copy of the client's sales application program and related credit limit master file and process a test data sample of sales transactions to determine whether the application software properly rejects those test sales transactions that exceed the customer's credit limit amount and accepts all other transactions.
Payroll is processed only for individuals currently employed.	Select a sample of payroll disbursements from the payroll journal and verify by reviewing human resource department files that the payee is currently employed.	Create a test data file of valid and invalid employee ID numbers and process that file using a controlled copy of the client's payroll application program to determine that all invalid employee ID numbers are rejected and that all valid employee ID numbers are accepted.
Column totals for the cash disbursements journal are subtotaled automatically by the computer.	Obtain a printout of the cash disbursements journal and manually foot each column to verify the accuracy of the printed column totals.	Obtain an electronic copy of the cash disbursements journal transactions and use generalized audit software to verify the accuracy of the column totals.

A public company's use of desktop computers in the financial reporting process may affect the audit of internal control over financial reporting. If the auditor concludes that general controls are ineffective, the auditor's tests of automated application controls may need to be increased. The auditor must also consider the implications of the lack of effective general controls on the opinion about the operating effectiveness of internal control over financial reporting.

Auditing in More Complex IT Environments

OBJECTIVE 12-5

Use test data, parallel simulation, and embedded audit module approaches to test automated controls.

As organizations expand their use of IT, internal controls are often embedded in applications that are available only electronically. When traditional source documents such as invoices, purchase orders, billing records, and accounting records such as sales journals, inventory listings, and accounts receivable subsidiary records exist only electronically, auditors must change their approach to auditing. This approach is often called **auditing through the computer**. Table 12-4 illustrates some differences between auditing around the computer and auditing through the computer.

Auditors use three categories of testing approaches when auditing through the computer: test data approach, parallel simulation, and embedded audit module approach.

Test Data Approach

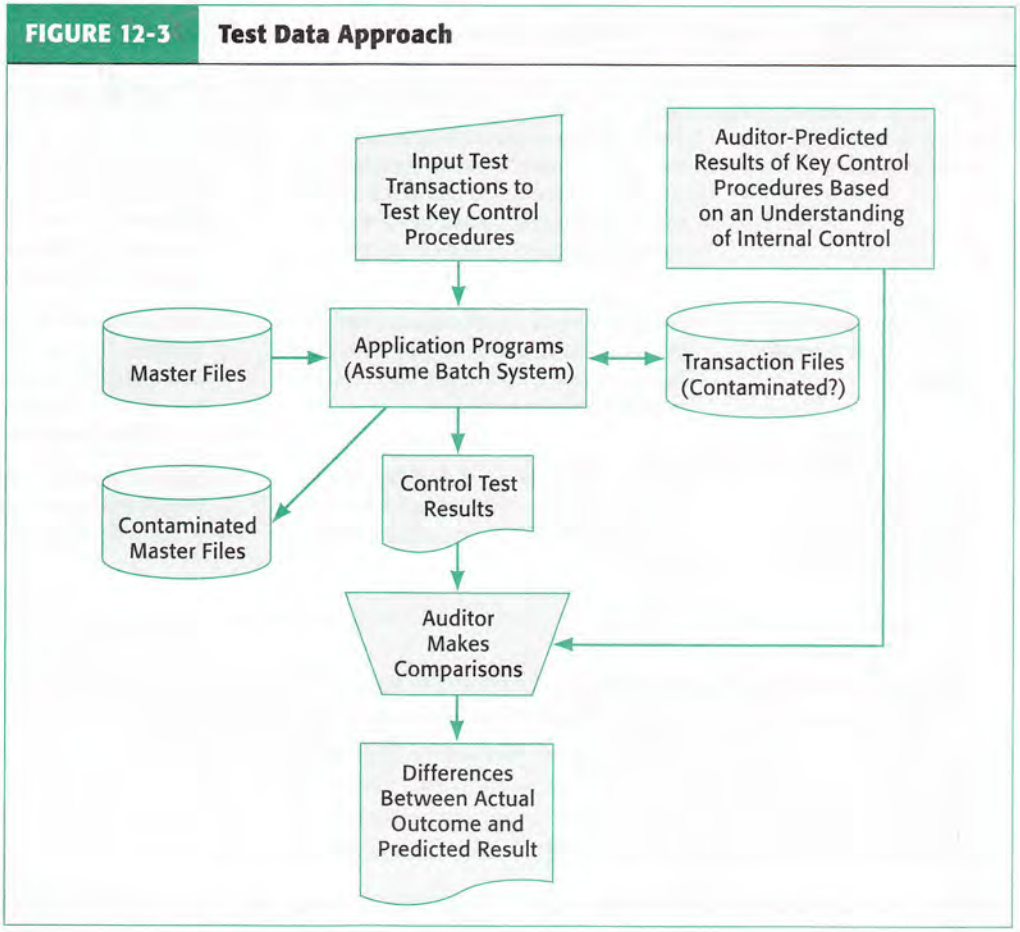
In the **test data approach**, auditors process their own test data using the client's computer system and application program to determine whether the automated controls correctly process the test data. Auditors design the test data to include transactions that the client's system should either accept or reject. After the test data are processed on the client's system, auditors compare the actual output to the expected output to assess the effectiveness of the application program's automated controls. Figure 12-3 (p. 402) illustrates the use of the test data approach.

When using the test data approach, auditors have three main considerations:

1. *Test data should include all relevant conditions that the auditor wants tested.* Auditors should design test data to test all key computer-based controls and include realistic data that are likely to be a part of the client's normal processing, including both valid and invalid transactions.

   For example, assume the client's payroll application contains a limit check that disallows a payroll transaction that exceeds 80 hours per week. To test this control, the auditor can prepare payroll transactions with 79, 80, and 81 hours for each sampled week and process them through the client's system in a manner shown in Figure 12-3. If the limit check control is operating effectively,

FIGURE 12-3 **Test Data Approach**



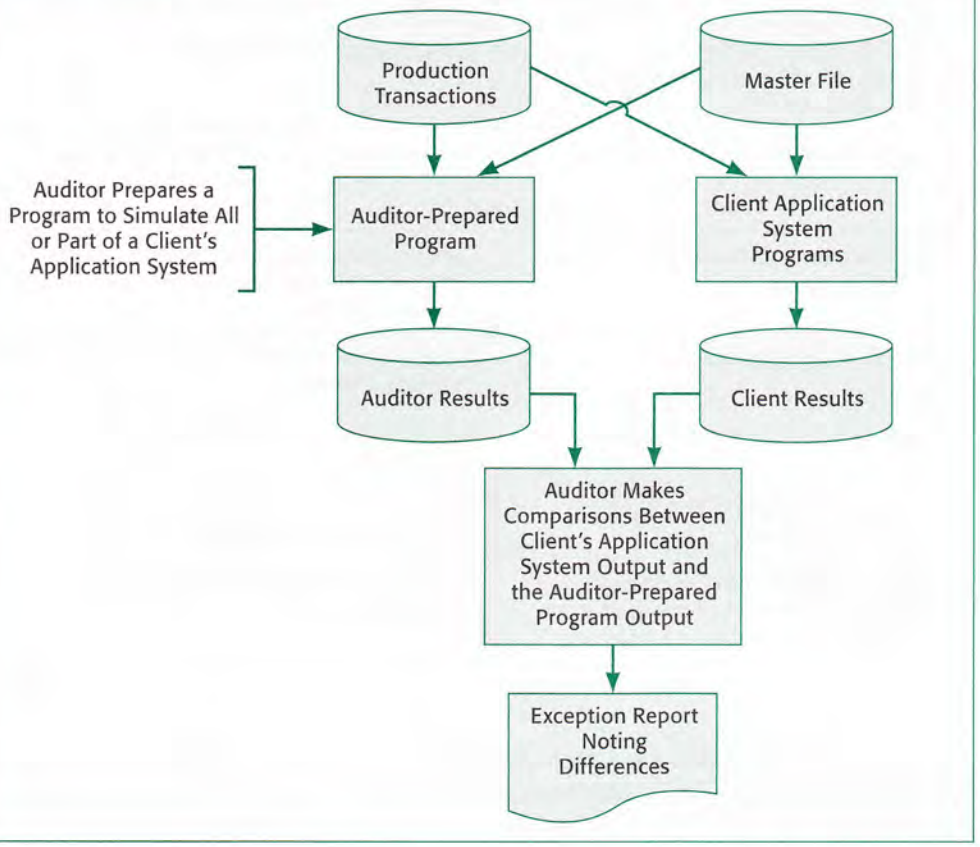
the client's system should reject the transaction for 81 hours, and the client's error listing should report the 81-hour transaction error.

2. *Application programs tested by auditors' test data must be the same as those the client used throughout the year.* One approach is to run the test data on a surprise basis, possibly at random times throughout the year, even though doing so is costly and time consuming. Another method is to rely on the client's general controls in the librarian and systems development functions to ensure that the program tested is the one used in normal processing.
3. *Test data must be eliminated from the client's records.* If auditors process test data while the client is processing its own transactions, auditors must eliminate the test data in the client's master files after the tests are completed to prevent master files and transaction files from being permanently contaminated by the auditor's testing. Auditors can do this by developing and processing data that reverses the effect of the test data.

Because of the complexities of many clients' application software programs, auditors who use the test data approach often obtain assistance from a computer audit specialist. Many larger CPA firms have staff dedicated to assisting in testing client application controls.

Parallel Simulation Auditors often use auditor-controlled software to do the same operations that the client's software does, using the same data files. The purpose is to determine the effectiveness of automated controls and to obtain evidence about electronic account balances. This testing approach is called **parallel simulation testing**. Figure 12-4 shows a typical parallel simulation. Whether testing controls or ending balances, the auditor compares the output from the auditor's software to output from

FIGURE 12-4 Parallel Simulation



the client's system to test the effectiveness of the client's software and to determine if the client's balance is correct. A variety of software is available to assist auditors.

Auditors commonly do parallel simulation testing using **generalized audit software (GAS)**, which are programs designed specifically for auditing purposes. Commercially available audit software, such as ACL or IDEA, can be easily operated on auditors' desktop or laptop computers. Auditors obtain copies of machine-readable client databases or master files and use the generalized audit software to do a variety of tests of the client's electronic data. Instead of GAS, some auditors use spreadsheet software to do simple parallel simulation tests. Others develop their own customized audit software.

Generalized audit software provides three advantages: it is relatively easy to train audit staff in its use, even if they have had little audit-related IT training, the software can be applied to a wide variety of clients with minimal customization, and it has the ability to do audit tests much faster and in more detail than using traditional manual procedures. Table 12-5 (p. 404) includes some of the common uses of generalized audit software. Two are examined in detail:

1. *Generalized audit software is used to test automated controls.* An auditor obtains copies of a client's customer credit limit master file and a customer order file, and then instructs the auditor's computer to list transactions that exceed the customer's authorized credit limit. The auditor then compares the audit output to the client's list of customer orders that were rejected for exceeding authorized credit limits.
2. *Generalized audit software is used to verify the client's account balances.* An auditor can use the software to sum the master file of customer accounts receivable to determine whether the total agrees with the general ledger balance.

TABLE 12-5 Common Uses of Generalized Audit Software

Uses	Description	Examples
Verify extensions and footings	Verify the accuracy of the client's computations by calculating information independently	Foot accounts receivable trial balance
Examine records for quality, completeness, consistency, and correctness	Scan all records using specified criteria	Review payroll files for terminated employees
Compare data on separate files	Determine that information in two or more data files agrees	Compare changes in accounts receivable balances between two dates using sales and cash receipts in transaction files
Summarize or resequence data and do analyses	Change or aggregate data	Resequence inventory items by location to facilitate physical observation
Select audit samples	Select samples from machine-readable data	Randomly select accounts receivable for confirmation
Print confirmation requests	Print data for sample items selected for confirmation testing	Print customer name, address, and account balance information from master files
Compare data obtained through other audit procedures with company records	Compare machine-readable data with audit evidence gathered manually, which is converted to machine-readable form	Compare confirmation responses with accounts receivable master files

Embedded Audit Module Approach When using the **embedded audit module approach**, auditors insert an audit module in the client's application system to identify specific types of transactions. For example, auditors might use an embedded module to identify all purchases exceeding $25,000 for follow-up with more detailed examination for the occurrence and accuracy transaction-related audit objectives. In some cases, auditors later copy the identified transactions to a separate data file and then process those transactions using parallel simulation to duplicate the function done by the client's system. The auditor then compares the client's output with the auditor's output. Discrepancies are printed on an exception report for auditor follow-up.

The embedded audit module approach allows auditors to continuously audit transactions by identifying actual transactions processed by the client as compared to test data and parallel simulation approaches, which only allow intermittent testing. Internal audit may also find this technique useful.

Although auditors may use one or any combination of testing approaches, they typically use:

- Test data to do tests of controls and substantive tests of transactions
- Parallel simulation for substantive testing, such as recalculating transaction amounts and footing master file subsidiary records of account balances
- Embedded audit modules to identify unusual transactions for substantive testing

ISSUES FOR DIFFERENT IT ENVIRONMENTS

OBJECTIVE 12-6

Identify issues for e-commerce systems and other specialized IT systems.

So far, we have addressed the effect of IT on the audit process for organizations that centralize the IT function. Although all organizations need good general controls regardless of the structure of their IT function, some general control issues vary depending on the IT environment. Next, we'll examine IT issues for clients who use networks, database management systems, e-commerce systems, and outsourced computer service centers.

Issues for Network Environments

The use of networks that link equipment such as desktops, midrange computers, mainframes, workstations, servers, and printers is common for most businesses. **Local area networks (LANs)** link equipment within a single or small cluster of buildings, and are used only within a company. LANs are often used to transfer data and programs from one computer or workstation using network system software that allow all of the devices to function together. **Wide area networks (WANs)** link equipment in larger geographic regions, including global operations.

In networks, application software and data files used to process transactions are included on several computers that are linked together. Access to the application from desktop computers or workstations is managed by network server software. Even small companies can have several computer servers linked together on a network, while larger companies may have hundreds of servers in dozens of locations networked together.

Most of the general controls discussed in this chapter apply to large client networks, because IT support and user involvement is centralized. For other companies, networks present control issues that the auditor must consider in planning the audit. For example, auditors often increase control risk when companies have networks consisting of servers located throughout various parts of the organization because decentralized network operations often lack security and management supervision over the various connected servers.

It is common for networks to consist of various combinations of equipment and procedures, which may not have standard security options. Lack of equipment compatibility across a network may occur when responsibility for purchasing equipment and software, maintenance, administration, and physical security resides with key user groups rather than with a centralized IT function. Sometimes network security may be compromised when networks consist of equipment with incompatible security features.

When clients have accounting applications processed in a network, the auditor should learn about the network configuration, including the location of computer servers and workstations linked to one another, network software used to manage the system, and controls over access and changes to application programs and data files located on servers. This knowledge may have implications for the auditor's control risk assessment when planning the audit of the financial statements and when testing controls in an audit of internal control over financial reporting.

Issues for Database Management Systems

Database management systems allow clients to create databases that include information that can be shared across multiple applications. In nondatabase systems, each application has its own data file, whereas in database management systems, many applications share files. Clients implement database management systems to reduce data redundancy, improve control over data, and provide better information for decision making by integrating information throughout functions and departments. For example, customer data, such as the customer's name and address, can be shared in the sales, credit, accounting, marketing, and shipping functions, resulting in consistent information for all users and significant cost reductions. Companies often integrate database management systems within the entire organization using **enterprise resource planning (ERP) systems** that integrate numerous aspects of an organization's activities into one accounting information system. ERP systems share data across accounting and non-accounting business functions of the organization. For example, customer order data may be used by accounting to record a sale, by production to meet increased production demand, by purchasing to order additional raw materials, and by human resources to arrange labor schedules.

Controls often improve when data are centralized in a database management system by eliminating duplicate data files. However, database management systems also can create internal control risks. Risks increase when multiple users, including individuals outside of accounting, can access and update data files. To counter the risks of unauthorized, inaccurate, and incomplete data files, companies must implement

proper database administration and access controls. With the centralization of data in a single system, they must also ensure proper backup of data on a regular basis.

Auditors of clients using database management systems should understand the clients' planning, organization, and policies and procedures to determine how well the systems are managed. This understanding may affect the auditor's assessment of control risk and the auditor's opinion about the operating effectiveness of internal control over financial reporting.

Issues for e-Commerce Systems

Companies using e-commerce systems to transact business electronically link their internal accounting systems to external parties' systems, such as customers and suppliers. As a result, a company's risks depend in part on how well its e-commerce partners identify and manage risks in their own IT systems. To manage these interdependency risks, companies must ensure that their business partners manage IT system risks before conducting business with them electronically. Some of the assurance services discussed in Chapter 1, such as *SysTrust*, provide objective information about the reliability of a business partner's IT system.

The use of e-commerce systems also exposes sensitive company data, programs, and hardware to potential interception or sabotage by external parties. To limit these exposures, companies use firewalls, encryption techniques, and digital signatures.

A **firewall** protects data, programs, and other IT resources from unauthorized external users accessing the system through networks, such as the Internet. A firewall is a system of hardware and software that monitors and controls the flow of e-commerce communications by channeling all network connections through controls that verify external users, grant accesses to authorized users, deny access to unauthorized users, and direct authorized users to requested programs or data.

Encryption techniques protect the security of electronic communication when information is transmitted and when it is stored. Computerized encryption changes a standard message or data file into one that is coded (encrypted), requiring the receiver of the electronic message or user of the encrypted data file to use a decryption program to decode the message or data. A public key encryption technique is often used, where one key (the public key) is used for encoding the message and another key (the private key) is used to decode the message. The public key is distributed to all approved users of the e-commerce system. The private key is distributed only to internal users with the authority to decode the message.

To authenticate the validity of a trading partner conducting business electronically, companies may rely on external certification authorities who verify the source of the public key by using **digital signatures**. A trusted certification authority issues a digital certificate to individuals and companies engaging in e-commerce. The digital signature contains the holder's name and its public key. It also contains the name of the certification authority and the certificate's expiration date and other specified information. To guarantee integrity and authenticity, each signature is digitally signed by the private key maintained by the certification authority.

Auditors should understand the nature of firewall and encryption controls to ensure that they are properly implemented and monitored. An inadequate firewall may increase the likelihood of unauthorized changes to software and data. Thus, the auditor may need to test controls surrounding the use of the firewall to ensure that automated application controls used to support assessed control risk below the maximum have not been changed without the auditor's knowledge. Similarly, auditors may need to understand and test encryption controls to satisfy transaction and account balance objectives. Failure to adequately encrypt transaction or account data may result in changes in amounts supporting transactions or account balances.

Issues When Clients Outsource IT

Many clients outsource some or all of their IT needs to an independent computer **service center**, including **application service providers (ASPs)** and **cloud computing environments**, rather than maintain an internal IT center. Smaller companies often

CLOUD COMPUTING

"Cloud computing" is a computer resource deployment and procurement model that enables an organization to obtain IT resources and applications from any location via an Internet connection. Depending on the arrangement, all or parts of an entity's IT hardware, software, and data might reside in an IT service center shared with other organizations and managed by a third-party vendor. The name comes from the use of a cloud-shaped symbol in systems diagrams to represent complex IT infrastructures.

Companies including Amazon, IBM, Microsoft, Google, Cisco, and Red Hat have emerged as heavyweights in the cloud computing field. Cloud computing helps users spare the expense of acquiring their own servers, storage, and backup systems, hiring and retaining IT professionals to keep the systems running, and other high-cost IT support activities.

Instead of running their own systems, users pay vendors to host the application and store related data. Cloud computing solutions are appearing in a number of business process areas, including customer relationship management, human resources, payroll, billing, and help desk management.

Relying on cloud computing solutions does come with risks that need to be managed. Data is transmitted and then stored in environments not directly controlled by users and another entity hosts the software. As a result, the underlying code for the software is basically the same for all users, which restricts user customization. And, when systems are down, user access depends on restoration by the vendor. Backup options may also not be available for users since their decision to contract with a cloud computing vendor is often driven by a desire to avoid costs of buying servers and hardware to host the software.

Massive scale cloud computing environments are emerging as well. IBM's "Blue Cloud," a series of cloud computing offerings, allows corporate data centers to operate more like the Internet by enabling computing across widely distributed, global highly powerful computers.

Sources: 1. *Enterprise Risk Management for Cloud Computing*, Committee of Sponsoring Organizations of the Treadway Commission, New York, 2012 (www.coso.org); 2. Jon Brodkin, "Amazon and IBM are the 'Cloud Champions', Report Says," *CIO Magazine*, June 15, 2010; 3. Alan Cohen, "Cloud Computing: Is it Safe?," *Law.com*, October 31, 2008 (www.law.com); 4. IBM, Inc., "IBM Introduces Ready-to-Use Cloud Computing" (www.ibm.com), November 15, 2007.

outsource their payroll function because payroll is reasonably standard from company to company, and many reliable providers of payroll services are available. Companies also outsource their e-commerce systems to external Web site service providers, including those that offer cloud computing services as described in the vignette above. Like all outsourcing decisions, companies decide whether to outsource IT on a cost-benefit basis.

When outsourcing to a computer service center, the client submits input data, which the service center processes for a fee, and returns the agreed-upon output and the original input. For payroll, the company submits data from time cards, pay rates, and W-4s to the service center. The service center returns payroll checks, journals, and input data each week and W-2s at the end of each year. The service center is responsible for designing the computer system and providing adequate controls to ensure that the processing is reliable.

Understanding Internal Controls in Outsourced Systems The auditor faces a difficulty when obtaining an understanding of the client's internal controls in these situations because many of the controls reside at the service center, and the auditor cannot assume that the controls are adequate simply because it is an independent enterprise. Auditing standards require the auditor to consider the need to obtain an understanding and test the service center's controls if the service center application involves processing significant financial data. For example, many of the controls for payroll transaction-related audit objectives reside within the software program maintained and supported by the payroll services company, not the audit client.

When obtaining an understanding and testing the service center's controls, the auditor should use the same criteria that was used in evaluating a client's internal controls. The depth of the auditor's understanding depends on the complexity of the system and the extent to which the control is relied upon to reduce control risk. The depth of understanding also depends on the extent to which key controls over transaction-related audit objectives reside at the service center for audits of internal

control for public companies. If the auditor concludes that active involvement at the service center is the only way to conduct the audit, it may be necessary to obtain an understanding of internal controls at the service center and test controls using test data and other tests of controls.

Reliance on Service Center Auditors In recent years, it has become increasingly common for the service center to engage a CPA firm to obtain an understanding and test internal controls of the service center and issue a report for use by all customers and their independent auditors. The purpose of this independent assessment is to provide service center customers reasonable assurance about the adequacy of the service center's general and application controls and to eliminate the need for redundant audits by customers' auditors. If the service center has many customers and each requires an understanding of the service center's internal control by its own independent auditor, the inconvenience and cost to the service center can be substantial.

Attestation standards provide guidance to auditors who issue reports on the internal control of service organizations (*service auditors*), while auditing standards provide guidance to auditors of user organizations (*user auditors*) that rely on the service auditor's report. Service auditors may issue two types of reports:

- Report on management's description of a service organization's system and the suitability of the design of controls (referred to as a Type 1 report)
- Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls (referred to as a Type 2 report)

A Type 1 report helps auditors obtain an understanding of internal control to plan the audit. However, auditors also require evidence about the operating effectiveness of controls to assess control risk, especially when auditing internal control over financial reporting for public companies. This evidence can:

- Be based on the service auditor's Type 2 report that includes tests of the operating effectiveness of controls
- Come from tests of the user organization's controls over the activities of the service organization
- Be created when the user auditor does appropriate tests at the service organization

If the user auditor decides to rely on the service auditor's report, appropriate inquiries should be made about the service auditor's reputation. Auditing standards state that the user auditor should not make reference to the report of the service auditor in the opinion on the user organization's financial statements.

SUMMARY

This chapter studied how IT influences the audit process. Even when a client's use of IT leads to improved internal control, the use of IT-based accounting systems introduces new risks typically not associated with traditional manual systems. Well-managed companies recognize these risks and respond by implementing effective general and application controls in the IT system to reduce the impact of these risks on financial reporting. The auditor must be knowledgeable about these risks and obtain an understanding of the client's general and application controls to effectively plan an audit. Knowledge about general controls provides a basis for the auditor to rely on automated application controls and may reduce the extent of tests of key automated controls in audits of financial statements and internal controls. Some of the auditor's tests of controls can be done by the computer, often as a way to achieve more effective and efficient audits. Reliance on general and application controls to reduce control risk is likely to change when clients use desktop computers, networks, database management systems, e-commerce systems, and outsourced computer service centers instead of centralized IT systems.

ESSENTIAL TERMS

Application controls—controls typically at the business process level that apply to processing transactions, such as the inputting, processing, and outputting of sales or cash receipts

Application service providers (ASPs)—a third-party entity that manages and supplies software applications or software-related services to customers through the Internet

Auditing around the computer—auditing without relying on and testing automated controls embedded in computer application programs, which is acceptable when the auditor has access to readable source documents that can be reconciled to detailed listings of output or when sufficient nonautomated controls exist

Auditing through the computer—auditing by testing automated internal controls and account balances electronically, generally because effective general controls exist

Automated controls—application controls done by the computer

Cloud computing environments—a computer resource deployment and procurement model that enables an organization to obtain IT resources and applications at an IT service center shared with other organizations from any location via an Internet connection

Database management systems—hardware and software systems that allow clients to establish and maintain databases shared by multiple applications

Digital signatures—electronic certificates that are used to authenticate the validity of individuals and companies conducting business electronically

Embedded audit module approach—a method of auditing transactions processed by IT whereby the auditor embeds a module in the client's application software to identify transactions with characteristics that are of interest to the auditor; the auditor is then able to analyze these transactions on a real-time, continuous basis as client transactions are processed

Encryption techniques—computer programs that change a standard message or data file into one that is coded, then decoded using a decryption program

Enterprise resource planning (ERP) systems—systems that integrate numerous aspects of an organization's activities into one accounting information system

Firewall—a system of hardware and software that monitors and controls the flow of e-commerce communications by channeling all network connections through a control gateway

General controls—controls that relate to all parts of the IT function and affect many different software applications

Generalized audit software (GAS)—computer programs used by auditors that provide data retrieval, data manipulation, and reporting capabilities specifically oriented to the needs of auditors

Hardware controls—controls built into the computer equipment by the manufacturer to detect and report equipment failure

Input controls—controls designed by an organization to ensure that the information to be processed by the computer is authorized, accurate, and complete

Local area networks (LANs)—networks that connect computer equipment, data files, software, and peripheral equipment within a local area, such as a single building or a small cluster of buildings, for intracompany use

Manual controls—application controls done by people

Output controls—controls designed to ensure that computer-generated data are valid, accurate, complete, and distributed only to authorized people

Parallel simulation testing—an audit testing approach that involves the auditor's use of audit software, either purchased or programmed by the auditor, to replicate some part of a client's application system

Parallel testing—a company's computer testing approach that involves operating the old and new systems simultaneously

Pilot testing—a company's computer testing approach that involves imple-

menting a new system in just one part of the organization, while maintaining the old system at other locations

Processing controls—controls designed to ensure that data input into the system are accurately and completely processed

Service center—an organization that provides IT services for companies on an outsourcing basis

Test data approach—a method of auditing an IT system that uses the auditor's test data to determine whether the client's computer program correctly processes valid and invalid transactions

Wide area networks (WANs)—networks that connect computer equipment, databases, software, and peripheral equipment that reside in many geographic locations, such as client offices located around the world

REVIEW QUESTIONS

12-1 (Objective 12-1) Explain how client internal controls can be improved through the proper installation of IT.

12-2 (Objective 12-2) Identify risks for accounting systems that rely heavily on IT functions.

12-3 (Objective 12-2) Define what is meant by an audit trail and explain how it can be affected by the client's integration of IT.

12-4 (Objective 12-2) Distinguish between random error resulting from manual processing and systematic error resulting from IT processing and give an example of each category of error.

12-5 (Objective 12-2) Identify the traditionally segregated duties in noncomplex IT systems and explain how increases in the complexity of the IT function affect that separation.

12-6 (Objective 12-3) Distinguish between general controls and application controls and give two examples of each.

12-7 (Objective 12-3) Identify the typical duties within an IT function and describe how those duties should be segregated among IT personnel.

12-8 (Objective 12-4) Explain how the effectiveness of general controls affects the auditor's tests of automated application controls, including the auditor's ability to rely on tests done in prior audits.

12-9 (Objective 12-4) Explain the relationship between application controls and transaction-related audit objectives.

12-10 (Objective 12-4) Explain what is meant by auditing around the computer, and describe what must be present for this approach to be effective in the audit of a client that uses IT to process accounting information.

12-11 (Objective 12-5) Explain what is meant by the test data approach. What are the major difficulties with using this approach? Define parallel simulation with audit software and provide an example of how it can be used to test a client's payroll system.

12-12 (Objective 12-6) Describe risks that are associated with purchasing software to be installed on desktop computer hard drives. What precautions can clients take to reduce those risks?

12-13 (Objective 12-6) Compare the risks associated with network systems to those associated with centralized IT functions.

12-14 (Objective 12-6) How does the use of a database management system affect risks?

12-15 (Objective 12-6) An audit client is in the process of creating an online Web-based sales ordering system for customers to purchase products using personal credit cards for payment. Identify three risks related to an online sales system that management should consider. For each risk, identify an internal control that could be implemented to reduce that risk.

12-16 (Objective 12-6) Your client has outsourced the majority of the accounting information system to a third-party data center. What impact would that have on your audit of the financial statements?

MULTIPLE CHOICE QUESTIONS FROM CPA EXAMINATIONS

12-17 (Objectives 12-1, 12-4) The following questions concern the characteristics of IT systems. Choose the best response.

a. Which of the following is an advantage of a computer-based system for transaction processing over a manual system? A computer-based system
   (1) does not require as stringent a set of internal controls.
   (2) will produce a more accurate set of financial statements.
   (3) will be more efficient in generating financial statements.
   (4) eliminates the need to reconcile control accounts and subsidiary ledgers.

b. Which of the following is an example of an application control?
   (1) The client uses access security software to limit access to each of the accounting applications.
   (2) Employees are assigned a user ID and password that must be changed every quarter.
   (3) The sales system automatically computes the total sale amount and posts the total to the sales journal master file.
   (4) Systems programmers are restricted from doing applications programming functions.

c. Which of the following is generally *not* considered a category of IT general controls?
   (1) Controls that determine whether a vendor number matches the pre-approved vendors in the vendor master file.
   (2) Controls that restrict system-wide access to programs and data.
   (3) Controls that oversee the acquisition of application software.
   (4) Controls that oversee the day-to-day operation of IT applications.

d. As general IT controls weaken, the auditor is most likely to
   (1) reduce testing of automated application controls done by the computer.
   (2) increase testing of general IT controls to conclude whether they are operating effectively.
   (3) expand testing of automated application controls used to reduce control risk to cover greater portions of the fiscal year under audit.
   (4) ignore obtaining knowledge about the design of general IT controls and whether they have been implemented.

12-18 (Objectives 12-2, 12-4) The following questions concern auditing complex IT systems. Choose the best response.

a. Which of the following client IT systems generally can be audited without examining or directly testing the computer programs of the system?
   (1) A system that performs relatively uncomplicated processes and produces detailed output.
   (2) A system that affects a number of essential master files and produces limited output.
   (3) A system that updates a few essential master files and produces no printed output other than final balances.
   (4) A system that does relatively complicated processing and produces little detailed output.

b. Which of the following procedures most likely could prevent IT personnel from modifying programs to bypass automated controls?
   (1) Periodic management review of computer utilization reports and systems documentation.
   (2) Segregation of duties within IT for computer programming and computer operations.
   (3) Participation of user department personnel in designing and approving new systems.
   (4) Physical security of IT facilities in limiting access to IT equipment.

c. Before processing, the system validates the sequence of items to identify any breaks in sequence of input documents. This automated control is primarily designed to ensure the
(1) accuracy of input.
(2) authorization of data entry.
(3) completeness of input.
(4) restriction of duplicate entries.

d. An auditor will use the test data approach to obtain certain assurances with respect to the
(1) input data.
(2) machine capacity.
(3) procedures contained within the program.
(4) degree of data entry accuracy.

DISCUSSION QUESTIONS AND PROBLEMS

12-19 (Objectives 12-2, 12-3) The following are misstatements that can occur in the sales and collection cycle:

1. A data entry operator accidentally transposed a zip code in a customer's address. As a result, the bills sent to the customer are returned to the company.
2. A new online ordering service was created to increase sales and customer base. However, a glitch in the software allows only existing customers to make purchases.
3. During the night, a company lost power, which inadvertently wiped all of the previous day's entries and sales from their records. The company does not regularly back up their data.
4. A computer virus scrambled some of the contact information for several customers, which resulted in packages being sent to incorrect addresses.
5. A former employee created a fictitious account for a supplier and deposited the money paid for invoices into this account.
6. A data entry operator accidentally re-entered the sales data from a previous week's sale.
7. A data entry operator attempted to change customer information; however, a glitch in the computer program deleted the customer's profile.
8. A shipment of goods was supposed to arrive pre-priced. Upon opening the shipment, the manager found that the items were not the same items listed on the invoice that came with the shipment.

Required

a. Identify transaction-related audit objective(s) to which misstatement pertains.

b. Identify one automated control that would have likely prevented each misstatement.

12-20 (Objectives 12-2, 12-3) You are doing the audit of Phelps College, a private school with approximately 2,500 students. With your firm's consultation, they have instituted an IT system that separates the responsibilities of the computer operator, systems analyst, librarian, programmer, and data control group by having a different person do each function. Now, a budget reduction is necessary and one of the five people must be laid off. You are requested to give the college advice as to how the five functions could be done with reduced personnel and minimal negative effects on internal control. The amount of time the functions take is not relevant because all five people also do nonaccounting functions.

Required

a. Divide the five functions among four people in such a way as to maintain the best possible control system.

b. Assume that economic times become worse for Phelps College and it must terminate employment of another person. Divide the five functions among three people in such a way as to maintain the best possible internal control. Again, the amount of time each function takes should not be a consideration in your decision.

c. Assume that economic times become so severe for Phelps College that only two people can be employed to do IT functions. Divide the five functions between two people in such a way as to maintain the best possible control system.

d. If the five functions were done by one person, will internal controls be so inadequate that an audit cannot be done? Discuss.

12-21 (Objectives 12-2, 12-3, 12-4, 12-5) The Meyers Pharmaceutical Company has the following system for billing and recording accounts receivable:

1. An incoming customer's purchase order is received in the order department by a clerk who prepares a prenumbered company sales order on which the pertinent information, such as the customer's name and address, customer's account number, and items and quantities ordered, is inserted. After the sales order has been prepared, the customer's purchase order is stapled to it.
2. The sales order is then passed to the credit department for credit approval. Rough approximations of the billing values of the orders are made in the credit department for those accounts on which credit limitations are imposed. After investigation, approval of credit is noted on the sales order.
3. Next the sales order is passed to the billing department, where a clerk key-enters the sales order information into a data file, including unit sales prices obtained from an approved price list. The data file is used to prepare sales invoices.

   The billing application automatically accumulates daily totals of customer account numbers and invoice amounts to provide "hash" totals and control amounts. These totals, which are inserted in a daily record book, serve as predetermined batch totals for verification of computer inputs. The billing is done on prenumbered, continuous, multi-copy forms that have the following designations:

   (a) Customer copy
   (b) Sales department copy, for information purposes
   (c) File copy
   (d) Shipping department copy, which serves as a shipping order

   Bills of lading are also prepared as by-products of the invoicing procedure.
4. The shipping department copy of the invoice and the bills of lading are then sent to the shipping department. After the order has been shipped, copies of the bill of lading are returned to the billing department. The shipping department copy of the invoice is filed in the shipping department.
5. In the billing department, one copy of the bill of lading is attached to the customer's copy of the invoice and both are mailed to the customer. The other copy of the bill of lading, together with the sales order is then stapled to the invoice file copy and filed in invoice numerical order.
6. The data file is updated for shipments that are different from those billed earlier. After these changes are made, the file is used to prepare a sales journal in sales invoice order and to update the accounts receivable master file. Daily totals are printed to match the control totals prepared earlier. These totals are compared with the "hash" and control totals by an independent person.

Required

a. Identify the important controls and related sales transaction-related audit objectives.
b. List the procedures that a CPA will use in an audit of sales transactions to test the identified controls and the substantive aspects of the sales transactions.

12-22 (Objective 12-3) During your audit of Wilcoxon Sports, Inc., a retail chain of stores, you learn that a programmer made an unauthorized change to the sales application program even though no work on that application had been approved by IT management. In order for the sales application program to work, the programmer had to make modifications to the operating software security features. The unauthorized change forced the sales program to calculate an automatic discount for a customer who happens to be the brother-in-law of the programmer. The customer and programmer split the savings from the unauthorized discount. The programmer modified the program and returned it to the librarian who placed it into the files for live production use. No other information was forwarded to the librarian.

Required

1. What recommendation do you have for management of Wilcoxon Sports, Inc., to prevent this from recurring?
2. Explain why you believe the suggested internal control improvements will prevent problems in the future.

12-23 (Objectives 12-1, 12-2, 12-5) Most grocery stores use bar code scanning technologies that interface with cash registers used to process customer purchases. Cashiers use the scanners to read bar code labels attached to each product, which the system then uses to obtain unit prices, calculate transaction totals, including sales taxes, and update perpetual inventory databases. Similarly, cashiers scan bar codes on coupons or member discount cards presented by the customer to process discounts. Along with the scanning technologies, groceries use point-of-sale technologies that allow customers to swipe debit and credit cards for payment, while still maintaining the ability for customers to pay with cash.

Required

a. Which financial statement accounts are impacted by the use of these technologies in a typical grocery store?

b. Identify risks inherent to this business process in a grocery store that might affect the financial statement accounts identified in part a. For each risk, describe how these technologies help reduce the inherent risk.

c. How does the use of these technologies create new risks for a grocery store?

d. How might an auditor use technology to test the operating effectiveness of a bar code scanner based check-out system?

12-24 (Objective 12-5) A CPA's client, Boos & Baumkirchner, Inc., is a medium-size manufacturer of products for the leisure-time activities market (camping equipment, scuba gear, bows and arrows, and so forth). During the past year, a computer system was installed and inventory records of finished goods and parts were converted to computer processing. The inventory master file is maintained on a disk. Each record of the file contains the following information:

- Item or part number
- Description
- Size
- Unit-of-measure code
- Quantity on hand
- Cost per unit
- Total value of inventory on hand at cost
- Date of last sale or usage
- Quantity used or sold this year
- Economic order quantity
- Code number of major vendor
- Code number of secondary vendor

In preparation for year-end inventory, the client has two identical sets of preprinted inventory count cards. One set is for the client's inventory counts, and the other is for the CPA's use to make audit test counts. The following information is on each card:

- Item or part number
- Description
- Size
- Unit-of-measure code

In taking the year-end inventory, the client's personnel will write the actual counted quantity on the face of each card. When all counts are complete, the counted quantity will be entered into the system. The cards will be processed against the inventory database, and quantity-on-hand figures will be adjusted to reflect the actual count. A computer-generated edit listing will be prepared to show any missing inventory count cards and all quantity adjustments of more than $100 in value. These items will be investigated by client personnel, and all required adjustments will be made. When adjustments have been completed, the final year-end balances will be computed and posted to the general ledger.

The CPA has available generalized audit software that will run on the client's computer and can process both card and disk files.

Required

a. In general and without regard to the facts in this case, discuss the nature of generalized audit software and list the various types and uses.

b. List and describe at least five ways generalized audit software can be used to assist in all aspects of the audit of the inventory of Boos & Baumkirchner, Inc. (For example, the software can be used to read the disk inventory master file and list items and parts with a high unit cost or total value. Such items can be included in the test counts to increase the dollar coverage of the audit verification.)*

12-25 (Objectives 12-2, 12-3) One of the firm's audit partners, Alice Goodwin, just had lunch with a good friend, Sara Hitchcock, who is president of Granger Container Corporation. Granger Container Corp. is a fast-growing company that has been in business for only a few years. During lunch, Sara asked Alice for some advice and direction on how Granger Container should structure its systems development process within the Information Systems Department. Sara noted that because Granger has experienced such tremendous growth, the systems development process has evolved into its current state without much direction. Given Granger Container's current size, Sara questions whether their current processes are reasonable. Sara's concern is magnified by the fact that she has little understanding of information systems processes. Alice told Sara about your information systems evaluation experience and agreed to have you look at Granger Container's current systems development procedures. Sara gave Alice the following summary of the current processes:

> Eric Winecoff is the information systems manager at Granger Container and has been at the company for 3 years. Before becoming an employee, Eric provided software consulting services for Granger Container. Granger Container purchased a basic software package from Eric's former employer. Granger Container has the capability to make extensive modifications to the purchased software to adapt the software to Granger Container's specific business needs.
>
> Program change requests are initiated by either the operations staff (two employees) or the programming staff (two employees), depending on the nature of the change. All change requests are discussed in Eric's office with the initiating staff. Based on that discussion, Eric provides a verbal approval or denial of the requested change. For approved projects, he encourages the programmers to visit with him from time to time to discuss progress on the projects. Eric's long and varied experience with this particular software is helpful in the evaluation of work done, and he is able to make substantive suggestions for improvement. Eric has complete faith in his programmers. He believes that if he controlled their activities too carefully, he would stifle their creativity.
>
> Upon completion of the technical programming, Eric reviews the programs and related systems flowcharts. Eric only rarely identifies last-minute changes before granting his final approval for implementation. One evening a week is set aside in the computer room for program debugging and testing.
>
> The programmers stay late on those evenings so that they can load the programs themselves. To speed up the coding, debugging, and testing process, the programmers work with the actual production program. As a safeguard, however, testing is done on copies of the data files. The original data files are locked carefully in the file storage room. Eric is the only person who has access to the room.
>
> When program changes are tested to the satisfaction of the programmers, Eric reviews the test results. If he approves the test results, he personally takes care of all the necessary communications and documentation. This involves preparing a short narrative description of the change, usually no longer than a paragraph. A copy of the narrative is sent to the user. Another copy is filed with the systems documentation. When the narrative is complete, Eric instructs operations to resume normal production with the new program.

Required

a. Describe controls in Granger Container's systems development and program change processes.

b. Describe deficiencies in Granger Container's systems development and program change processes.

c. Provide recommendations for how Granger Container could improve its processes.

12-26 (Objective 12-4) Following are 10 key internal controls in the payroll cycle for Gilman Stores, Inc.

Key Controls

1. To input hours worked, payroll accounting personnel input the employee's Social Security number. The system does not allow input of hours worked for invalid employee numbers.

2. The payroll application is programmed so that only human resource personnel are able to add employee names to the employee master files.
3. Input menus distinguish executive payroll, administrative payroll, and factory payroll.
4. The system automatically computes pay at time and a half once hours worked exceed 80 in a 2-week pay period.
5. The system accumulates totals each pay period of employee checks processed and debits the payroll expense general ledger account for the total amount.
6. Each pay period, payroll accounting clerks count the number of time sheets submitted by department heads for processing and compare that total with the number of checks printed by the system to ensure that each time sheet has a check.
7. For factory personnel, the payroll system matches employee ID numbers with ID numbers listed on job costing tickets as direct labor per the cost accounting system. The purpose of the reconciliation is to verify that the amount paid to each employee matches the amount charged to production during the time period.
8. The system generates a listing by employee name of checks processed. Department heads review these listings to ensure that each employee actually worked during the pay period.
9. On a test basis, payroll accounting personnel obtain a listing of pay rates and withholding information for a sample of employees from human resources to recalculate gross and net pay.
10. The system automatically rejects processing an employee's pay if inputted hours exceed 160 hours for a 2-week pay period.

Required For each control:

a. Identify whether the control is an automated application control (AC) or a manual control done by Gilman employees (MC).

b. Identify the transaction-related audit objective that is affected by the control.

c. Identify which controls, if tested within the last two prior year audits, would not have to be retested in the current year, assuming there are effective IT general controls and no changes to the noted control have been made since auditor testing was completed.

12-27 (Objectives 12-2, 12-3) Your new audit client, Hardwood Lumber Company, has a computerized accounting system for all financial statement cycles. During planning, you visited with the information systems vice president and learned that personnel in information systems are assigned to one of four departments: systems programming, applications programming, operations, or data control. Job tasks are specific to the individual and no responsibilities overlap with other departments. Hardwood Lumber relies on the operating system software to restrict online access to individuals. The operating system allows an employee with "READ" capabilities to only view the contents of the program or file. "CHANGE" allows the employee to update the contents of the program or file. "RUN" allows the employee to use a program to process data. Programmers, both systems and applications, are restricted to a READ-only access to all live application software program files but have READ and CHANGE capabilities for test copies of those software program files. Operators have READ and RUN capabilities for live application programs. Data control clerks have CHANGE access to data files only and no access to software program files. The person in charge of operations maintains access to the operating software security features and is responsible for assigning access rights to individuals. The computer room is locked and requires a card-key to access the room. Only operations staff have a card-key to access the room, and security cameras monitor access. A TV screen is in the information systems vice president's office to allow periodic monitoring of access. The TV presents the live picture and no tape record is maintained. The librarian, who is in the operations department, is responsible for maintaining the library of program tapes and files. The librarian has READ and CHANGE access rights to program tapes and files. The files, when not being used, are stored in shelves located in a room adjacent to the computer room. They are filed numerically based on the tape label physically attached on the outside of the tape cartridge to allow for easy identification by operators as they access tapes from the shelves for processing.

Required What recommendations for change can you suggest to improve Hardwood's information systems function?

12-28 (Objective 12-6) Parts for Wheels, Inc., has historically sold auto parts directly to consumers through its retail stores. Due to competitive pressure, Parts for Wheels installed an Internet-based sales system that allows customers to place orders through the company's Web site. The company hired an outside Web site design consultant to create the sales system because the company's IT personnel lack the necessary experience.

Customers use the link to the inventory parts listing on the Web site to view product descriptions and prices. The inventory parts listing is updated weekly. To get the system online quickly, management decided not to link the order system to the sales and inventory accounting systems. Customers submit orders for products through the online system and provide credit card information for payment. Each day, accounting department clerks print submitted orders from the online system. After credit authorization is verified with the credit card agency, the accounting department enters the sale into the sales journal. The accounting department then sends a copy of the order to warehouse personnel who process the shipment. The inventory system is updated based on bills of lading information forwarded to accounting after shipment.

Customers may return parts for full refund if returned within 30 days of submitting the order online. The company agrees to refund shipping costs incurred by the customer for returned goods.

Required

a. Describe deficiencies in Parts for Wheels' online sales system that may lead to material misstatements in the financial statements.

b. Identify changes in manual procedures that could be made to minimize risks, without having to reprogram the current online system.

c. Describe customer concerns about doing business online with Parts for Wheels. What types of controls could be implemented to address those concerns?

12-29 (Objective 12-6) Based on a cost-benefit analysis, management at First Community Bank decided to contract with Technology Solutions, a local data center operator, to host all of the bank's financial reporting applications. To avoid the significant costs of developing and maintaining its own data center, First Community contracts with Technology Solutions to provide IT server access in a highly secure, environmentally controlled data center facility owned by Technology Solutions. Similar to First Community, other businesses also contract with Technology Solutions to host applications at the same data center.

The bank is directly linked through highly secure telecommunication lines to the data center, which allows bank personnel to transmit data to and from the data center as if the data center was owned by First Community. For a monthly fee, Technology Solutions supports the server hardware in an environment with numerous backup controls in the event power is lost or other hardware failures occur. Bank personnel are responsible for selecting and maintaining all application software loaded on Technology Solutions servers, and selected bank personnel have access to those servers located at the Technology Solutions data center. Bank personnel enter all data, run applications hosted at Technology Solutions, and retrieve reports summarizing the processing of all bank transactions.

Required

a. What risks might First Community assume with this approach to IT system support?

b. How does the use of Technology Solutions impact First Community's internal controls?

c. What impact, if any, does reliance on Technology Solutions as the data center provider have on the audit of First Community's financial statements?

CASE

12-30 (Objectives 12-2, 12-3) The information systems (IS) department at Jacobsons, Inc., consists of eight employees, including the IS Manager, Melinda Cullen. Melinda is responsible for the day-to-day oversight of the IS function and reports to Jacobsons' chief operating officer (COO). The COO is a senior vice president responsible for the overall retail operations who reports directly to the president and chief executive officer. The COO attends board of director meetings to provide an update of key operating performance issues. Because Melinda takes an active role in managing the IS department,

the COO rarely discusses IS issues with the board or CEO. Melinda and the COO identify hardware and software needs and are authorized to approve those purchases.

In addition to Melinda, the IS department is composed of seven other individuals: three programmers, three operators, and one data control clerk. Melinda has been employed by Jacobsons for 12 years, working her way up through various positions in the department. Fortunately, she has been able to retain a fairly stable staff and has experienced minimal turnover. All IS personnel have been employed in their current positions since mid-2009. When hiring personnel, Melinda does extensive background checks on prospective employees, including reference, credit, and criminal checks. Melinda has developed a trust with each employee and, as a result, delegates extensively to each individual. This is especially beneficial because Melinda spends most of her time working with user departments in a systems analyst role, identifying changes needed to existing applications. She conducts weekly IS departmental meetings on Tuesday mornings. Each staff member attends, including night operators, to discuss issues affecting the performance of the department.

The three programmers are responsible for maintaining and updating systems and application software. The lead programmer is responsible for assigning duties among the programming staff. All three programmers have extensive experience with the operating, utility, security, and library software as well as all of Jacobsons' application software packages. Programming assignments are made based on who is least busy among the programming staff at the time. This method of management keeps all programmers familiar with most software packages in use at Jacobsons and keeps programmers excited about the job tasks because of the variety of assignments they receive. Melinda encourages each programmer to take continuing education courses to keep current with the latest technical developments. In addition to programming responsibilities, the programming staff maintains the library of programs and data tapes, which is located in a locked room nearby. The programming staff maintains extensive logs of tape use and of changes made to program files.

The three operators consist of a day operator and two night operators. Most of the applications are based on online inputting from various user departments for batch processing overnight. Thus, the heaviest volume of processing occurs during the night shift, although there is some daytime processing of payroll and general ledger applications. All operators are responsible for monitoring the operation of the equipment and correcting system-caused errors. In addition, they do routine monthly backup procedures. The computer operators have programming experience with the program language used in application programs. Occasionally, when a small change is identified for an application program, Melinda asks the day shift operator to implement that change to avoid overburdening the programming staff.

Operators follow the production schedule prepared by Melinda, who consults with user departments to develop the schedule. The day shift operator reviews the job processed log (which chronologically details the jobs processed) generated at the end of the previous night shift for deviations from the schedule, and the lead night shift operator reviews the job processed log generated at the end of the previous day shift for deviations from the schedule. If jobs processed reconcile to the job schedule, the job processed log is discarded. When there are deviations, the operator doing the review leaves a copy for Melinda, highlighting the deviation. Before doing batch processing jobs, the operators generate an input listing report that summarizes the number of online input entries submitted during the day for processing. This number is recorded and then later compared by the operators with the computer output generated after batch processing and file updating occur. This provides a check figure of the number of transactions processed. When the numbers agree, the output is submitted to the data control clerk. When the numbers disagree, the operators identify the error and resubmit the application for processing.

The data control clerk collates all computer output, including output reports and exception listings. The data control clerk reviews exception reports and prepares correction

forms for reprocessing. Examples of changes that the data control clerk might make include correcting inputting errors (for example, amounts accidentally transposed) and preparing change request forms for changes to existing master files (examples include revising sales price lists and inventory product numbers in the sales master file and adding new employee names, addresses, and Social Security numbers to the payroll master file). After all corrections are made, the data control clerk distributes all computer output to the various user departments. User departments have high regard for the IS staff. Output reports are reconciled to input reports by users on a test basis quarterly.

Required

You are the senior auditor assigned to the audit of Jacobsons. The audit partner has asked you to assist in doing the IS general controls review. The partner has asked you to review this narrative information and respond to the following questions:

1. What controls and deficiencies exist in the lines of reporting from IS to senior management? If you note any deficiencies, provide recommendations that can be included in the management letter.
2. What is your assessment of how Melinda Cullen fulfills her IS management responsibilities? Identify tasks that she does that strengthen the department. Which of her tasks cause you concern? What changes in her day-to-day responsibilities would you make?
3. What is your assessment of the programming function at Jacobsons? What are the strengths? What are the deficiencies? Make recommendations for improvement.
4. What is your assessment of the IS operations function at Jacobsons? What are the strengths? What are the deficiencies? Make recommendations for improvement.
5. What is your assessment of the data control function at Jacobsons? What are the strengths? What are the deficiencies? Make recommendations for improvement.
6. Make recommendations for improving controls over the involvement of users.

ACL PROBLEM

12-31 (Objective 12-5) This problem requires the use of ACL software, which is included in the CD attached to the text. Information about installing and using ACL and solving this problem can be found in Appendix, pages 850–854. You should read all of the reference material preceding the instructions about "Quick Sort" before locating the appropriate command to answer questions a. through f. For this problem use the Metaphor_Trans_2002 file in ACL_Demo, which is a file of purchase transactions. The suggested command or other source of information needed to solve the problem requirement is included at the end of each question.

Required

a. Use Quick Sort for each column in the table and identify any concerns you have about the data. (Quick Sort)

b. Determine the total cost of all purchases, ignoring any concerns in part a. (Total)

c. Determine if there are any duplicates or missing numbers in the voucher file (Invoice column). State your audit concerns with any gaps or duplicates. Provide a possible explanation for any gaps or duplicates that you find. (Gaps and Duplicates)

d. Determine and print the total purchases for the period by product (Summarize). Determine if the total cost is the same as in part b. (Total). What product number has the greatest amount of purchases (Quick Sort)?

e. Determine and print the percent of total purchases by product. Save the classified file for use in requirement f. (Classify). Based on that output, what percentage is product number 024133112 of the total amount?

f. Using the classified file from requirement e., stratify and print the purchases by product. Exclude all items smaller than $1,000. Sort the items to determine the smallest and largest amounts. Use the smallest amount as the minimum in the Stratify window. Because the largest amount is significantly larger than all other items, use the second highest amount as the maximum in the Stratify window. (Filter, Quick Sort, and Stratify)

RESEARCH PROBLEM 12-1: ASSESSING RISKS OF CLOUD COMPUTING

A growing number of organizations are using cloud computing as a viable alternative for their IT resource needs. Cloud computing allows organizations to increase their ability to meet computing resource demands while avoiding significant investments in IT infrastructure, personnel, and software. While forecasts are for continued increases in demand for cloud computing, the benefits also bring a host of new risk considerations. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a thought paper, *Enterprise Risk Management for Cloud Computing*, to help organizations assess and mitigate risks arising from cloud computing. Visit the COSO Web site (www.coso.org). Read the thought paper to answer the following questions:

Required

a. What is cloud computing?

b. What are private clouds, community clouds, public clouds, and hybrid clouds?

c. The paper identifies examples of risks associated with cloud computing. Describe each of the following risks:
   (1) Disruptive force
   (2) Lack of transparency
   (3) Vendor lock-in and lack of application portability
   (4) High-value cyber attack targets