Chapter 12

Computer Controls for Organizations and Accounting Information Systems

After reading this chapter, you will:

1. *Be familiar with* the term ''general computer control objectives'' and *understand* how these objectives are achieved.
2. *Be able* to identify general controls for an organization and understand why they are essential for corporate governance.
3. *Understand* general controls for information technology (IT) and why these should be considered when designing and implementing accounting information systems.
4. *Be familiar with* IT general security and control issues for wireless technology, networked systems, and personal computers.
5. *Understand* the value of the COBIT framework and the part this guidance can play in helping IT managers in an organization.
6. *Know* what input controls, processing controls, and output controls are, and *be familiar with* specific examples of control procedures for each of these categories of controls.

"One way organizations can manage security risks from insiders is to implement centralized and automated identity and access management (IAM) controls."

Georg Aldhizer, III, ''The Insider Threat,''
Internal Auditor (April 2008), p. 71.

INTRODUCTION

This chapter continues the discussion of internal controls from Chapter 11 by focusing on specific security and control procedures that organizations use at three different levels. The highest level takes the perspective of ''enterprise-wide,'' which encourages organizations to use resources efficiently. At the next level, we discuss general controls for information technology (IT) that the organization uses. As we know, IT is pervasive, as are the networks that may be used to access information—anytime, anywhere. One of the primary challenges associated with all this connectivity is security. How do we protect sensitive data and information that is stored or transferred from one device to another? The answer is that organizations must have the appropriate security and control procedures in place. Although no organization can be 100% confident that its assets are protected 24/7, the goal is to obtain a reasonable level of assurance.

Application controls are the third level of controls that we cover in this chapter. Because these controls are designed to protect transaction processing (i.e., to ensure complete and accurate processing of data), they are automatically performed by the information system. We discuss the various categories of application controls near the end of the chapter.

GENERAL CONTROLS FOR ORGANIZATIONS

General controls begin with a **security policy**, a comprehensive plan that helps protect an enterprise from both internal and external threats. Figure 12-1 contains issues that organizations should consider when developing this policy.

In developing its security policies, an organization should also consider ISO 17799, the international information security standards that establish information security best practices.[1] This Standard includes ten primary sections: security policy, system access control, computer and operations management, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, asset classification and control, and business continuity management. ISO certification is becoming an important consideration as more businesses maintain a web presence. The first step to becoming certified under ISO 17799 is to comply with the Standard, and one way to measure and manage compliance is to use a risk analysis tool such as the COSO enterprise risk management (ERM) framework that we discussed in Chapter 11.

[1]Source: http://iso-17799.com

Issue	Example/Explanation
Identify and evaluate assets	• What assets need to be protected?
Identify threats	• What are the sources of potential security problems? • Examples of **external threats** are viruses, worms, retaliation from former employees. • Examples of **internal threats** are misuse of assets by employees and embezzlement.
Assess risk	• Loss of data, privacy, legal liability, loss of customers, etc.
Assign responsibilities	• Choose a development team to help identify potential threats in all areas of the enterprise.
Establish security policies	• Outline security responsibilities, and who owns the specific systems and data. • Be sure to document these relative to computing and technology platforms.
Implement across the organization	• To ensure compliance; appoint individuals to monitor compliance; allot necessary funds.
Manage the security program	• Top-level management oversight is critical.

Source: enterprisesecurity-symantec.com, Article ID: 1128.

FIGURE 12-1 Issues that should be considered when developing a security policy.

Integrated Security for the Organization

A current trend in security practice is to merge **physical security** and **logical security** across an organization. Physical security refers to any measures that an organization uses to protect its facilities, resources, or its proprietary data that are stored on physical media. Logical security uses technology to limit access to the organization's systems and information to only authorized individuals. Figure 12-2 identifies a number of examples of physical security and logical security measures that firms commonly use. The IT Governance Institute published a document that is specifically targeted at this task, called *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd Edition (2006).

Physical Security

- facility monitoring (surveillance systems, cameras, guards, exterior lighting)
- access controls to facilities/data center/computers (biometrics, access cards)
- alarm systems (fire, burglar, water, humidity, power fluctuations)
- shred sensitive documents
- proper storage/disposal of hard drives and other electronic storage media
- secure storage of backup copies of data and master copies of critical software

Logical Security

- e-IDs and passwords
- system authentication
- biometrics
- logs of logon attempts
- application-level firewalls
- anti-virus and anti-spyware software
- intrusion detection systems
- encryption for data in transit
- smart cards

FIGURE 12-2 Examples of physical security and logical security measures.

Many firms now use an integrated approach to security by combining a number of logical and physical security technologies, including firewalls, intrusion detection systems, content filtering, vulnerability management, virus protection, and virtual private networks. An **integrated security** system, supported by a comprehensive security policy, can significantly reduce the risk of attack because it increases the costs and resources needed by an intruder. According to security experts, convergence (of physical and logical security) is the single most overlooked gap in enterprise-wide security—that is, the most insidious security risks are those that slip between physical and logical security systems.[2] Figure 12-3 and the following example illustrate this.

Case-in-Point 12.1 Assume Greg Smith is authorized to scrap inventory. He also has an access badge for the warehouse where the scrapped inventory is located and could enter the warehouse after hours. Although independently these actions are not particularly interesting,

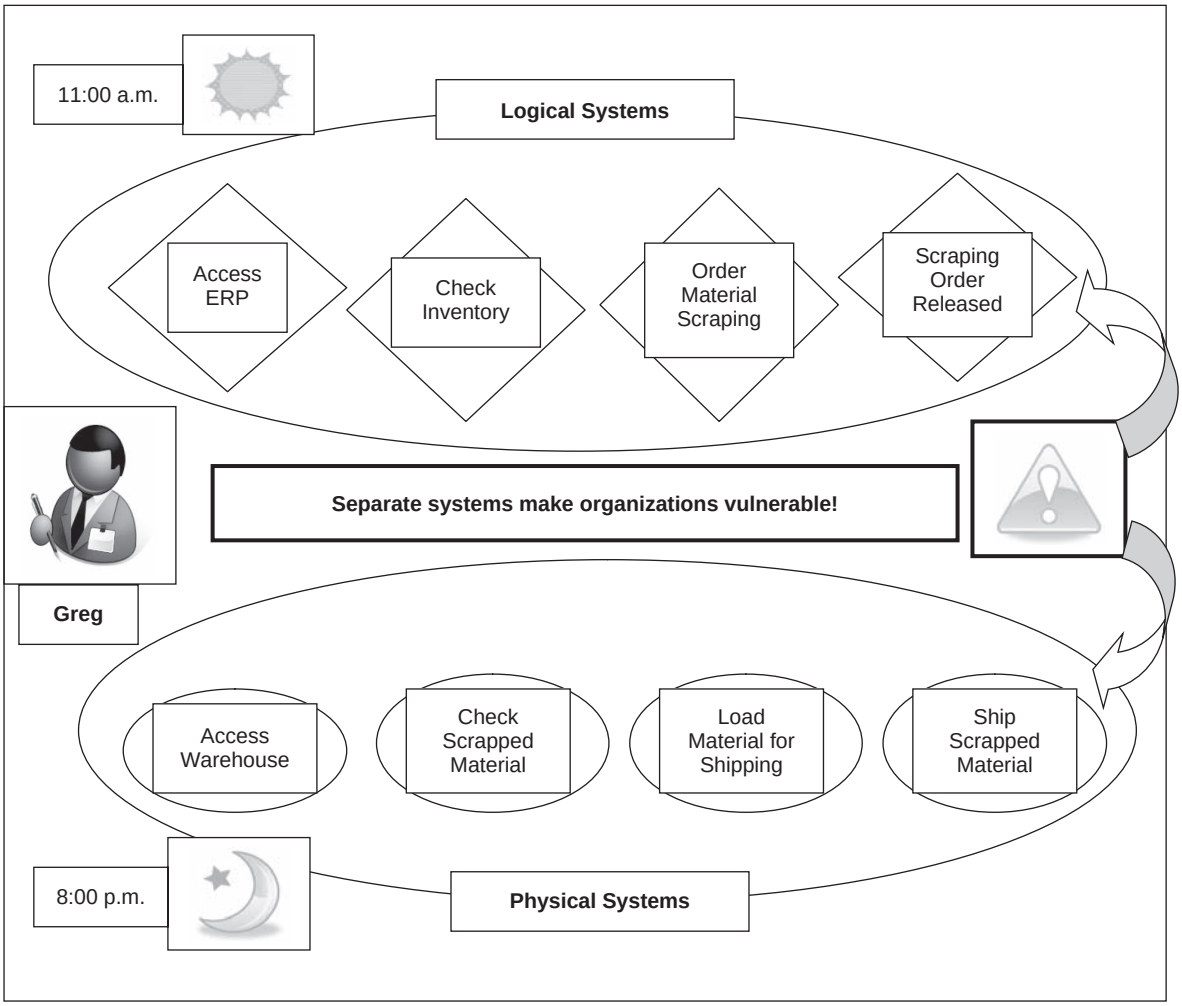

FIGURE 12-3 Diagram of the example in Case-in-Point 12-1.

[2]Source: http://www.alertenterprise.net/

when combined they create a wide variety of problems that could go unnoticed if the physical and logical security systems are not integrated, such as fraud, which could lead to misstated financial statements.

Organization-Level Controls

As we discussed in the previous chapter, management's philosophy, operating style, integrity, policies, and procedures are all important characteristics that influence the tone of a company. These characteristics help to establish the level of security and control consciousness in the organization, which is the basis for the **control environment**. Organization-level controls are particularly important because they often have a pervasive impact on many other controls, such as IT general controls and application-level controls.

In 2007, the Public Company Accounting Oversight Board (PCAOB) released Auditing Standard No. 5, ''An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements.'' This Standard introduces a three-level framework describing entity-level controls at varying levels of precision (direct, monitoring, and indirect).[3] Certainly, if the external auditor must evaluate these controls, then management of the organization must also attend to these controls. We identified a number of these controls in Chapter 11: management's ethical values, philosophy, assignment of authority and responsibility, and the effectiveness of the board of directors. Additional controls that are also very important include the following:

- Consistent policies and procedures, such as formal codes of conduct and fraud-prevention policies. For example, a company may require all employees to periodically sign a formal code of conduct stipulating that computer resources are to be used only for appropriate business purposes, and any acts of fraud or abuse will be prosecuted.
- Management's risk assessment process.
- Centralized processing and controls.
- Controls to monitor results of operations.
- Controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs.
- The period-end financial reporting process.
- Board-approved policies that address significant business-control and risk-management practices.

In addition to these controls, management must have controls over the human resources and data resources of the firm. We examine five types of general controls for IT environments within the organization: (1) personnel policies; (2) file security controls; (3) business continuity planning; (4) computer facility controls; and (5) access to computer files.

Personnel Policies

An AIS depends heavily on people for creating the system, inputting data into the system, supervising data processing during computer operations, distributing processed data to

[3]Source: http://www.pcaobus.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf

authorized recipients, and using approved controls to ensure that these tasks are performed properly. General controls within IT environments that affect personnel include: separation of duties, use of computer accounts, and informal knowledge of employees.

Separation of Duties. Within IT environments, separation of duties should be designed and implemented by requiring *separate* accounting and IT subsystems or departments, and also by *separate* responsibilities within the IT environment.

Separate Accounting and Information Processing from Other Subsystems. An organization's accounting and information processing subsystems are support functions for the other organizational subsystems and should be independent, or separate, from the subsystems that *use* data (accumulated by the accounting function and processed by the information processing subsystem) and *perform* the various operational activities. To achieve this separation, the functional design identified in Figure 12-4 should exist within organizations.

Separate Responsibilities within IT Environment. Highly integrated AISs often combine procedures that used to be performed by separate individuals. Consequently, an individual who has unlimited access to the computer, its programs, and live data also has the opportunity to execute and subsequently conceal a fraud. To reduce this risk, a company should design and implement effective *separation of duties* control procedures. Figure 12-5 describes several functions within a company's IT environment where it is essential to divide the *authority* and *responsibility* for these two functions.

The design and implementation of effective separation-of-duties control procedures make it difficult for any one employee to commit a successful fraudulent activity. However, detecting fraud is even more challenging when two or more individuals *collude* to override separation-of-duties control procedures. A recent survey by the Association of Certified Fraud Examiners (ACFE) reports that over 36% of all fraud cases are committed by two or more individuals who work together to embezzle organizational assets. The median loss in these cases is $500,000, compared to a median loss of $115,000 in fraud cases that involve only one person.[4]

Case-in-Point 12.2 The former D.C. tax manager, Harriette Walters, was able to embezzle more than $48 million over two decades largely because the culture in the finance office in the District of Columbia was one of apathy and silence. As a result, Walters and 10 accomplices,

1. User subsystems initiate and authorize all systems changes and transactions.
2. Asset custody resides with designated operational subsystems.
3. Corrections for errors detected in processing data are entered on an error log, referred back to the specific user subsystem for correction, and subsequently followed up on by the *data control group* (discussed shortly).
4. Changes to existing systems as well as all new systems require a formal written authorization from the user subsystem.

FIGURE 12-4 Functional design to separate accounting and information processing subsystems from other subsystems.

[4]Source: 2008 ACFE Report to the Nation; http://www.acfe.com/documents/2008-rttn.pdf

Function	Explanation of Function/Division
Systems Analysis Function	• Analyze information; process needs; design/modify application programs. • The person performing this function should not perform other related functions. For example, do not allow a programmer for a bank to use actual data to test her program for processing loan payments (she could conceivably erase her own car loan balance).
Data Control Function	• **Use a data control group**; maintain registers of computer access codes; help acquire new accounting software (or upgrades); coordinate security controls with specific computer personnel (e.g., database administrator); reconcile input/output; distribute output to authorized users. • Should be independent of computer operations. This function inhibits unauthorized access to computer facility and contributes to more efficient data processing operations.
Programming Function	• Require formal authorizations for program changes; submit written description of changes to a supervising manager for approval; test changes to programs prior to implementation.
Computer Operations Function	• Rotate computer operators among jobs to avoid any single operator always overseeing the same application. • Do not give computer operators access to program documentation or logic. • Two operators in the computer room during processing of data; maintain a processing log and periodically review for evidence of irregularities. • Without these control procedures a computer operator could alter a program (e.g., to increase his salary).
Transaction Authorization Function	• For each batch of input data, user subsystems submit signed form to verify input data are authorized and proper batch control totals are compiled. • Data control group personnel verify signatures and batch control totals before processing data. • These procedures help prevent errors (e.g., a payroll clerk cannot submit unauthorized form to increase pay rate).
AIS Library Function	• Maintain custody of files, databases, and computer programs in separate storage area called the AIS library. • Limit access to files, databases, and programs for usage purposes to authorized operators at scheduled times or with user authorization; maintain records of all usage. • The librarian does not have computer access privileges. (Regularly, data control group personnel review records for evidence of unauthorized computer access.)

FIGURE 12-5 Divide certain authority and responsibility functions within an IT environment.

who did not work for the city, pleaded guilty to creating and laundering bogus tax refund checks. The embezzlement scheme is the largest involving a city or state government.[5]

Use of Computer Accounts. Most computer networks maintain a system of separate *computer accounts*. Each user has an account and each account has a unique password. When the user logs onto the computer, the system checks the password against a master list of accounts. Only users with current passwords can access computer resources. Some organizations also use account numbers to allocate computer charges to departments. This control procedure is important to protect scarce computer resources from unauthorized use.

[5]Source: D. Nakamura and H. Harris, ''Report on Embezzlement Blames 'Culture of Apathy and Silence','' washingtonpost.com (December 16, 2008), p. B04

Although passwords have been the most used security method to grant users access, IT administrators have a variety of problems with them. Individuals paste their passwords on their monitors, share them with others, or choose simple passwords that are relatively easy for a hacker to guess. As a result, many firms now use **biometric** identification instead (see Chapter 2).

Informal Knowledge of Employees. The 2008 ACFE survey notes that employees who are defrauding their organizations often display certain behaviors (**red flags**) that can alert co-workers and supervisors to trouble. Examples include lavish spending or becoming very irritable or secretive. In particular, the survey results indicate that in over 38% of the cases of fraud the fraudsters were living beyond their means, 34% had financial difficulties, 20% had ''wheeler-dealer'' attitudes, 19% were unwilling to share duties (control issues), and 17% had family problems or were in the middle of a divorce. Sadly, the survey results indicate that the highest percentage of fraud involved employees in the accounting department (29% of all cases reported by survey participants).

Although it might be difficult for co-workers or supervisors to know intimate details of co-workers personal lives, some of these behaviors may be observed without directly confronting the ''suspicious'' co-worker. The threats to an organization by its own employees should never be underestimated. To add emphasis to the need to be alert, PWC's Global State of Information Security Study estimated that people inside organizations were the culprits in 69% of database breaches, and new technologies (e.g., ERPs, B2B processes, mobile devices) make organizational data even more vulnerable to potential misappropriation.[6] Accordingly, it is essential for organizations to safeguard computer files in an AIS from both intentional and unintentional errors. Figure 12-6 describes several reasons for these safeguards.

1. The computer files are not human-readable. Controls must be installed to ensure that these files *can* be read when necessary.
2. The typical computer file contains a vast amount of data. In general, it is not possible to reconstruct such files from the memories of employees.
3. The data contained on computer files are in a very compact format. The destruction of as little as one inch of recording medium means the loss of thousands of characters of data.
4. The data stored on computer files are permanent only to the extent that tiny bits have been recorded on the recording tracks. Power disruptions, power surges, and even accidentally dropping a disk pack, for example, may cause damage.
5. The data stored on computer files may be confidential. Information such as advertising plans, competitive bidding plans, payroll figures, and innovative software programs must be protected from unwarranted use.
6. The reconstruction of file data is costly no matter how extensive a company's recovery procedures. It is usually more cost-effective to protect against file abuse than to depend on backup procedures for file protection.
7. File information itself should be considered an asset of a company. As such, it deserves the same protection accorded other organizational assets.

FIGURE 12-6 Reasons for safeguarding computer files from both accidental and intentional errors.

[6]Source: James Roth & Donald Espersen. ''The Insider Threat,'' *Internal Auditor* (April 2008), pp. 71–73.

File Security Controls

The purpose of file security controls is to protect computer files from either accidental or intentional abuse. For example, this requires control procedures to make sure that computer programs use the correct files for data processing. Control procedures are also needed for the purpose of creating backup copies of critical files in the event that original copies of a file are lost, stolen, damaged, or vandalized. Figure 12-7 provides examples of file security control procedures to verify that the correct file is being updated and to prevent accidental destruction of files.

Business Continuity Planning

Organizations develop and test business continuity plans to be reasonably sure that they will be able to operate in spite of any interruptions, such as power failures, IT system crashes, natural disasters, supply chain problems, and others. Although the distinction between business continuity plans and disaster recovery is not always obvious, they are different. **Business continuity planning** is a more comprehensive approach to making sure organizational activities continue normally, whereas **disaster recovery** is the process and procedures that organizations follow to resume business after a disruptive event such as an earthquake, a terrorist attack, or a serious computer virus. In this section, we discuss disaster recovery controls, controls to ensure fault-tolerant systems, and controls to back up data.

Disaster Recovery. Examples of natural disasters include such events as fires, floods, hurricanes, and earthquakes, as well as man-made catastrophes (such as terrorist attacks). An organization's disaster recovery plan describes the procedures to be followed in the event of an emergency, as well as the role of every member of the *disaster recovery team* (which is made up of specific company employees). The company's management should appoint one person to be in charge of disaster recovery and one person to be second-in-command.

An important part of any disaster recovery plan is the designation of a specific backup site(s) to use for alternate computer processing. These backup sites may be other locations

File Security Control	Purpose of File Security Control
External file labels	• Identify contents of a computer file and help prevent an individual from accidentally writing over a disk file.
Internal file labels	• Record name of a file, date file created, and other identifying data on the file medium that will be read and verified by the computer. • Internal file labels include *header labels* and *trailer labels*. ○ Header label is a file description at the beginning of a file. ○ Trailer label indicates end of a file and contains summary data on contents of file.
Lockout procedures	• Use to prevent two applications from updating the same record or data item at the same time.
Read-only file designation	• Use to earmark data on floppy disks so that data is available for reading only, data cannot be altered by users, nor can new data be stored on the file.

FIGURE 12-7 Examples of file security control procedures.

owned by the company, such as another branch of the same bank, or a site that is owned by other organizations that can be used for short-term periods in the event of a disaster. It is a good idea for the various hardware locations for data processing to be some distance away from the original processing sites in case a disaster affects a regional location. An example would be companies located in flood zones.

Case-in-Point 12.3 USAA, a large insurance company in San Antonio, TX, engaged outside consultants to help determine where the company should locate an alternate data processing center for operations in the event of an emergency. The consulting firm suggested the company build a second data center in the area as a backup. After weighing the costs and benefits of such a project, USAA initially concluded that it would be more efficient to rent space on the East Coast. Ironically, USAA was set to sign the lease contract the week of September 11, 2001. Instead, USAA built a center in Texas, only 200 miles away from its offices—close enough to drive to, but far enough away to pull power from a different grid and water from a different source.[7]

Disaster recovery sites may be either hot sites or cold sites. A **hot site** has a computer system with capabilities similar to the system it will replace. A hot site that also includes up-to-date backup data is called a **flying-start site** because it can assume full data processing operations within a matter of seconds or minutes. A **cold site** is a location where power and environmentally controlled space are available to install processing equipment on short notice. If a disaster recovery plan designates a cold site, then arrangements are also necessary to obtain computer equipment matching the configuration of equipment lost in the disaster. In practice, the type of disaster recovery site used by a company should be determined by a cost-benefit analysis. Finally, simply preparing a disaster recovery plan does not provide assurance that the plan will work when needed. It is also important to periodically test the disaster recovery plan by simulating a disaster, thereby uncovering weaknesses in the plan as well as preparing employees for such emergencies.

Copies of a disaster recovery plan will not be of much use if they are located only in computer systems that are destroyed by a disaster. For this reason, members of a company's disaster recovery team should each keep current copies of the plan at their homes. Finally, in addition to periodic testing, a disaster recovery plan should be reviewed on a *continuous* basis and revised when necessary. This process is an integral part of business continuity planning.

Case-in-Point 12.4 The Deloitte & Touche 2005 Business Continuity Survey was designed to measure the business continuity management (BCM) program initiatives in both the public and private sectors. BCM programs are being elevated and extended to the enterprise level as executives become more involved in BCM governance, most likely due to their overall accountability for risk management. Further, 70% of all respondents reported that most or all functions of their organization have a developed and documented business continuity plan; almost one third of the respondents reported that their organization budgeted over $1 million annually for BCM[8]

Fault tolerant systems. Organizations use **fault-tolerant systems** to deal with computer errors and keep functioning so that data is accurate and complete. Fault-tolerant systems are often based on the concept of *redundancy*. Computer systems can be made

[7]Source: http://www.csoonline.com/article/print/204450.
[8]Source: http://www.deloitte.com/dtt/cda/doc/content/us_assur_2005%20BCM%20SURVEY%20REPORT.pdf.

fault-tolerant with duplicate communication paths or processors. Two major approaches are as follows: (1) Systems with **consensus-based protocols** contain an odd number of processors; if one processor disagrees with the others, it is thereafter ignored. (2) Some systems use a second **watchdog processor**. If something happens to the first processor, the watchdog processor then takes over the processing work.

Disks can be made fault-tolerant through a process called **disk mirroring** (also known as **disk shadowing**). This process involves writing all data in parallel to two disks. Should one disk fail, the application program can automatically continue using the good disk. At the transaction level, a fault-tolerant system can use **rollback processing**, in which transactions are never written to disk until they are complete. Should there be a power failure or should another fault occur while a transaction is being written, the database program, at its first opportunity, automatically *rolls* itself back (reverts) to its pre-fault state.

Backup. Backup is similar to the redundancy concept in fault-tolerant systems. For example, if you write a research paper on a computer, you would be wise to back up your work on a flash drive. As we know, a variety of unfortunate events could occur and you might lose all of your work! If you used a computer in a lab on campus, you are probably aware of the fact that the hard drives are automatically ''cleaned'' every night, so your paper would not be on the hard drive of that computer the next day. And of course other events such as a power failure or human error might occur and—poof!—your paper is gone. However, if you copied your paper on a flash drive, you created *redundancy* so that a problem will not cause you to lose your work.

Because of the risk of losing data before, during, or after processing, organizations have an even greater need to establish backup procedures for their files. The backup and reconstruction procedure typically used under batch processing is called the grandfather-parent-child procedure. Very large organizations might store more than three such copies (i.e., great-grandfather, great-great-grandfather) and banks typically keep many more copies because of the nature of their business.

Three generations of reference data (i.e., previously processed data stored on master files) are retained with the transaction data used during the general ledger updating process. If the most recent master file, the ''child'' copy, is destroyed, the data are reconstructed by rerunning the pertinent transaction data against the prior copy of the reference data (the ''parent'' master file). Should a problem occur during this reconstruction run, there is still one more set of backup data (the ''grandfather'' master file) to reconstruct the parent. The ''parent'' master file is then used to reconstruct the ''child'' master file. Figure 12-8 depicts this procedure.

With the sophisticated real-time systems widely used today, online backups are common. A **hot backup** is a backup performed while the database is on-line and available for read/write, whereas a **cold backup** is performed while the database is off-line and unavailable to its users. During processing, the reference data (master file) are periodically copied on a backup medium. A copy of all transaction data is stored as a *transaction log* as these data are entered into the system. The backup copies are stored at a remote site, which allows data to be recovered in the event a disaster occurs. Through a process called **electronic vaulting**, the data on backup media can be electronically transmitted to a remote site. Should the master file be destroyed or damaged, computer operations will *roll back* to the most recent backup copy of the master file. Recovery is then achieved by reprocessing the contents of the data transaction log against this master file backup copy.

A good disaster recovery plan also includes backups for hardware. With regard to electrical power backup, surge protectors provide protection in the case of short, intermittent power shortages or failures. However, large data processing centers may

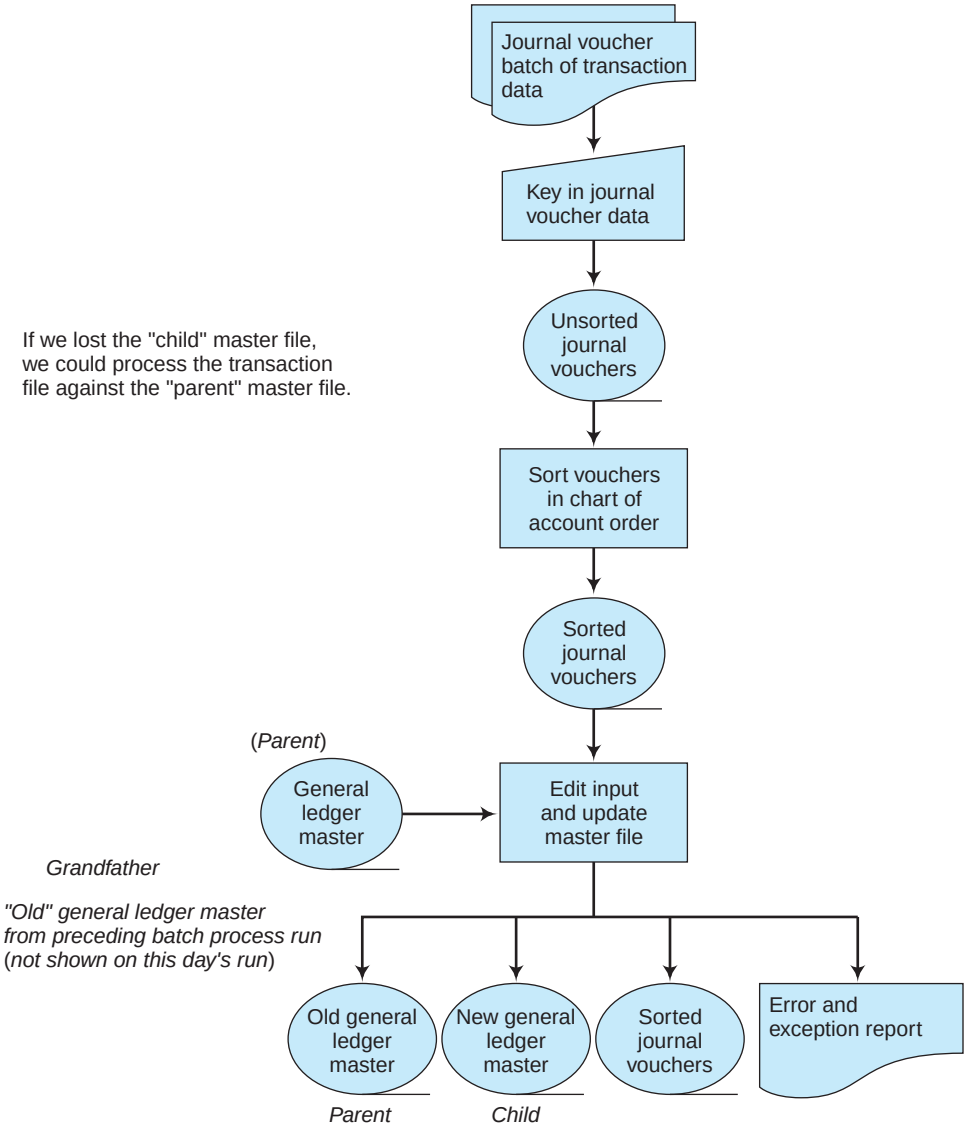

FIGURE 12-8 Grandfather–parent–child procedure under batch processing.

require additional generators for backup power. An **uninterruptible power system (UPS)** is an auxiliary power supply that can smooth the flow of power to the computer, thereby preventing the loss of data due to momentary surges or dips in power. Should a complete power failure occur, the UPS provides a backup power supply to keep the computer system functioning.

Computer Facility Controls

Computer security experts point out that a blunt hammer trumps a strong password every time. What this means is that the physical assets of the data processing center (such as

the web servers, the peripheral devices, and the disk files of the computer library) must be protected. Here are some **computer facility controls** that prevent both unintentional and intentional physical harm.

Locate Data Processing Centers in Safe Places. Usually, organizations locate data processing centers where the public does not have access. Locations away from public scrutiny and guarded by personnel are obviously preferred, especially when the location has a secured entrance. The location of a data processing center should also take into consideration natural disasters. Although it is impossible to protect data processing centers completely from such hazards, advanced planning can minimize exposure to them. For example, companies can increase their protection from fires by locating computer facilities away from boiler rooms, heating furnaces, or fuel storage areas. Similarly, locating computer facilities on high ground or the upper stories of office buildings provides protection from floods. Finally, locating computer facilities in single-story buildings or in heavily reinforced ones can limit earthquake damage.

Limit Employee Access. Few people have reason to be inside a data processing center. Thus, another facility control is to limit access to those company personnel who wear *color-coded identification badges* with full-face pictures. Security badges typically have embedded magnetic, electronic, or optical codes that can be read only by special badge-reading devices. With advanced identification techniques, it is possible to have each employee's entry into and exit from the data processing center automatically recorded in a computer log, which should be periodically reviewed by supervisory personnel.

Another facility control is to place a guard at the entrance to the data processing center. A **man trap** is a small antechamber room between a public corridor and a controlled room. The inner door to the center is self-locking and can be ''buzzed'' open only by the control person, who permits only authorized personnel to enter. Finally, issuing keys to authorized personnel or using dial-lock combinations limits access to the data processing center. With regard to this last control, it is also a good idea to change locks or lock combinations often and to use keys that cannot easily be duplicated.

Buy Insurance. Although insurance is usually thought to be an important method of protection for computer systems, it is actually the protection of last resort. Insurance does not protect the purchaser from loss, it merely compensates for losses if they occur. Insurance policies for computer damages are usually limited in coverage which means that not all instances of loss may be recoverable by the policyholder. Furthermore, compensation usually is restricted to the actual losses suffered by a company. As you might imagine, a fair estimate of what these actual losses entail is not an easy matter. Of special difficulty is placing dollar values on a company's computer equipment that has long since lost any real market value, yet performs vital data processing services for the company.

Computer Access Controls

Regulating who is permitted logical access to computers and files is an important general control in terms of safeguarding sensitive organizational data and software. Remote terminals may be placed anywhere in the country and hooked up to a company's computer by means of ordinary telephone lines or Internet connection. As a result, it is difficult to safeguard logical computer access with direct physical surveillance of terminals. Most

computer systems therefore use passwords to restrict access. Such codes vary in length and type of password information required, but all have the same intent: to limit logical access to the computer only to those individuals authorized to have it.

Organizations should encourage employees to create **strong passwords**. Each character that is added to a password increases the protection that it provides. Passwords should be 8 or more characters in length; 14 characters or longer is ideal. For instance, a 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard.[9] An ideal password combines both length and different types of symbols. The greater the variety of characters (letters, numbers, and symbols) that are included in a password, the harder it is to guess.

As we discussed earlier, passwords can be a problem because they can be lost, given away, or stolen. Thus, security can be increased significantly by using biometrics and/or integrated security measures. **Biometric identification** devices *identify* distinctive user physical characteristics such as voice patterns, fingerprints, facial patterns and features, retina prints, body odor, signature dynamics, and keyboarding methods (i.e., the way a user types certain groups of characters). When an individual wants to access a company's computer system, his or her biometric identifications are matched against those accumulated within the computer. A match must occur for the individual to be given access to the computer system.

GENERAL CONTROLS FOR INFORMATION TECHNOLOGY

The major objectives of an organization's IT controls are to provide reasonable assurance that (1) development of, and changes to, computer programs are authorized, tested, and approved before their usage, and (2) access to programs and data is granted only to authorized users to increase the likelihood that processed accounting data are accurate and complete. These **IT general controls** apply to all information systems. Accordingly, the controls at this level are critical for reliance on application controls. For example, if an employee is allowed to change a program, and that change was not properly authorized or tested, the reliability of company data may be jeopardized.

Firms design and implement cost-effective controls for computers and computer network systems to minimize known vulnerabilities to help protect the data and information contained in these systems. In the process of designing and implementing a system of computer controls for a company's accounting system, the consistency, speed, and flexibility of a computer raise a number of control concerns (see Figure 12-9).

Ironically, sensitive data can sometimes be compromised by the companies who hold the data, although that was not the intent at all, as is illustrated in the following case-in-point.

Case-in-Point 12.5 In violation of its own privacy policy, JetBlue gave about 5 million passenger records to Torch Concepts (a Defense Department contractor). The CEO for JetBlue said the decision to provide the data was a well-intentioned attempt to help the DoD in a national security matter. Subsequently, JetBlue hired Deloitte & Touche to review the airlines' privacy policy implementation. Unfortunately, the lack of controls over this data may cost the airline a lot of money because of class action suits that have been filed against the company for releasing private information.[10]

[9]Source: http://www.microsoft.com/athome/security/privacy/password.mspx.
[10]A. Compart. ''JetBlue Rues the Day it Shared its PNR Data.'' *Travel Weekly*, September 29, 2003,Vol. 62, p. 69.

Control Concern	Explanation
Errors may be magnified	For example, a computer prepares sales invoices by taking the quantity input and multiplying this input by a price from the sales price master file. But, if the computer selects incorrect sales prices, all sales invoices will likely be incorrect.
Inadequate separation of duties	Due to decreased manual involvement within the accounting system
Audit trails	May be reduced, eliminated, or exist only for a brief time in computer-readable form
Unauthorized changes	By individuals who lack sufficient understanding of control procedures and accounting policies, or such changes made without adequate testing or without the consent of management
Greater access to data	Data are a critical organizational resource. When entities have online computer systems and computer networks, individuals can access data from various points where terminals and online PCs are located. Knowledgeable but unauthorized persons might access important files.
Characteristics of magnetic or optical media	Data are invisible. Data (except for read-only memory) are erasable; thus, valuable data may be lost. Data are stored in compressed form—a single magnetic disk can hold as much data as several file cabinets. A single CD-ROM has the storage capacity of 700 floppy disks, which is equivalent to approximately 300,000 pages of text. Thus, damage to a single disk can result in the loss of a large quantity of valuable accounting data.

FIGURE 12-9 The consistency, speed, and flexibility of computers raise control concerns.

The U.S. government also considers computer security a critical issue that should be addressed. In 2005, the National Institute of Standards and Technology (NIST) issued final guidelines on computer security controls for federal information systems. NIST believes that these security guidelines will play a key role in helping federal agencies effectively select and implement security controls and, by using a risk-based approach, do so in a cost-effective manner.[11] This document, which is mandatory for most federal systems, will probably influence controls for systems at all governmental levels, businesses, and other entities. Security controls (management, operational, and technical safeguards) are critical to protect the confidentiality, integrity, and availability of a computer system and its information.

Security for Wireless Technology

As we mentioned in Chapter 1, an important change in today's business environment is the desire for instantly connecting with one another and rapidly exchanging ideas and data. Wireless fidelity (Wi-Fi) technology is based on radio wave transmissions, which makes the transmitted information vulnerable to interception. As a result, organizations that rely on wireless technology must understand the vulnerabilities that exist and explore the various methods of compensating for this risk.

Probably one of the largest users of wireless technology is education. Worldwide, colleges and universities are installing wireless local area networks (WLANs) for a variety of

[11] Source: http://www.nist.gov/public_affairs/releases/computer_security.htm.

reasons: a technologically savvy and highly mobile audience (students and faculty); older, often historic buildings (which cannot be wired); as well as innovative curricula that make use of wireless applications. Probably the most important control for wireless technology is installing a virtual private network **(VPN)**, which is a security appliance that runs behind a university's (or a company's) firewall and allows remote users to access entity resources by using wireless, handheld devices.

Case-in-Point 12.6 The University of Michigan's network infrastructure connects more than 200 departmental LANs on three geographically dispersed campuses spanning 3177 acres and 538 major buildings. The University recently contracted with a firm that provides Wi-Fi security so that authorized users can easily access the University's network with whichever mobile device they choose (PDAs, laptops, digital mobile phones). This type of security is known as a virtual private network.[12]

The risk of unauthorized access to data through electronic eavesdropping is minimized by using **data encryption**. It can be used to prevent a company's competitors from electronically monitoring confidential data transmissions. Through an encryption technique, data are converted into a scrambled format prior to their transmission and converted back in a meaningful form once data transmission is finished. The encrypted data can be read only by a person with a matching decryption key. Data encryption is relatively inexpensive.

Case-in-Point 12.7 Lancaster, California is an example of a whole city that decided to adopt wireless communications technology. The initial installation included high-speed Internet access and has the capacity to transmit voice, data, and video over the same line simultaneously with exceptional speed. All of the transmissions are guarded by military grade security.[13]

Controls for Networks

When desktop computers became economically feasible, firms began placing them throughout the organization and linked them to a centralized computer to form a *distributed data processing (DDP) system*. The basic objective of each remote computer was to meet the specific processing needs of the remote location and communicate summary results to the centralized (host) computer.

DDP systems are still viable in today's business organizations. Large volumes of data are regularly transmitted over long-distance telecommunications technologies. As with wireless technology, the routine use of systems such as DDP and client/server computing increases the potential control problems for companies. These problems include unauthorized access to the computer system and its data through **electronic eavesdropping** (which allows computer users to observe transmissions intended for someone else), hardware or software malfunctions causing computer network system failures, and errors in data transmission. Managers use data encryption to protect information. For example, many companies are encrypting all of their email messages on Local Area Networks (LANs) and Wide Area Networks (WANs).

To reduce the risk of computer network system failures, companies design their network capacity to handle periods of peak transmission volume. Redundant components,

[12]Website: www.bluesocket.com and ''Interworks and Bluesocket Supply University of Michigan with Wireless Security,'' *Business Wire*, January 26, 2004.
[13]''City of Lancaster, California First to Install Revolutionary New Wireless Communications Technology,'' *PR Newswire*, February 18, 2004.

such as servers, are used so that a system can switch to a backup unit in the event of hardware failure. To recover from such a failure, a control procedure, such as a **checkpoint**, helps. Under a *checkpoint control procedure*, which is performed at periodic intervals during processing, a company's computer network system temporarily does not accept new transactions. Instead, it completes updating procedures for all partially processed transactions and then generates an exact copy of all data values and other information needed to restart the system. The system records the checkpoint data on a separate disk file and repeatedly executes this process several times per hour. Should a hardware failure occur, the system is restarted by reading in the last checkpoint and then reprocessing only those transactions that have occurred since the checkpoint.

Two control procedures that reduce the risk of errors in data transmission are routing verification procedures and message acknowledgment procedures. **Routing verification procedures** help to ensure that no transactions or messages are routed to the wrong computer network system address. They work in the following manner: any transaction or message transmitted over a network should have a *header label* that identifies its destination. Before sending the transaction or message, the system should verify that the transaction or message destination is valid and is authorized to receive data. Finally, when the transaction or message is received, the system should verify that the identity of the receiving destination is consistent with the transaction's or message's destination code.

Message acknowledgment procedures are useful in preventing the loss of part or all of a transaction or message on a computer network system. For example, if messages contain a *trailer label*, the receiving destination (or unit) can check to verify that the complete message was received. Furthermore, if large messages or sets of transactions are transmitted in a batch, each message or transaction segment can be numbered sequentially. The receiving destination can then check whether all parts of the messages or transactions were received and were in the correct sequence. The receiving unit will signal the sending unit regarding the outcome of this evaluation. Should the receiving unit detect a data transmission error, the data will be retransmitted once the sending unit has been signaled about this error.

Controls for Personal Computers

Developing control procedures for an organization's portable laptops and desktop PCs begins by taking an inventory of them throughout the organization. The various applications for which each PC is used should also be identified. This should be followed by classifying each PC according to the types of *risks* and *exposures* associated with its applications. To discourage outright theft of desktop PCs, many companies bolt them in place or attach monitors to desks with strong adhesives. A control procedure for laptops is to lock them in cabinets before employees leave at night. Additional control procedures for laptops are identified in Figure 12-10.

PCs are relatively inexpensive. Therefore, it may not be cost-effective for a company to go to elaborate lengths to protect them. What companies should do is use inexpensive, yet effective, control procedures for PCs. It should be noted that because of the compact nature of laptop PCs, theft of these assets has become a big problem for both corporate entities and government agencies.

Case-in-Point 12.8 Recently, an insurance company handled $1 billion in claims for stolen laptops in a single year. In a survey of major corporations and large government agencies conducted a few years ago by the Computer Security Institute and the FBI computer crime squad, 69% of the respondents acknowledged incidents of laptop theft. One hundred fifty

Identify your laptop	• Which model? What configuration? What is the serial number? Are there any other unique identifiers? Without these details, law enforcement agencies, airlines, hotels, and so on, have little chance of retrieving your company's stolen laptop. • Keep a copy of all relevant information about your laptop in a safe place. Leave it in your desk at the office or at your home. Never tape the relevant information to the laptop or store the information electronically on the laptop's hard disk.
Use nonbreakable cables to attach laptops to stationary furniture	• For example, in a hotel room be sure to use a cable or other security device to attach the laptop to some stationary object such as a desk or some other piece of heavy furniture.
Load anti-virus software onto the hard disk	• Automatically perform an anti-virus scan whenever the laptop is turned on or whenever a diskette is inserted. • Have anti-virus scanning software check all changed or new files. • Keep anti-virus software current. Keep virus definitions current.
Back up laptop information	• Never keep backups in the laptop case. • While traveling, keep backup diskettes in a pocket or briefcase. • If possible, back up to your company's internal network via modem, when you are out of the office. • Back up frequently and test regularly to ensure data integrity.

FIGURE 12-10 Additional control procedures for laptops.

organizations cited a total of over $13 million in financial losses. The average annual price tag of losses per organization was $86,920.

As laptops become more sophisticated, people are using them as primary PCs and are saving large amounts of critical data on portable drives. Three simple safeguards are (1) back up important laptop data often, (2) password protect them, and (3) encrypt sensitive files. Organizations can also install anti-theft systems in them—for example, software that uses the integrated web cam to take a picture of whoever uses it next, or GPS systems to track the equipment itself.

Case-in-Point 12.9 "Laptops hardly ever get backed up," laments Scott Gaidano, president of DriveSavers, "and because laptops are portable, they get into more adventures." Among the many disasters he has seen regarding laptop computers include: one fell into the Amazon River, one melted in a car fire, one run over by a bus, and four dumped in bathtubs. In each case, although the machine was trashed, the data were salvaged.

IT Control Objectives for Sarbanes-Oxley[14]

The Sarbanes-Oxley Act of 2002 (SOX) profoundly impacts public companies, their managers, the internal auditors, and the external auditors as they each assess internal controls throughout the company to comply with the provisions of the Act. Companies must also consider the requirements of the PCAOB Standard No. 2 (discussed at the

[14]Sources of information for this section: Cook, Lynn, "IT control objectives for Sarbanes-Oxley: New guidance on IT control and compliance," (October 31, 2003) at www.deloitte.com; and www.itgi.org (resource center—entire document available as a pdf file).

beginning of this chapter) and PCAOB Standard No. 5. To help organizations comply with SOX and the PCAOB requirements, the IT Governance Institute (ITGI) issued ''IT Control Objectives for Sarbanes-Oxley'' in April 2004.

Neither the SOX legislation, nor the PCAOB Standards, includes detailed guidance for organizations. The ITGI publication provides that detail by starting with the IT controls from COBIT and linking those to the IT general control categories in the PCAOB standards, and then the control objectives are linked to the COSO framework. As we discussed in Chapter 11, COBIT is an IT governance framework that provides company-level objectives and controls around those objectives, as well as activity-level objectives and controls. It is important to point out that COBIT identifies controls that may be used for both operational and compliance objectives; however, the ITGC document only focuses on controls that support financial reporting.

APPLICATION CONTROLS FOR TRANSACTION PROCESSING

General controls focus on organization-level issues, while IT general controls apply to all information systems. The purpose of **application controls** is to prevent, detect, and correct errors and irregularities in processing transactions. The ITGI document discussed in the previous section states that IT general controls and application controls are becoming more integrated—that IT general controls support application controls and together they ensure complete and accurate information processing. The point is that organizations process information 24/7, and the typical manager cannot afford to wait several weeks for manual reconciliation of an error.

Application controls are those controls that are embedded in business process applications. The three major stages of data processing work are accumulating the input data, processing the data, and reporting the processed data in some form of output (e.g., a performance report). We discuss various application control procedures for AISs based on these three stages. First, we examine application controls over data input (called *input controls*). Next, we identify application controls that are intended to protect the processing of data (called *processing controls*), and finally, we survey application controls related to data output (called *output controls*).

Figure 12-11 emphasizes the important point that a company's application controls consist of input, processing, and output controls. Because every company's system is somewhat different, each company must consider the risk of errors and irregularities going undetected in processing its accounting data. The company must then design and implement its own cost-effective combination of input, processing, and output application controls.

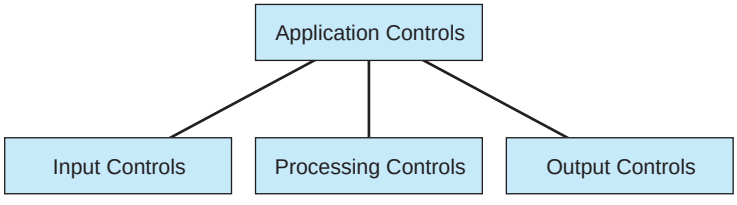

FIGURE 12-11 The composition of a company's application controls.

Input Controls

Although many organizations are now using automated systems to collect data (e.g., barcode scanners), some applications still require employees to manually enter data in the information system. As a result, the risk of undetected errors and irregularities is typically higher in this stage compared to the processing and output stages. In an attempt to reduce this risk factor, the strongest application controls are commonly found in the input stage of data processing.

Input controls help ensure the validity, accuracy, and completeness of the data entered into an AIS. It is usually cost effective to test input data for the attributes of validity, accuracy, and completeness as early as possible. There are at least five reasons for this:

1. Data that are rejected at the time they are input can be more easily corrected—for example, by reference to a source document.
2. Data that have been transcribed accurately are not necessarily good data, merely data that have been copied correctly. Further data testing is useful.
3. It is not cost-effective to screen accounting data continuously throughout the processing cycles of an AIS. Past some point in the job stream, all data are considered valid and error-free.
4. It is vital that an AIS use accurate data in later data processing operations. This protects master files from inaccuracies and safeguards computer processing in subsequent stages of the data processing work.
5. An AIS cannot provide good outputs if it does not start with good inputs.

For discussion purposes, it is convenient to divide the topic of input application controls into three categories: (1) observation, recording, and transcription of data; (2) edit tests; and (3) additional input controls.

Observation, Recording, and Transcription of Data. In general, data enter an AIS when business transactions are recorded. An organization often finds it useful to install one or more observation control procedures to assist in collecting data that will be recorded. One such control procedure is the introduction of a *confirmation mechanism*—for example, requiring a customer to sign, and therefore confirm, a sales order.

The data observation process can also make use of *dual observation*. Under this control procedure, the accuracy of the data observation process is enhanced because more than one employee participates in the process. In some organizations, the dual observation control procedure is *supervisory*. Here, the supervisor of the employee (or employees) involved in collecting data is required to confirm the accuracy of the data gathered by the employee.

Once accounting data have been collected, they must be recorded. Data collection and the subsequent recording of these data are areas in which a great deal of automation has taken place. For example, the use of *point-of-sale (POS) devices* (such as *bar code readers* that interpret the universal product code—UPC—commonly printed on store products and *smart cash registers* that are connected to offsite computers) to encode data have been found to substantially decrease error rates in the recording process as well as to eliminate the expense involved in rekeying data.

In some instances, automated data collection and recording are not feasible, and an initial source document must be prepared manually. To encourage accuracy in the data collection and recording processes in these situations, several control procedures are

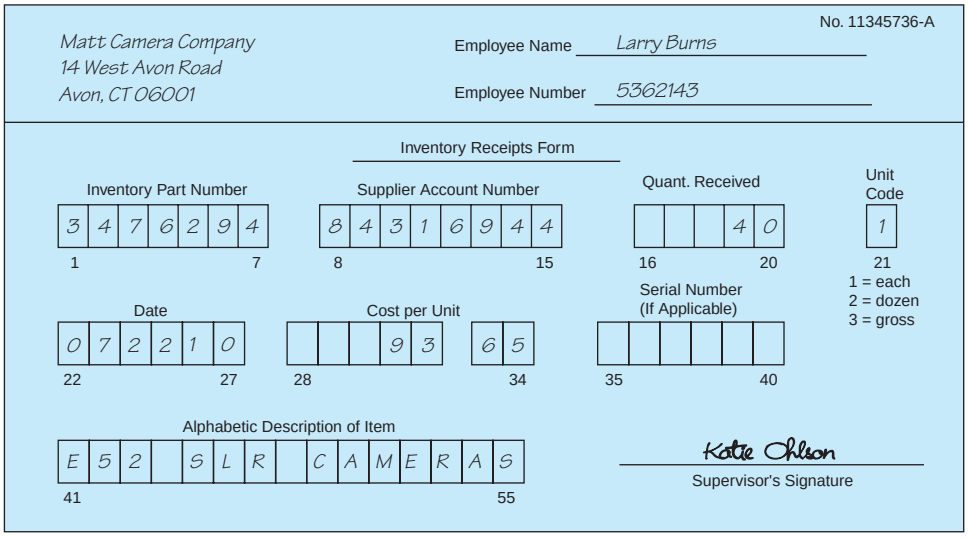

FIGURE 12-12 A preprinted recording form for inventory receipts.

possible. One example is to use *preprinted recording forms*, such as the inventory receipts form illustrated in Figure 12-12. In general, these forms ensure that all the data required for processing have been collected and also enhance accuracy in the recording process. For example, the exact number of spaces required for such field items as the inventory part number and the supplier account number is clear because a box has been provided for each numerical digit, thus guarding against the loss or addition of digits in these fields. Organizations can use similar controls on web pages.

When using transcription, the data on source documents should be organized to facilitate the transcription process. Thus, well-designed, preprinted source-document forms are an important input control because they encourage adherence to the general principle of source-document and computer-input compatibility. Specially-designed input forms are the most commonly used method to enter data in a database. The person who designs the form can make the electronic version look just like the old paper version of the form that employees are accustomed to using. A big advantage of a database form is that it can be designed to lock certain fields to prevent changes, to control certain fields so that a user cannot enter an unreasonable value, to limit data values in certain fields, and a variety of other useful input controls.

Edit Tests. Programs or subroutines that check the validity and accuracy of input data after the data have been entered and recorded on a machine-readable file are called **input validation routines** (or **edit programs**). The specific types of validity and accuracy checks that input validation routines perform are called *edit tests* (or *edit checks*). **Edit tests** examine selected fields of input data and reject those transactions (or other types of data input) whose data fields do not meet the preestablished standards of data quality. Real-time processing systems perform edit tests during the data-entry process. Batch processing systems (illustrated in Figure 12-13) execute edit tests before regular data processing.

Edit tests can also be coordinated in what is called a *redundant data check* to ensure data accuracy. The idea is to encode repetitious data on a file or transaction record, thereby enabling a later processing test to compare the two data items for compatibility. For example, the reason you are always asked for the expiration date of your credit card is

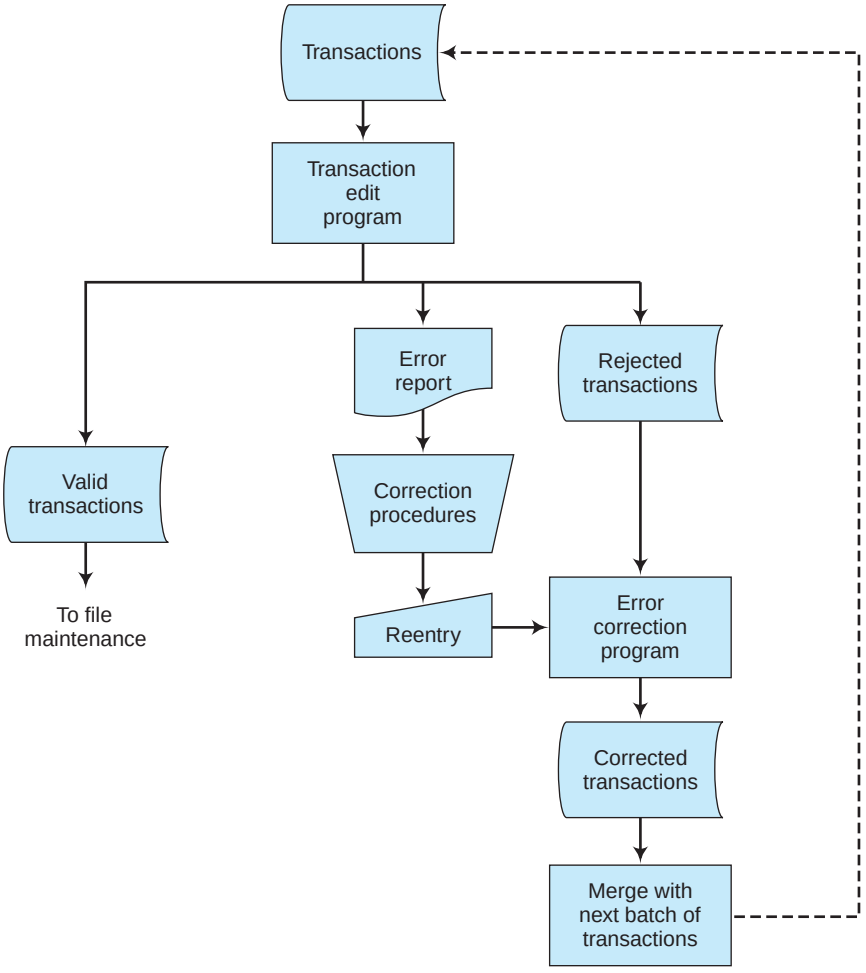

FIGURE 12-13 Use of edit program to execute edit tests under batch processing.

because that value is also encoded in the credit card number as well. Examples of edit tests are listed in Figure 12-14.

Additional Input Controls. It is possible for a data field to pass all of the edit tests previously described and still be invalid. To illustrate, a bank might use the incorrect account number 537627 (instead of the proper account number 537621) when processing a customer's transaction. When the incorrect account number is keyed into a remote terminal and submitted to edit tests, it will, for example, (1) pass a test of numeric field content ensuring that all digits were numeric, (2) pass a test of reasonableness ensuring that the account number itself fell within a valid range of values (e.g., account number greater than 100,000 and less than 800,000), (3) pass a test of sign (i.e., account number positive), and (4) pass a test of completeness (i.e., no blanks in fields).

Thus, additional control procedures are required for this error to be detected. One control procedure is to incorporate an *unfound-record test* into the data processing

Tests of:	Purpose
Numeric field content	To make sure that such data fields as Social Security number, sales invoice number, and date contain only numbers
Alphabetic field content	To make sure such fields as customer name contain only alphabetic letters
Alphanumeric field content	To make sure that fields such as inventory parts descriptions contain letters and/or numbers, but no special characters
Valid codes	e.g., 1 = cash sale; 2 = credit sale
Reasonableness	e.g., total hours worked by an employee during a weekly pay period does not exceed 50
Sign	e.g., paycheck amounts always positive
Completeness	To check that there are no blanks in fields that require data
Sequence	To make sure that successive input data are in some prescribed order (e.g., ascending, descending, chronological, alphabetical)
Consistency	e.g., all transactions for the same sales office have the same office code number

FIGURE 12-14 Examples of edit tests.

routine used to update the master file of bank records. With this approach, any transaction for which there is no corresponding master file record would be recognized as invalid and rejected from the transaction sequence (it would be returned for correction). But what if a master file record did exist for account 537627—the incorrect account number? This would indeed be unfortunate because our ''unfound-record'' control procedure would not detect the error, and, even worse, the legitimate master file record with account number 537627 would be updated with the transaction data generated by another customer.

Continuing with our bank example, an alternative to this unfound-record test is to expand the six-digit data field of customer bank account numbers to seven digits with *a check-digit control procedure*. Normally, the check digit is computed as a mathematical function of the other digits in a numeric field, and its sole purpose is to test the validity of the associated data. To illustrate, consider the original (correct) account number 537621. The sum of these six digits is $5 + 3 + 7 + 6 + 2 + 1 = 24$. One type of check digit would append the low-order digit of this sum ''4'' to the account number. The seven-digit value 5376214 would be used instead of the six-digit series 537621 to represent the account number. The computer program would duplicate this computational procedure at the time of data access, and therefore validate the accuracy of the data before the transaction data were used to update a master file record.

A check digit does not guarantee data validity. For example, the check-digit procedure described here would be unable to distinguish between the correct account number 5376214 and the transposed number 5736214 because the transposition of digits does not affect the sum. There are, however, check-digit techniques that do include ''ordering of digits'' in the construction of check-digit values. An example of one of these techniques is the *Modulus 11 technique*. Through this technique, the check digit is calculated by subtracting the sum of the digit products from the next highest multiple of 11. An example to illustrate the calculation of a check digit under the Modulus 11 technique is provided in Figure 12-15.

Let's assume that in preparing the Alan Company's biweekly payroll, two of the employees have the following payroll numbers: 3478 and 3748. To utilize the Modulus 11 technique for our check-digit control procedure, we determine the check-digit value for an employee's payroll number by applying an algorithm based on each employee's four digits. The calculation below shows under the Modulus 11 technique how we arrived at the check-digit value of 9 to append to the payroll number 3478 to come up with the employee's new payroll number using the Modulus 11 technique.

Four digits of employee number:	3	4	7	8
Weighting factors:	5	4	3	2
Digit products:	15	16	21	16
Sum of digit products:				68
Next higher multiple of 11 (11×7):				77
Check digit (difference of above two numbers):				9
Employee's new payroll number:				34789

Validation involves having the computer recompute the check digit, using the same algorithm by which this digit was predetermined. The computer then compares the result of the recomputation to the original keyed-in value. If a particular payroll transaction involves the correct employee number 34789 and this number was properly keyed into the system, the algorithm will generate a 9 as the check digit. Since the digit 9 is the same as the last digit on the employee payroll number, the computer accepts the number as correct. On the other hand, if the incorrect number 37489 is entered by mistake for the above payroll transaction (the digits 3748 represent the four digits of the other employee's payroll number before a check digit is added), the check digit generated by the algorithm will be 6, computed as follows: $(3 \times 5) + (7 \times 4) + (4 \times 3) + (8 \times 2) = 71$. The next highest multiple of 11 is 77:77 minus 71 = 6. Since this check digit of 6 is not the same as the last digit on the entered number (which is a 9), the employee payroll number 37489 will be rejected by the computer as incorrect.

FIGURE 12-15 Illustration of Modulus 11 technique for calculating a check digit.

Processing Controls

Processing controls focus on the manipulation of accounting data after they are input to the computer system. An important objective of processing controls is to contribute to a good audit trail. A clear audit trail is essential, for example, to enable individual transactions to trace, to provide documentation for changes in general ledger account balances, to prepare financial reports, and to correct errors in transactions. To achieve a good audit trail, require a printed *transaction listing* during each file-update by batch processing systems and at the end of every day by online processing systems.

Furthermore, use a unique and sequentially assigned transaction reference designator to identify each transaction in a listing. These transaction reference designators should be posted to the general ledger account records and recorded on the specific source documents pertaining to the transactions. Figure 12-16 illustrates an audit trail for a computer-based system, showing how source documents can be easily located by tracing back from an activity (or proof) listing, which is discussed shortly under output controls.

Control Totals. Suppose you were the data processing manager at a bank that processed over 100,000 bank checks per day. How would you make sure that all these checks are

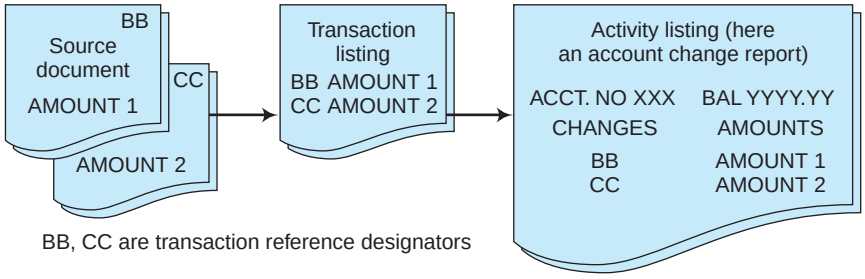

FIGURE 12-16 An audit trail for a computer-based system.

correctly processed by the computer? One procedure is to batch the checks in separate bundles of, say 200 checks, and prepare a special *batch control document* to serve as a control on the contents of each bundle. The information on this document might include the bundle number, today's date, and the total dollar amount for the checks themselves. The total dollar amount represents the **batch control total**. When computer processing commences, the special information on the lead control record (i.e., the batch control document) is accessed first and the batch control total is stored in computer memory. As the checks are accessed individually, their amounts are also accumulated in computer memory. Once all the checks in the batch are read, the accumulated total is compared with the batch control total. A match signals acceptable processing. A non-match signals an error, which may then be traced either to an error in the batch control total or to some difficulty in processing—e.g., the inability of the MICR reader to understand the data on one or more checks.

In fact, MICR readers are themselves a form of control. An original check has a line of magnetic ink with specific information that is recognized by highly reliable MICR readers. Even the best printers do not use this magnetic ink and copied checks can therefore be detected immediately.[15]

A control total that involves a dollar amount is called a *financial control total*. Other examples of financial control totals include the sum of cash receipts in an accounts receivable application, the sum of cash disbursements in an accounts payable application, and the sum of net pay in a payroll application.

AISs also use *nonfinancial control totals*, which compute nondollar sums—for example, the sum of the total number of hours worked by employees in a payroll application. A similar control is a *record count*. With this control procedure, the number of transaction items is counted twice: once when preparing transactions in a batch and again when actually performing the data processing. Yet a third example is the exact byte count of a legitimate computer program, which IT personnel can use to detect tampering.

Control totals do not have to make sense to be useful. For example, when cash receipts from customers are processed, the manual sum of the customers' account numbers in a batch of transactions might be computed to form a **hash total**. This sum is meaningless, but is useful as a check against an ''internal'' tally of this same hash total by the computer at the time of data access.

Data Manipulation Controls. Once data have been validated by earlier portions of data processing, they usually must be manipulated (i.e., processed) in some way by computer programs to produce decision-useful information, such as a report. One

[15]www.pointofsale.com

processing control procedure is to make sure that the computer programs are complete and thorough in their data manipulation. Ordinarily, this is accomplished by examining *software documentation*. System flowcharts, program flowcharts, data flow diagrams, and decision tables can also function as controls because they help systems analysts do a thorough job in planning data processing functions.

After computer programs have been coded, they are translated into machine language by an error-testing *compiler*. The compiler controls the possibility that a computer program contains programming language errors. A computer program can also be tested with specially designed *test data* that expose the program to all the exception conditions likely to occur during its actual use.

Output Controls

Once data have been processed internally by a computer system, they are usually transferred to some form of output medium for storage, screen display, or in the case of printed output, prepared as a report. The objective of **output controls** is to ensure the output's validity, accuracy, and completeness. Two major types of output application controls within IT environments are (1) validating processing results and (2) regulating the distribution and use of printed output.

Validating Processing Results. The validity, accuracy, and completeness of computerized output in AISs can be established through the preparation of *activity* (or proof) *listings* that document processing activity. (A simplified activity listing was illustrated in Figure 12-16.) These listings provide complete, detailed information about all changes to master files, and thus contribute to a good audit trail. Organizational employees use such activity listings to trace file changes back to the events or documents that triggered these changes and thereby verify current file information or printed information as valid, accurate, and complete output.

Regulating Distribution and Use of Printed Output. One of the more compelling aspects of output control deals with the subject of *forms control*. Perhaps the most interesting situations involve computerized check-writing applications in which MICR forms or perforated printer forms become the encoding media for preparing a company's checks. Usually, these forms are preprinted with the company's name, address, and bank account number. Control over the forms associated with check writing is vital.

The most common type of control used with computer-generated check-writing procedures is the coordination of a preprinted check number on the printer form with a computer-generated number that is printed on the same form at run time. The numbers on these *pre-numbered forms* advance sequentially and are prepared by the forms' supplier according to the specifications of an organization. The computer-generated numbers also run sequentially and are initialized by adding 1 to the check sequence number stored from the last processing run. The numbers on the pre-numbered forms and the computer-generated numbers should match during normal processing. Discrepancies should be examined carefully and the causes fully resolved. Other examples of forms that enjoy a special control advantage when pre-numbered include reports containing sensitive corporate information and computer-generated lottery and athletic event tickets.

Computer reports often contain sensitive information, and it is important that such information be restricted. Thus, for example, a payroll register, indicating the earnings of each employee during a given pay period, is a type of report whose distribution should be

restricted. The most common approach to distributional control is through an *authorized distribution list*. For each output report (hard copy or electronic), distribution is limited to authorized users only. Where data processing activities are centralized, it is sometimes the case that the user will physically visit the computer facility to pick up a copy of a sensitive report. In these instances, a notebook, or log, of pickups can be maintained and the pickup employee asked to sign the book. The employee's identification number is recorded for security purposes at the time the report is taken.

In situations where it is not possible to have representatives from user groups pick up reports, bonded employees can be authorized to deliver the reports to users. Subsequently, random checks on the distribution of these reports can be made by the bonded employees' supervisors to verify distribution. After sensitive reports are no longer needed, it is important to properly destroy them (i.e., use a document shredder). Shredding reports is a stronger control than throwing them away because discarded reports can be retrieved from trash bins.

AIS AT WORK
Biometrics Are Opening Many Eyes[16]

Databases are one of the most critical assets of any Global 2000 enterprise and are often overlooked by managers when assessing and ensuring the appropriate levels of IT security. An increasing number of serious attacks by hackers and viruses, and the frequent security-related patches and service packs, continue to vex security and database administrators. And no wonder! A perfect example of this is the Internet Crash in 2003 that we discussed in Chapter 10. The attacker was able to achieve such widespread havoc by taking advantage of a weakness in Microsoft's SQL Server 2000 software. According to Davoll at PentaSafe, ''What we are seeing from customers is that while they are methodically locking down operating systems and Web servers, they are not consistently taking the same steps to secure their underlying databases.''

A variety of integrated security solutions are available that specifically address the security issues that concern database security managers. These include vulnerability assessments, database auditing, and intrusion protection through passwords and biometrics.

United Bankers' Bank (UBB) is one of the largest banks in the Federal Reserve's 9th District, with more than 1,200 community banks. After a considerable amount of investigation into various biometric options, UBB determined that fingerprint authentication was the most trusted, practical, and affordable. In 2004, UBB changed to fingerprint authentication to eliminate the hassles and security vulnerabilities associated with employee and customer-driven password management. The fingerprint system is used to authenticate employees' entry into the bank as they arrive in the morning and to access other applications during their workday.

Attacks on databases can (and do) occur from both inside and outside the company's firewalls. Biometrics can be used in conjunction with other security measures to help protect databases. After all, even Kevin Mitnick (probably still the most widely known hacker in the U.S.) is quick to point out that the end-user is the weakest link in the security chain.

[16]Sources: ''Biometrics are Opening Many Eyes,'' *Banking Wire* (2004) Vol. 8, p.54. ''PentaSafe Extends Database Security to Microsoft SQL Server,'' *PR Newswire* (November 5, 2002).

SUMMARY

- Firms are using an integrated approach to security by combining a number of technologies, including: firewalls, intrusion detection systems, content filtering, vulnerability management, virus protection, and virtual private networks.
- An integrated security system, supported by a comprehensive security policy, can significantly reduce the risk of attack because it increases the costs and resources needed by an intruder.
- Organization-level controls are so important because they often have a pervasive impact on many other controls, such as IT general controls and application-level controls.
- At the organization level, examples of important controls are: management's ethical values, philosophy, assignment of authority and responsibility, and the effectiveness of the board of directors.
- In addition, senior management must have controls over human resources and data resources. These controls include: (1) personnel policies; (2) file security controls; (3) business continuity planning; (4) computer facility controls; and (5) computer access controls.
- Business continuity planning and management are becoming an organization-level concern due to the many natural disasters and other business disruptions over the recent past.
- IT general controls are controls that are embedded in IT processes and are applied to all IT service activities. These controls are critical for reliance on application controls.
- Organizations are increasingly relying on wireless networks and must recognize the need for a virtual private network (VPN) so that users may safely access entity data and other online resources.
- Due to increased mobility of employees, organizations must also develop controls for laptop computers to protect those assets as well as the data that resides on them.
- At the transaction processing level, application controls are critical for preventing, detecting, and correcting errors and irregularities.
- Three major types of application controls are: (1) input controls, (2) processing controls, and (3) output controls.

KEY TERMS YOU SHOULD KNOW

application controls
backup
batch control total
biometric identifications
business continuity plan (BCP)
checkpoint
cold backup
cold site
computer facility controls
consensus-based protocols
control environment
data encryption
data manipulation controls
disaster recovery
disk mirroring
disk shadowing
edit programs
edit tests
electronic eavesdropping
electronic vaulting
fault-tolerant systems
flying-start site
hash total
hot backup
hot site
input controls
input validation routines
integrated security
IT general controls
logical security
man trap
message acknowledgment procedures
organization-level controls
output controls
physical security
processing controls

red flags
rollback processing
routing verification procedures
security policy
strong passwords
uninterruptible power system (UPS)
watchdog processor
virtual private network (VPN)

TEST YOURSELF

Q12-1. A _____ is a comprehensive plan that helps protect the enterprise from internal and external threats.
a. Firewall **b**. Security policy **c**. Risk assessment **d**. VPN

Q12-2. According to PCAOB Standard No. 2, which of the following is an example of a company-level control?
a. Controls to monitor results of operations **c**. Access to computer files
b. Personnel controls **d**. All of the above

Q12-3. Fault-tolerant systems are designed to tolerate computer errors and are built on the concept of _____.
a. Redundancy **c**. COSO
b. COBIT **d**. Integrated security

Q12-4. A _____ site is a disaster recovery site that includes a computer system like the one the company regularly uses, software, and up-to-date data so the company can resume full data processing operations within seconds or minutes.
a. Hot **b**. Cold **c**. Flying-start **d**. Backup

Q12-5. Disaster recovery plans may not be of much use if _____.
a. They are not fully documented
b. The organization does not have a cold site for relocation purposes
c. The organization does not expect any natural disasters to occur
d. They are not tested periodically and revised when necessary

Q12-6. Which of the following is not a computer facility control?
a. Place the data processing center where unauthorized individuals cannot gain entry
b. Limit access to the data processing center to all employees of the company
c. Buy insurance to protect against loss of equipment in a computer facility
d. Use advanced technology to identify individuals who are authorized access to the data processing center

Q12-7. A _____ is a security appliance that runs behind a firewall and allows remote users to access entity resources by using wireless, hand-held devices.
a. Data encryption **c**. Checkpoint
b. WAN **d**. VPN

Q12-8. Organizations use _____ controls to prevent, detect, and correct errors and irregularities in transactions that are processed.
a. Specific **b**. General **c**. Application **d**. Input

Q12-9. All of the following are considered organization-level controls except:
a. Personnel controls
b. Business continuity planning controls
c. Processing controls
d. Access to computer files

DISCUSSION QUESTIONS

12-1. What is a security policy? What do we mean when we say organizations should have an integrated security plan?

12-2. What do we mean when we talk about convergence of physical and logical security? Why might this be important to an organization?

12-3. What guidance or framework would you use to establish IT governance if you were a senior executive in a firm? If you were a mid-level IT manager who was designing IT general controls? A manager who was responsible for identifying the appropriate application controls?

12-4. Discuss the major differences between wireless LANs and hard-wired LANs. What controls must be used to protect data that is transmitted over these networks?

12-5. Why is business continuity planning so important? What is it? Identify several reasons why testing the plan is a good idea.

12-6. What is backup, and why is it important when operating an accounting system?

12-7. Discuss some of the unique control risks associated with the use of PCs and laptop computers compared to using mainframes. List what you consider to be three of the most important control procedures that should be implemented for PCs. For each control procedure, give your reason for including this procedure as an important control.

12-8. Jean & Joan Cosmetics has a complete line of beauty products for women and maintains a computerized inventory system. An eight-digit product number identifies inventory items, of which the first four digits classify the beauty product by major category (hair, face, skin, eyes, etc.) and the last four digits identify the product itself. Identify as many controls as you can that the company might use to ensure accuracy in this eight-digit number when updating its inventory-balance file.

12-9. Explain how each of the following can be used to control the input, processing, or output of accounting data: (a) edit tests, (b) check digits, (c) passwords, (d) activity listings, and (e) control totals.

12-10. What is the difference between *logical* access to the computer and *physical* access to the computer? Why is the security of both important?

12-11. Discuss the following statement: ''The separation of duties control is very difficult in computerized accounting information systems because computers often integrate functions when performing data processing tasks. Therefore, such a control is not advisable for those organizations using computers to perform their accounting functions.''

12-12. Discuss the role of the *control total* in accounting information systems. Why are control totals insufficient to guard against data inaccuracies?

PROBLEMS

12-13. E. Wilson & Sons, Inc. hired a consulting team from Chesapeake and Associates to discuss application controls for the company's accounting data processing. In one of the workshops, the seminar leader stated, ''We can classify all errors in processing accounting data as either accidental or intentional. Controls such as edit tests are primarily aimed at the former type of error, whereas personnel controls are primarily aimed at the latter type of error.'' Comment.

12-14. Mark Goodwin, a computer programmer, had a grudge against his company. To get even, he coded a special routine in the mortgage loan program that erased a small, random number of accounts on the disk file every time the program was run. The company did not detect the routine until almost all of its records had been erased. Discuss what controls might have protected this company from its own programmer.

12-15. Jack Drucker, an accountant working for a medium-size company, set up several dummy companies and began directing the computer to write checks to them for fictitious merchandise. He was apprehended only when several of the company executives began to wonder how he could afford a ski vacation in the Alps every year. What controls might have prevented this fraudulent activity?

12-16. Identify one or more *control procedures* (either *general* or *application* controls, or both) that would guard against each of the following errors or problems.

a. Leslie Thomas, a secretary at the university, indicated that she had worked 40 hours on her regular time card. The university paid her for 400 hours worked that week.

b. The aging analysis indicated that the Grab and Run Electronics Company account was so far in arrears that the credit manager decided to cut off any further credit sales to the company until it cleared up its account. Yet, the following week, the manager noted that three new sales had been made to that company—all on credit.

c. The Small Company employed Mr. Fineus Eyeshade to perform all its accounts receivable data processing. Mr. Eyeshade's 25 years with the company and his unassuming appearance helped him conceal the fact that he was embezzling cash collections from accounts receivable to cover his gambling losses at the racetrack.

d. The Blue Mountain Utility Company was having difficulty with its customer payments. The payment amounts were entered directly onto a terminal, and the transaction file thus created was used to update the customer master file. Among the problems encountered with this system were the application of customer payments to the wrong accounts and the creation of multiple customer master file records for the same account.

e. The Landsford brothers had lived in Center County all their lives. Ben worked for the local mill in the accounts payable department, and Tom owned the local hardware store. The sheriff couldn't believe that the brothers had created several dummy companies that sold fictitious merchandise to the mill. Ben had the mill pay for this merchandise in its usual fashion, and he wrote off the missing goods as ''damaged inventory.''

12-17. Identify one or more *control procedures* (either *general* or *application* controls, or both) that would guard against each of the following errors or problems.

a. A bank deposit transaction was accidentally coded with a withdrawal code.

b. The key-entry operator keyed in the purchase order number as a nine-digit number instead of an eight-digit number.

c. The date of a customer payment was keyed 2001 instead of 2010.

d. A company employee was issued a check in the amount of $135.65 because he had not worked a certain week, but most of his payroll deductions were automatic each week.

e. A patient filled out her medical insurance number as 123465 instead of 123456.

f. An applicant for the company stock option plan filled out her employee number as 84-7634-21. The first two digits are a department code. There is no department 84.

g. A high school student was able to log onto the telephone company's computer as soon as he learned what telephone number to call.

h. The accounts receivable department sent 87 checks to the computer center for processing. No one realized that one check was dropped along the way and that the computer therefore processed only 86 checks.

12-18. To achieve effective separation of duties within a company's IT environment, the company's accounting and information processing subsystems should be separate from the departments that use data and perform operational activities. Discuss some of the ways this ''separation of duties'' is achieved.

12-19. Bristol Company has a high turnover rate among its employees. It maintains a very large computer system that supports approximately 225-networked PCs. The company maintains fairly extensive databases regarding its customers. These databases include customer profiles,

Application	Field Name	Field Length	Example
Invoicing	Customer number	6	123456
	Customer name	23	Al's Department Store
	Salesperson number	3	477
	Invoice number	6	123456
	Item catalog number	10	9578572355
	Quantity sold	8	13
	Unit price	7	10.50
	Total price	12	136.50
Salesperson activity	Salesperson number	3	477
	Salesperson name	20	Kathryn Wilson
	Store department number	8	10314201
	Week's sales volume	12	1043.75
	Regular hours worked	5	39.75
	Overtime hours worked	4	0.75
Inventory control	Inventory item number	10	9578572355
	Item description	15	Desk lamp
	Unit cost	7	8.50
	Number of units dispersed this week	4	14
	Number of units added to inventory	4	20
Purchasing	Vendor catalog number	12	059689584996
	Item description	18	Desk pad
	Vendor number	10	8276110438
	Number of units ordered	7	45
	Price per unit	7	8.75
	Total cost of purchase	14	313.75

FIGURE 12-17 Data for the Blatz Furniture Company's applications.

past purchasing patterns, and prices charged. Recently, Bristol Company has been having major problems with competitors. It appears that one competitor seems to be very effective at taking away the company's customers. This competitor has visited most of Bristol Company's customers, and identical products have been offered to these customers at lower prices in every case.

a. What do you feel is the possible security problem at Bristol Company?

b. What can be done about this problem?

12-20. The Blatz Furniture Company uses an online data input system for processing its sales invoice data, salesperson data, inventory control, and purchase order data. Representative data for each of these applications are shown in Figure 12-17. Identify specific editing tests that might be used to ensure the accuracy and completeness of the information in each data set.

CASE ANALYSES

12-21. Simmons Corporation (Problems with Computer-based Information System)

Simmons Corporation is a multi-location retailing concern with stores and warehouses throughout the United States. The company is in the process of designing a new, integrated, computer-based information system. In conjunction with the design of the new system,

the management of the company is reviewing the data processing security to determine what new control features should be incorporated. Two areas of specific concern are (1) confidentiality of company and customer records, and (2) safekeeping of computer equipment, files, and data processing center facilities.

The new information system will be employed to process all company records, which include sales, purchases, the financial budget, customer, creditor, and personnel information. The stores and warehouses will be linked to the main computer at corporate headquarters by a system of remote terminals. This will permit data to be communicated directly to corporate headquarters or to any other location from each location within the terminal network.

At the current time, certain reports have restricted distribution because not all levels of management need to receive them or because they contain confidential information. The introduction of remote terminals in the new system may provide access to these restricted data by unauthorized personnel. Simmons's top management is concerned that confidential information may become accessible and be used improperly.

The company's top management is also concerned with potential physical threats to the system, such as sabotage, fire damage, water damage, or power failure. Should any of these events occur in the current system and cause a computer shutdown, adequate backup records are available so that the company could reconstruct necessary information at a reasonable cost on a timely basis. However, with the new system, a computer shutdown would severely limit company activities until the system could become operational again.

Requirements:

1. Identify and briefly explain the problems Simmons Corporation could experience with respect to the confidentiality of information and records in the new system.
2. Recommend measures Simmons Corporation could incorporate into the new system that would ensure the confidentiality of information and records in this new system.
3. What safeguards can Simmons Corporation develop to provide physical security for its (a) computer equipment, (b) files, and (c) data processing center facilities?

12-22. MailMed Inc. (Control Weaknesses and a Disaster Recovery Plan)

MailMed Inc. (MMI), a pharmaceutical firm, provides discounted prescription drugs through direct mail. MMI has a small systems staff that designs and writes MMI's customized software. Until recently, MMI's transaction data were transmitted to an outside organization for processing on its hardware.

MMI has experienced significant sales growth as the cost of prescription drugs has increased and medical insurance companies have been tightening reimbursements in order to restrain premium cost increases. As a result of these increased sales, MMI has purchased its own computer hardware. The data processing center is installed on the ground floor of its two-story headquarters building. It is behind large, plate-glass windows so that the state-of-the-art data processing center can be displayed as a measure of the company's success and attract customer and investor attention. The computer area is equipped with halon gas fire suppression equipment and an uninterruptible power supply system.

MMI has hired a small computer operations staff to operate its data processing center. To handle MMI's current level of business, the operations staff is on a two-shift schedule, five days per week. MMI's systems and programming staff, now located in the same building, has access to the data processing center and can test new programs and program changes

when the operations staff is not available. Because the systems and programming staff is small and the work demands have increased, systems and programming documentation is developed only when time is available. Periodically, but not on a scheduled basis, MMI backs up its programs and data files, storing them at an off-site location.

Unfortunately, due to several days of heavy rains, MMI's building recently experienced serious flooding that reached several feet into the first-floor level and affected not only the computer hardware but also the data and program files that were on-site.

Requirements:

1. Describe at least four computer control weaknesses that existed at MailMed Inc. prior to the flood occurrence.
2. Describe at least five components that should be incorporated in a formal disaster recovery plan so that MailMed Inc. can become operational within 72 hours after a disaster affects its computer operations capability.
3. Identify at least three factors, other than the plan itself, that MailMed Inc.'s management should consider in formulating a formal disaster recovery plan.

12-23. Bad Bad Benny: A True Story (Identifying Controls for a System)[17]

In the early twentieth century, there was an ambitious young man named Arthur who started working at a company in Chicago as a mailroom clerk. He was a hard worker and very smart, eventually ending up as the president of the company, the James H. Rhodes Company. The firm produced steel wool and harvested sea sponges in Tarpon Springs, Florida for household and industrial use. The company was very successful, and Arthur decided that the best way to assure the continued success of the company was to hire trusted family members for key management positions—because you can always count on your family. Arthur decided to hire his brother Benny to be his Chief Financial Officer (CFO), and placed other members of the family in key management positions. He also started his eldest son, Arthur Junior (an accountant by training) in a management training program, hoping that he would eventually succeed him as president.

As the company moved into the 1920s, Benny was a model employee; he worked long hours, never took vacations, and made sure that he personally managed all aspects of the cash function. For example, he handled the entire purchasing process—from issuing purchase orders through the disbursement of cash to pay bills. He also handled the cash side of the revenue process by collecting cash payments, preparing the daily bank deposits, and reconciling the monthly bank statement.

The end of the 1920s saw the United States entering its worst Depression since the beginning of the Industrial Age. Because of this, Arthur and other managers did not get raises, and in fact, took pay cuts to keep the company going and avoid lay-offs. Arthur and other top management officials made ''lifestyle'' adjustments as well—e.g., reducing the number of their household servants and keeping their old cars, rather than purchasing new ones. Benny, however, was able to build a new house on the shore of Lake Michigan and purchased a new car. He dressed impeccably and seemed impervious to the economic downturn. His family continued to enjoy the theatre, new cars, and nice clothes.

[17]Source: Professor Constance Lehmann, Department of Accounting, University of Houston-Clear Lake.

Arthur's wife became suspicious of Benny's good fortune in the face of others' hardships, so she and Arthur hired an accountant to review the books. External audits were not yet required for publicly-held companies, and the Securities and Exchange Commission (SEC) had not yet been formed (that would happen in 1933–1934). Jim the accountant was eventually able to determine that Benny had diverted company funds to himself by setting up false vendors and having checks mailed to himself. He also diverted some of the cash payments received from customers and was able to hide it by handling the bank deposits and the reconciliation of the company's bank accounts. Eventually, Jim determined that Benny had embezzled about $500,000 (in 1930 dollars).

If we assume annual compounding of 5% for 72 years, the value in today's dollars would be about $17.61 million! Arthur was furious, and sent Benny ''away.'' Arthur sold most of his personal stock holdings in the company to repay Benny's embezzlement, which caused him to lose his controlling interest in the company, and eventually was voted out of office by the Board of Directors.

Jim, the accountant, wrote a paper about his experience with Benny (now referred to as ''Bad Bad Benny'' by the family). Jim's paper contributed to the increasing call for required annual external audits for publicly-held companies. Arthur eventually reestablished himself as a successful stockbroker and financial planner. Benny ''disappeared'' and was never heard from again.

Requirements:

1. Identify the control weaknesses in the revenue and purchasing processes.
2. Identify any general controls Arthur should have implemented to help protect the company.
3. From Chapter 11, identify the internal control activities that Arthur should have considered (or implemented) that would have thwarted Benny's bad behavior.

REFERENCES AND RECOMMENDED READINGS

Aldhizer, G. ''The Insider Threat,'' *Internal Auditor* (April 2008), pp. 71–73.

Anonymous. ''NIST Calls for Comments on Draft of Federal Computer Security Controls Guidelines,'' *M2 Presswire*, November 4, 2003.

Campbell, D., M. Campbell, & G. Adams. ''Adding Significant Value with Internal Controls,'' *The CPA Journal* (June 2006), pp. 20–25.

Cleary, B. ''How Safe is Your Data?'' *Strategic Finance* (October 2008), pp. 33–37.

COBIT, version 4.1 at: http://www.isaca.org.

Contos, B. ''The Convergence of Logical and Physical Security Solutions,'' *IT Defense* (August 2006), pp. 24–26.

Cook, L. ''IT control objectives for Sarbanes-Oxley: New guidance on IT control and compliance,'' (October 31, 2003) at wwww.deloitte.com.

Heffes, E. ''Hurricane Season 2006 is Approaching. Are you Ready?'' *Financial Executive* (April 2006), pp. 27–30.

Jensen, J. & C. Power. ''Treasury's Role in Planning for the Worst-Case Scenario: Business Continuity Planning,'' *Financial Executive* (June 2006), p 60.

Mameli, P. ''Protection Management: An Integrated Approach to Homeland Security,'' *The Public Manager* (Summer 2005), pp. 27–31.

Phelan, S. & M. Hayes. ''Before the Deluge—and After'' *Journal of Accountancy* (April 2003), pp. 57–63.

Pugliese, A. & A. Kendal. ''Support for CPAs in Post-Disaster Work,'' *Journal of Accountancy* (February 2004), pp. 19–21.

Siegel, J., M. Levine, & R. Siegel. ''Security safeguards over Wireless Networks,'' *The CPA Journal* (June 2004), pp. 68–70.

Vijayan, Jaikumar. ''Oracle adds ID Security to Database,'' *Computerworld* (2003), p. 14.

Wade, J. ''The Weak Link in IT Security,'' *Risk Management* (July 2004), pp. 32–36.

ANSWERS TO TEST YOURSELF

1. **b** 2. **a** 3. **a** 4. **c** 5. **d** 6. **b** 7. **d** 8. **c** 9. **c**