Chapter 10

Information Systems Controls for Systems Reliability—Part 3: Processing Integrity and Availability

Learning Objectives

After studying this chapter, you should be able to:

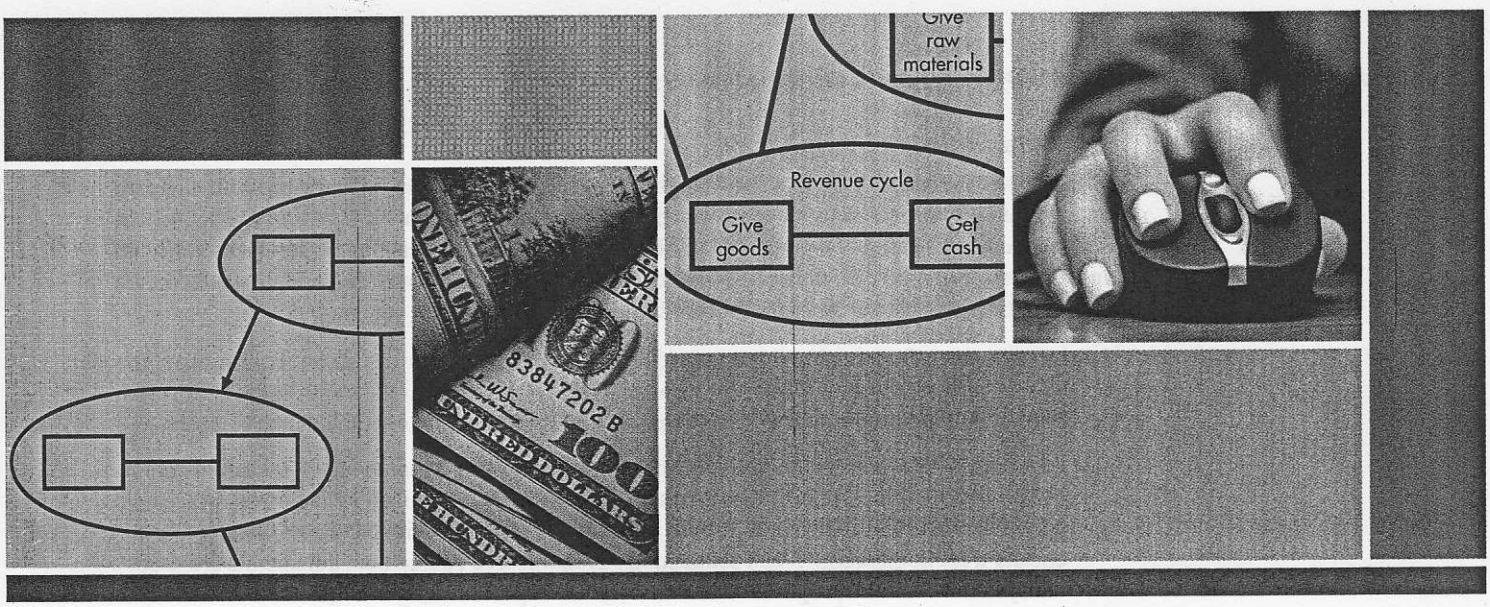
1. Identify and explain controls designed to ensure processing integrity.
2. Identify and explain controls designed to ensure systems availability.

INTEGRATIVE CASE NORTHWEST INDUSTRIES

Jason Scott began his review of Northwest Industries' processing integrity and availability controls by meeting with the CFO and the CIO. The CFO mentioned that she had just read an article about how spreadsheet errors had caused several companies to make poor decisions that cost them millions of dollars. She wanted to be sure that such problems did not happen to Northwest Industries. She also stressed the need to continue to improve the monthly closing process so that management would have more timely information. The CIO expressed concern about the company's lack of planning for how to continue business operations in the event of a major natural disaster such as the recent floods in the Midwest, which had forced several small businesses to close. Jason thanked them for their input and set about collecting evidence about the effectiveness of Northwest Industries' procedures for ensuring processing integrity and availability.

Introduction

The previous two chapters discussed the first three principles of systems reliability identified in the Trust Services Framework: security, confidentiality, and privacy. This chapter addresses the remaining two principles of reliable systems: processing integrity and availability. We conclude with a discussion of the importance of controlling changes to systems to ensure that the



new system continues to satisfy all five principles of systems reliability identified in the Trust Services Framework.

Processing Integrity

The Processing Integrity principle of the Trust Services Framework states that a reliable system is one that produces information that is accurate, complete, timely, and valid. As discussed in COBIT control objective DS 11.1, this requires controls over the input, processing, and output of data. Table 10-1 presents the six basic categories of application controls discussed in the COBIT framework for ensuring processing integrity.

TABLE 10-1 Application Controls Discussed in COBIT to Ensure Processing Integrity

Process Stage and COBIT Category	Threats/Risks	Controls
Input: • AC1—Source Data Preparation and Authorization • AC2—Source Data Collection and Entry • AC3—Accuracy, Completeness, and Authenticity Checks	Data that is: • Invalid • Unauthorized • Incomplete • Inaccurate	Forms design, cancellation and storage of documents, authorization and segregation of duties controls, visual scanning, data entry controls
Processing: • AC4—Processing Integrity and Validity	Errors in output and stored data	Data matching, file labels, batch totals, cross-footing and zero-balance tests, write-protection mechanisms, database processing integrity controls
Output: • AC5—Output Review, Reconciliation and Error Handling • AC6—Transaction Authenticity and Integrity	• Use of inaccurate or incomplete reports • Unauthorized disclosure of sensitive information • Loss, alteration, or disclosure of information in transit	Reviews and reconciliations, encryption and access controls, parity checks, message acknowledgement techniques

Input Controls

The phrase "garbage in, garbage out" highlights the importance of input controls. If the data entered into a system are inaccurate, incomplete, or invalid, the output will be too. Consequently, source documents should be prepared only by authorized personnel acting within their authority. In addition, forms design, cancellation and storage of source documents, and automated data entry controls are needed to verify the validity of input data.

FORMS DESIGN Source documents and other forms should be designed to minimize the chances for errors and omissions. Two particularly important forms design controls involve sequentially prenumbering source documents and using turnaround documents.

1. All source documents should be sequentially prenumbered. Prenumbering improves control by making it possible to verify that no documents are missing. (To understand this, consider the difficulty you would have in balancing your checking account if none of your checks were numbered.) When sequentially prenumbered source data documents are used, the system should be programmed to identify and report missing or duplicate source documents.
2. A ***turnaround document*** is a record of company data sent to an external party and then returned by the external party to the system as input. Turnaround documents are prepared in machine-readable form to facilitate their subsequent processing as input records. An example is a utility bill that a special scanning device reads when the bill is returned with a payment. Turnaround documents improve accuracy by eliminating the potential for input errors when entering data manually.

CANCELLATION AND STORAGE OF SOURCE DOCUMENTS Source documents that have been entered into the system should be canceled so they cannot be inadvertently or fraudulently reentered into the system. Paper documents should be defaced, for example, by stamping them "paid." Electronic documents can be similarly "canceled" by setting a flag field to indicate that the document has already been processed. *Note:* Cancellation does *not* mean disposal. Original source documents (or their electronic images) should be retained for as long as needed to satisfy legal and regulatory requirements and provide an audit trail.

DATA ENTRY CONTROLS Source documents should be scanned for reasonableness and propriety before being entered into the system. However, this manual control must be supplemented with automated data entry controls, such as the following:

- A ***field check*** determines whether the characters in a field are of the proper type. For example, a check on a field that is supposed to contain only numeric values, such as a U.S. Zip code, would indicate an error if it contained alphabetic characters.
- A ***sign check*** determines whether the data in a field have the appropriate arithmetic sign. For example, the quantity-ordered field should never be negative.
- A ***limit check*** tests a numerical amount against a fixed value. For example, the regular hours-worked field in weekly payroll input must be less than or equal to 40 hours. Similarly, the hourly wage field should be greater than or equal to the minimum wage.
- A ***range check*** tests whether a numerical amount falls between predetermined lower and upper limits. For example, a marketing promotion might be directed only to prospects with incomes between $50,000 and $99,999.
- A ***size check*** ensures that the input data will fit into the assigned field. For example, the value 458,976,253 will not fit in an eight-digit field.
- A ***completeness check*** on each input record determines whether all required data items have been entered. For example, sales transaction records should not be accepted for processing unless they include the customer's shipping and billing addresses.
- A ***validity check*** compares the ID code or account number in transaction data with similar data in the master file to verify that the account exists. For example, if product number 65432 is entered on a sales order, the computer must verify that there is indeed a product 65432 in the inventory database.
- A ***reasonableness test*** determines the correctness of the logical relationship between two data items. For example, overtime hours should be zero for someone who has not worked the maximum number of regular hours in a pay period.

- Authorized ID numbers (such as employee numbers) can contain a ***check digit*** that is computed from the other digits. For example, the system could assign each new employee a nine-digit number, then calculate a tenth digit from the original nine and append that calculated number to the original nine to form a ten-digit ID number. Data entry devices can then be programmed to perform ***check digit verification*** by using the first nine digits to calculate the tenth digit each time an ID number is entered. If an error is made in entering any of the ten digits, the calculation made on the first nine digits will not match the tenth, or check digit.

The preceding data entry tests are used for both batch processing and online real-time processing. Additional data input controls differ for the two processing methods.

ADDITIONAL BATCH PROCESSING DATA ENTRY CONTROLS

- Batch processing works more efficiently if the transactions are sorted so that the accounts affected are in the same sequence as records in the master file. For example, accurate batch processing of sales transactions to update customer account balances requires that the transactions first be sorted by customer account number. A ***sequence check*** tests whether a batch of input data is in the proper numerical or alphabetical sequence.
- An error log that identifies data input errors (date, cause, problem) facilitates timely review and resubmission of transactions that cannot be processed.
- ***Batch totals*** summarize important values for a batch of input records. The following are three commonly used batch totals:
  1. A ***financial total*** sums a field that contains monetary values, such as the total dollar amount of all sales for a batch of sales transactions.
  2. A ***hash total*** sums a nonfinancial numeric field, such as the total of the quantity ordered field in a batch of sales transactions.
  3. A ***record count*** is the number of records in a batch.

These batch totals are calculated and stored by the system when data is initially entered. They will be recalculated later to verify that all input was processed correctly.

ADDITIONAL ONLINE DATA ENTRY CONTROLS

- ***Prompting***, in which the system requests each input data item and waits for an acceptable response, ensures that all necessary data are entered (i.e., prompting is an online completeness check).
- ***Closed-loop verification*** checks the accuracy of input data by using it to retrieve and display other related information. For example, if a clerk enters an account number, the system could retrieve and display the account name so that the user could verify that the correct account number had been entered.
- A transaction log includes a detailed record of all transactions, including a unique transaction identifier, the date and time of entry, and who entered the transaction. If an online file is damaged, the transaction log can be used to reconstruct the file. If a malfunction temporarily shuts down the system, the transaction log can be used to ensure that transactions are not lost or entered twice.

Processing Controls

Controls are also needed to ensure that data is processed correctly. Important processing controls include the following:

- ***Data matching.*** In certain cases, two or more items of data must be matched before an action can take place. For example, before paying a vendor, the system should verify that information on the vendor invoice matches information on both the purchase order and the receiving report.
- ***File labels.*** File labels need to be checked to ensure that the correct and most current files are being updated. Both external labels that are readable by humans and internal labels that are written in machine-readable form on the data recording media should be used. Two important types of internal labels are header and trailer records. The ***header record*** is located at the beginning of each file and contains the file name, expiration date, and other

identification data. The ***trailer record*** is located at the end of the file and contains the batch totals calculated during input. Programs should be designed to read the header record *prior* to processing, to ensure that the correct file is being updated. Programs should also be designed to read the information in the trailer record *after* processing, to verify that all input records have been correctly processed.

- ***Recalculation of batch totals.*** Batch totals should be recomputed as each transaction record is processed, and the total for the batch should then be compared to the values in the trailer record. Any discrepancies indicate a processing error. Often, the nature of the discrepancy provides a clue about the type of error that occurred. For example, if the recomputed record count is smaller than the original, one or more transaction records were not processed. Conversely, if the recomputed record count is larger than the original, either additional unauthorized transactions were processed, or some transaction records were processed twice. If a financial or hash total discrepancy is evenly divisible by 9, the likely cause is a ***transposition error***, in which two adjacent digits were inadvertently reversed (e.g., 46 instead of 64). Transposition errors may appear to be trivial but can have enormous financial consequences. For example, consider the effect of misrecording the interest rate on a loan as 6.4% instead of 4.6%.
- ***Cross-footing and zero-balance tests.*** Often totals can be calculated in multiple ways. For example, in spreadsheets a grand total can be computed either by summing a column of row totals or by summing a row of column totals. These two methods should produce the same result. A ***cross-footing balance test*** compares the results produced by each method to verify accuracy. A ***zero-balance test*** applies this same logic to control accounts. For example, the payroll clearing account is debited for the total gross pay of all employees in a particular time period. It is then credited for the amount of all labor costs allocated to various expense categories. The payroll clearing account should have a zero balance after both sets of entries have been made; a nonzero balance indicates a processing error.
- ***Write-protection mechanisms.*** These protect against overwriting or erasing of data files stored on magnetic media. Write-protection mechanisms have long been used to protect master files from accidentally being damaged. Technological innovations also necessitate the use of write-protection mechanisms to protect the integrity of transaction data. For example, radio frequency identification (RFID) tags used to track inventory need to be write-protected so that unscrupulous customers cannot change the price of merchandise.
- ***Concurrent update controls.*** Errors can occur when two or more users attempt to update the same record simultaneously. ***Concurrent update controls*** prevent such errors by locking out one user until the system has finished processing the transaction entered by the other.

Output Controls

Careful checking of system output provides additional control over processing integrity. Important output controls include the following:

- ***User review of output.*** Users should carefully examine system output to verify that it is reasonable, that it is complete, and that they are the intended recipients.
- ***Reconciliation procedures.*** Periodically, all transactions and other system updates should be reconciled to control reports, file status/update reports, or other control mechanisms. In addition, general ledger accounts should be reconciled to subsidiary account totals on a regular basis. For example, the balance of the inventory control account in the general ledger should equal the sum of the item balances in the inventory database. The same is true for the accounts receivable, capital assets, and accounts payable control accounts.
- ***External data reconciliation.*** Database totals should periodically be reconciled with data maintained outside the system. For example, the number of employee records in the payroll file can be compared with the total number of employees in the human resources database to detect attempts to add fictitious employees to the payroll database. Similarly, inventory on hand should be physically counted and compared to the quantity on hand recorded in the database.

- *Data transmission controls.* Organizations also need to implement controls designed to minimize the risk of data transmission errors. Whenever the receiving device detects a data transmission error, it requests the sending device to retransmit that data. Generally, this happens automatically, and the user is unaware that it has occurred. For example, the Transmission Control Protocol (TCP) discussed in Chapter 8 assigns a sequence number to each packet and uses that information to verify that all packets have been received and to reassemble them in the correct order. Two other common data transmission controls are checksums and parity bits.
  1. *Checksums.* When data are transmitted, the sending device can calculate a hash of the file, called a ***checksum***. The receiving device performs the same calculation and sends the result to the sending device. If the two hashes agree, the transmission is presumed to be accurate. Otherwise, the file is resent.
  2. *Parity bits.* Computers represent characters as a set of binary digits called bits. Each bit has two possible values: 0 or 1. Many computers use a seven-bit coding scheme, which is more than enough to represent the 26 letters in the English alphabet (both upper- and lowercase), the numbers 0 through 9, and a variety of special symbols ($, %, &, etc.). A **parity bit** is an extra digit added to the beginning of every character that can be used to check transmission accuracy. Two basic schemes are referred to as *even parity* and *odd parity*. In even parity, the parity bit is set so that each character has an even number of bits with the value 1; in odd parity, the parity bit is set so that an odd number of bits in the character have the value 1. For example, the digits 5 and 7 can be represented by the seven-bit patterns 0000101 and 0000111, respectively. An even parity system would set the parity bit for 5 to 0, so that it would be transmitted as 00000101 (because the binary code for 5 already has two bits with the value 1). The parity bit for 7 would be set to 1 so that it would be transmitted as 10000111 (because the binary code for 7 has 3 bits with the value 1). The receiving device performs **parity checking**, which entails verifying that the proper number of bits are set to the value 1 in each character received.

Illustrative Example: Credit Sales Processing

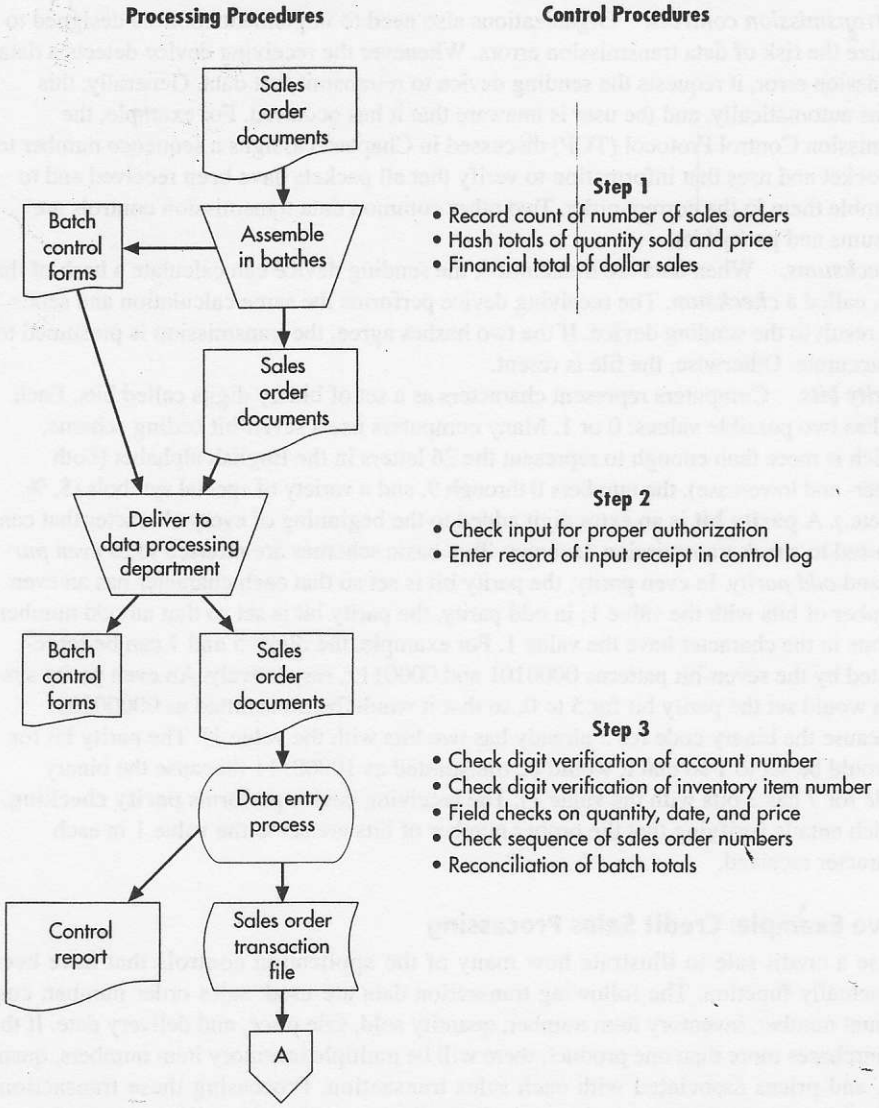
We now use a credit sale to illustrate how many of the application controls that have been discussed actually function. The following transaction data are used: sales order number, customer account number, inventory item number, quantity sold, sale price, and delivery date. If the customer purchases more than one product, there will be multiple inventory item numbers, quantities sold, and prices associated with each sales transaction. Processing these transactions includes the following steps: (1) entering and editing the transaction data; (2) updating the customer and inventory records (the amount of the credit purchase is added to the customer's balance; for each inventory item, the quantity sold is subtracted from the quantity on hand); and (3) preparing and distributing shipping and/or billing documents. Examples for both batch and online processing are presented.

BATCH PROCESSING INTEGRITY CONTROLS Figure 10-1 shows the application controls that should be applied at each step of processing a batch of credit sales transactions:

1. *Prepare batch totals.* The sum of all sales amounts is calculated as a financial total and recorded on batch control forms that accompany each group of sales documents.
2. *Deliver the transactions to the computer operations department for processing.* Each batch is checked for proper authorization and recorded in a control log.
3. *Enter the transaction data into the system.* As data are entered, the system performs several preliminary validation tests. Check digit verification identifies transactions with invalid account numbers or invalid inventory item numbers. Field checks verify that the quantity ordered and price fields contain only numbers and that the date field follows the correct MM/DD/YYYY format. A sequence check on sales order numbers and reconciliation of the batch totals calculated in step 1 verifies that no transactions are missing.

   A control report lists all data entry errors. Data entry errors that occurred because an operator read a source document incorrectly or accidentally struck the wrong key can usually be corrected immediately after being detected. Incorrect source data, such as an

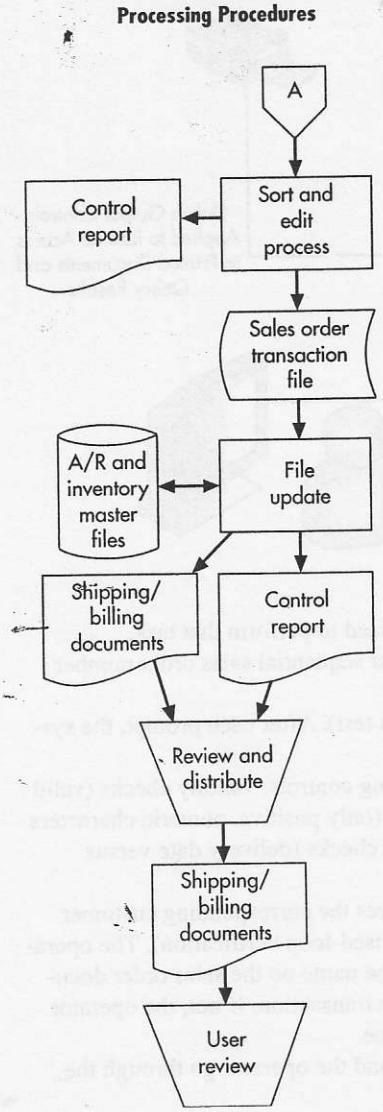
FIGURE 10-1
Application Controls in Batch Processing of Credit Sales



unauthorized sales transaction or an invalid account number, are more problematic and should be returned to the sales department for correction.

4. ***Sort and edit the transaction file.*** The transaction file is now sorted by customer account number. Additional validation checks are performed, including sign checks that both the quantity ordered and price fields contain positive numbers, and a range check on promised delivery dates to verify that it is not earlier than the date of the order nor later than the company's advertised policies. Rejected transactions are listed on a control report along with the computed batch totals. Data control reconciles the batch totals, investigates and corrects any errors, and submits the corrected transactions for processing.
5. ***Update the master files.*** The sales transaction file is processed against customer (accounts receivable) and inventory databases or master files. The operator reads the external label, and the program reads the internal header record to ensure that the correct master file is being updated. Sales transactions with customer numbers or item numbers that do not exist in the corresponding master file are not processed; instead, they are entered on an error report. After a sales transaction is processed, a sign check is performed to ensure that the quantity-on-hand field in the inventory master record is not negative. Tests are also performed to ensure that sales prices fall within normal ranges, that the order does not exceed the customer's credit limit, and that the quantity ordered is reasonable given the nature of the item and the customer's order history. Redundant data checks—for example, comparing inventory item number and description—are used to ensure that the correct master file

FIGURE 10-1 Continued



Control Procedures

Step 4

- Sequence check on account number
- Limit checks on quantity and price
- Range check on delivery date
- Completeness test on entire record
- Reconciliation of batch totals
- Review errors identified by edit checks
- Investigation and correction of erroneous input

Step 5

- Security of master files in file library
- Protection of master files with file labels
- Maintenance of backup copies of master files
- Validity check of customer account number
- Validity check of inventory item number
- Sign check of inventory quantity on hand
- Limit check of sale amount versus credit limit
- Range check on sale price
- Reasonableness test of quantity ordered
- Redundant data check on customer data
- Redundant data check on inventory data

Step 6

- Reconciliation of batch totals
- Review of errors identified by edit checks
- Investigation and correction of erroneous input
- Distribution of billing and shipping documents
- Recording of output distribution in control log
- Return of master files to file library

Step 7

- Visual inspection of output
- Reconciliation of batch totals

record is updated. The total change in customer balances is computed; this financial total is compared to the total sales amount of all transactions that were processed.

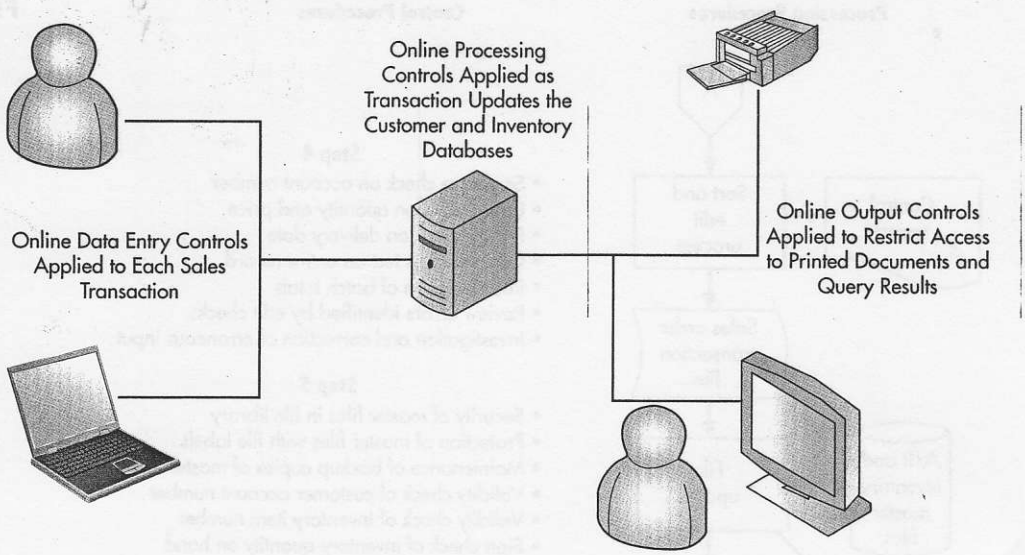
6. ***Prepare and distribute output.*** Outputs include billing and/or shipping documents and a control report. The control report contains batch totals accumulated during the file update run and a list of transactions rejected by the update program.
7. ***User review.*** Users in the shipping and billing departments perform a limited review of the documents for incomplete data or other obvious deficiencies. They also compare the system-generated batch totals to those calculated in step 1 to verify that all transactions were processed.

ONLINE PROCESSING INTEGRITY CONTROLS Online real-time processing records each credit sales transaction individually as it occurs (Figure 10-2). This enables more timely detection and correction of errors. The various application controls discussed in this chapter are applied at each stage (input, processing, output) of online transaction processing, as follows.

Online Data Entry Controls

- When an employee accesses the online system, logical access controls confirm the identity of the data entry device (personal computer, terminal) and the validity of the employee's user ID number and password.

FIGURE 10-2
Application Controls in Online Processing of Credit Sales



- A compatibility test ensures that the employee is authorized to perform that task.
- The system automatically assigns the transaction the next sequential sales order number and the current date as the date of the invoice.
- The system prompts for all required input (completeness test). After each prompt, the system waits for a response.
- Each response is tested using one or more of the following controls: validity checks (valid customer and inventory numbers), field and sign checks (only positive, numeric characters in the quantity, date, and price fields), and limit or range checks (delivery date versus current date).
- When the customer number is entered, the system retrieves the corresponding customer name from the database and displays it on the screen (closed-loop verification). The operator visually examines the customer name. If it matches the name on the sales order document, the operator signals the system to proceed with the transaction. If not, the operator rechecks the customer number and enters the correct value.
- When the inventory item number is entered, the system and the operator go through the same procedures as they do with the customer number.

Online Processing Controls. Because the file update program accesses the customer and inventory database records, it performs additional input validation tests by comparing data in each transaction record with data in the corresponding database record. These tests often include the following:

- Validity checks on the customer and inventory item numbers
- Sign checks on inventory-on-hand balances (after subtracting quantities sold)
- Limit checks that compare each customer's total amount due with the credit limit
- Range checks on the sale price of each item sold relative to the permissible range of prices for that item
- Reasonableness tests on the quantity sold of each item relative to normal sales quantities for that customer and that item

Online Output Controls. Outputs of this process include billing and/or shipping documents and a control report. The following output controls are used:

- Billing and shipping documents are forwarded electronically only to preauthorized users.
- Users in the shipping and billing departments perform a limited review of the documents by visually inspecting them for incomplete data or other obvious errors.
- The control report is sent automatically to its intended recipients, or the recipients can query the system for the report. If they query the system, logical access controls confirm the identity of the device making the query and the validity of the user's ID number and password.

FOCUS 10-1 Ensuring the Processing Integrity of Electronic Procurement Systems

Today many organizations implement and benefit from electronic procurement systems. Among these benefits are dramatic cost savings, which, studies by the European Committee indicate, can be as large as 40% to 75%.

To improve the efficiency and reliability of the procurement process, a large Dutch university implemented BasWare, an enterprise purchase-to-pay and financial management solution. The university processes approximately 10,000 invoices per month. However, most invoices are still received through the mail. These invoices are scanned and, by the use of an Optical Character Recognition technique, are automatically matched to a purchase order or a contract in the Financial Accounting and Controlling module of SAP (SAP FI/CO). After verifying that the recipient received the goods or services, the budget owner receives an e-mail asking him/her to verify and authorize the invoice within five working days. The budget owner has the ability to see the original invoice and can therefore easily authorize it. If the budget owner has not authorized the invoice within five days, BasWare resends the invoice to a substitute budget owner or a manager after seven days. After the invoice has been approved, BasWare generates a journal entry, which is entered automatically in SAP FI/CO. In turn, SAP FI/CO generates a weekly batch file. This file is imported by an online banking application, after which the financial manager and/or director can authorize the payment.

The university implemented a number of controls in the process to guarantee the processing integrity of their invoices. The legality of the payment and the archiving of the invoices were crucial elements in complying with the controls requirements of the European Commission and the local tax authorities. Key controls include the following:

- Segregation of duties (authorizations)
- Automated three-way match
- Automatic allocation of accounts in the general ledger and cost centers
- Data transmission controls between the different IT systems
- Write-protection of the scanned files and payment files

The preceding example illustrated the use of application controls to ensure the integrity of processing business transactions. Focus 10-1 explains the importance of processing integrity controls at a large Dutch university.

Processing Integrity Controls in Spreadsheets

Most organizations have thousands of spreadsheets that are used to support decision making. The importance of spreadsheets to financial reporting is reflected in the fact that the ISACA document *IT Control Objectives for Sarbanes-Oxley* contains a separate appendix that specifically addresses processing integrity controls that should be used in spreadsheets. Yet, because spreadsheets are almost always developed by end users, they seldom contain adequate application controls. Therefore, it is not surprising that many organizations have experienced serious problems caused by spreadsheet errors. For example, an August 17, 2007, article in *CIO Magazine*[1] describes how spreadsheet errors caused companies to lose money, issue erroneous dividend payout announcements, and misreport financial results.

These kinds of costly mistakes could have been prevented by careful testing of spreadsheets before use. Although most spreadsheet software contains built-in "audit" features that can easily detect common errors, spreadsheets intended to support important decisions need more thorough testing to detect subtle errors. Nevertheless, a survey of finance professionals[2] indicates that only 2% of firms use multiple people to examine every spreadsheet cell, which is the only reliable way to effectively detect spreadsheet errors. It is especially important to check for *hardwiring*, where formulas contain specific numeric values (e.g., sales tax = 8.5% × A33), instead of referencing a cell that contains the current value for that variable (e.g., sales tax = A8 × A33). The problem with hardwiring is that the spreadsheet initially produces correct answers, but when the hardwired variable (e.g., the sales tax rate in the preceding example) changes, the formula may not be corrected.

---

[1]Thomas Wailgum, "Eight of the Worst Spreadsheet Blunders," *CIO Magazine* (August 2007), available at www.cio.com/article/131500/Eight_of_the_Worst_Spreadsheet_Errors

[2]Raymond R. Panko, "Controlling Spreadsheets," *Information Systems Control Journal-Online* (2007): Volume 1. Accessible at www.isaca.org/publications

Availability

Interruptions to business processes due to the unavailability of systems or information can cause significant financial losses. Consequently, COBIT section DS 4 addresses the importance of ensuring that systems and information are available for use whenever needed. The primary objective is to minimize the risk of system downtime. It is impossible, however, to completely eliminate the risk of downtime. Therefore, organizations also need controls designed to enable quick resumption of normal operations after an event disrupts system availability. Table 10-2 summarizes the key controls related to these two objectives.

Minimizing Risk of System Downtime

Organizations can undertake a variety of actions to minimize the risk of system downtime. COBIT control objective DS 13.5 identifies the need for preventive maintenance, such as cleaning disk drives and properly storing magnetic and optical media, to reduce the risk of hardware and software failure. The use of redundant components provides ***fault tolerance***, which is the ability of a system to continue functioning in the event that a particular component fails. For example, many organizations use ***redundant arrays of independent drives (RAID)*** instead of just one disk drive. With RAID, data is written to multiple disk drives simultaneously. Thus, if one disk drive fails, the data can be readily accessed from another.

COBIT section DS 12 addresses the importance of locating and designing the data centers housing mission-critical servers and databases so as to minimize the risks associated with natural and human-caused disasters. Common design features include the following:

- Raised floors provide protection from damage caused by flooding.
- Fire detection and suppression devices reduce the likelihood of fire damage.
- Adequate air-conditioning systems reduce the likelihood of damage to computer equipment due to overheating or humidity.
- Cables with special plugs that cannot be easily removed reduce the risk of system damage due to accidental unplugging of the device.
- Surge-protection devices provide protection against temporary power fluctuations that might otherwise cause computers and other network equipment to crash.
- An ***uninterruptible power supply (UPS)*** system provides protection in the event of a prolonged power outage, using battery power to enable the system to operate long enough to back up critical data and safely shut down. (However, it is important to regularly inspect and test the batteries in a UPS to ensure that it will function when needed.)
- Physical access controls reduce the risk of theft or damage.

Training can also reduce the risk of system downtime. Well-trained operators are less likely to make mistakes and will know how to recover, with minimal damage, from errors they do commit. That is why COBIT control objective DS 13.1 stresses the importance of defining and documenting operational procedures and ensuring that IT staff understand their responsibilities.

System downtime can also occur because of computer malware (viruses and worms). Therefore, it is important to install, run, and keep current antivirus and anti-spyware programs. These programs should be automatically invoked not only to scan e-mail, but also any removable

TABLE 10-2 Availability: Objectives and Key Controls

Objective	Key Controls
1. To minimize risk of system downtime	• Preventive maintenance • Fault tolerance • Data center location and design • Training • Patch management and antivirus software
2. Quick and complete recovery and resumption of normal operations	• Backup procedures • Disaster recovery plan (DRP) • Business continuity plan (BCP)

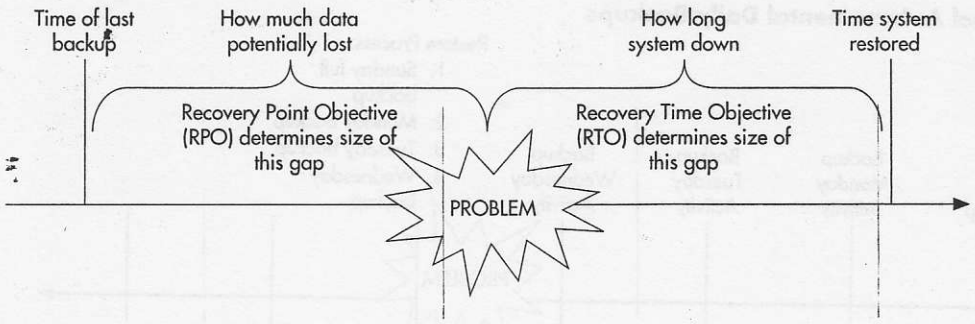


FIGURE 10-3
Relationship of Recovery Point Objective and Recovery Time Objective

computer media (CDs, DVDs, USB drives, etc.) that are brought into the organization. A patch management system provides additional protection by ensuring that vulnerabilities that can be exploited by malware are fixed in a timely manner.

Recovery and Resumption of Normal Operations

The preventive controls discussed in the preceding section can minimize, but not entirely eliminate, the risk of system downtime. Hardware malfunctions, software problems, or human error can cause data to become inaccessible. That's why backup procedures are necessary. A ***backup*** is an exact copy of the most current version of a database, file, or software program that can be used in the event that the original is no longer available. Natural disasters or terrorist acts can destroy not only data but also the entire information system. That's why organizations also need disaster recovery and business continuity plans.

An organization's backup procedures and disaster recovery and business continuity plans reflect management's answers to two fundamental questions:

1. How much data are we willing to recreate from source documents (if they exist) or potentially lose (if no source documents exist)?
2. How long can the organization function without its information system?

Figure 10-3 shows the relationship between these two questions. When a problem occurs, data about everything that has happened since the last backup is lost unless it can be reentered into the system. Thus, management's answer to the first question determines the organization's ***recovery point objective (RPO)***, which represents the maximum amount of data that the organization is willing to potentially lose. The answer to the second question determines the organization's ***recovery time objective (RTO)***, which represents the length of time that the organization is willing to attempt to function without its information system.

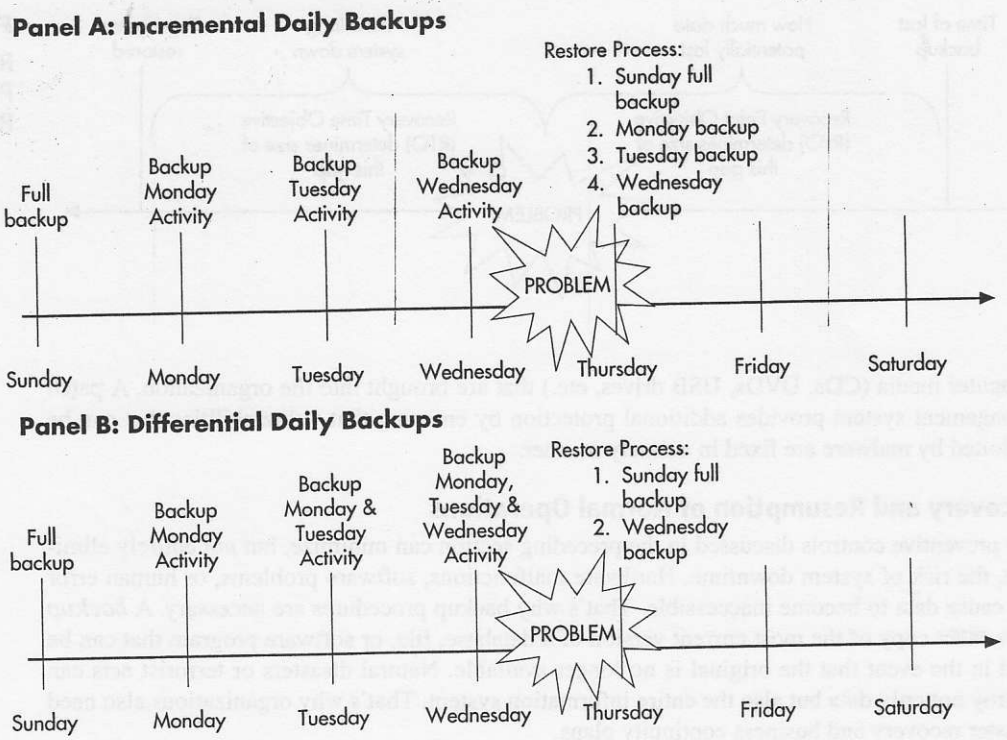
For some organizations, the answer to both questions is close to zero. Airlines and financial institutions, for example, cannot operate without their information systems, nor can they afford to lose information about transactions. For such organizations, the goal is not quick recovery from problems, but resiliency. The solution is to employ real-time mirroring. ***Real-time mirroring*** involves maintaining two copies of the database at two separate data centers at all times and updating both copies in real-time as each transaction occurs. In the event that something happens to one data center, the organization can immediately switch all daily activities to the other.

For other organizations, however, acceptable RPO and RTO may be measured in hours or even days. Achieving those goals requires data backup procedures plus disaster recovery and business continuity plans.

DATA BACKUP PROCEDURES Data backup procedures are designed to deal with situations where information is not accessible because the relevant files or databases have become corrupted as a result of hardware failure, software problems, or human error, but the information system itself is still functioning. Several different backup procedures exist. A *full backup* is an exact copy of the entire database. Full backups are time-consuming, so most organizations only do full backups weekly and supplement them with daily partial backups. Figure 10-4 compares the two types of daily partial backups:

1. An ***incremental backup*** involves copying only the data items that have changed since the last partial backup. This produces a set of incremental backup files, each containing the

FIGURE 10-4
Comparison of Incremental and Differential Daily Backups



results of one day's transactions. Restoration involves first loading the last full backup and then installing each subsequent incremental backup in the proper sequence.

2. A ***differential backup*** copies all changes made since the last full backup. Thus, each new differential backup file contains the cumulative effects of all activity since the last full backup. Consequently, except for the first day following a full backup, daily differential backups take longer than incremental backups. Restoration is simpler, however, because the last full backup needs to be supplemented with only the most recent differential backup, instead of a set of daily incremental backup files.

No matter which backup procedure is used, multiple backup copies should be created. One copy can be stored on-site, for use in the event of relatively minor problems, such as failure of a hard drive. In the event of a more serious problem, such as a fire or flood, any backup copies stored on-site will likely be destroyed or inaccessible. Therefore, a second backup copy needs to be stored off-site. These backup files can be transported to the remote storage site either physically (e.g., by courier) or electronically. In either case, the same security controls need to be applied to backup files as are used to protect the original copy of the information. This means that backup copies of sensitive data should be encrypted both in storage and during electronic transmission. Access to backup files also needs to be carefully controlled and monitored.

It is also important to periodically practice restoring a system from its backups. This verifies that the backup procedure is working correctly and that the backup media (tape or disk) can be successfully read by the hardware in use.

Backups are retained for only a relatively short period of time. For example, many organizations maintain only several months of backups. Some information, however, must be stored much longer. An ***archive*** is a copy of a database, master file, or software that is retained indefinitely as an historical record, usually to satisfy legal and regulatory requirements. As with backups, multiple copies of archives should be made and stored in different locations. Unlike backups, archives are seldom encrypted because their long retention times increase the risk of losing the decryption key. Consequently, physical and logical access controls are the primary means of protecting archive files.

What media should be used for backups and archives, tape or disk? Disk backup is faster, and disks are less easily lost. Tape, however, is cheaper, easier to transport, and more durable. Consequently, many organizations use both media. Data are first backed up to disk, for speed, and then transferred to tape.

Special attention needs to be paid to backing up and archiving e-mail, because it has become an important repository of organizational behavior and information. Indeed, e-mail often contains solutions to specific problems. E-mail also frequently contains information relevant to lawsuits. It may be tempting for an organization to consider a policy of periodically deleting all e-mail, to prevent a plaintiff's attorney from finding a "smoking gun" and to avoid the costs of finding the e-mail requested by the other party. Most experts, however, advise against such policies, because there are likely to be copies of the e-mail stored in archives outside the organization. Therefore, a policy of regularly deleting all e-mail means that the organization will not be able to tell its side of the story; instead, the court (and jury) will only read the e-mail created by the other party to the dispute. There have also been cases where the courts have fined organizations millions of dollars for failing to produce requested e-mail. Therefore, organizations need to back up and archive important e-mail while also periodically purging the large volume of routine, trivial e-mail.

DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING Backups are designed to mitigate problems when one or more files or databases become corrupted because of hardware, software, or human error. Disaster recovery and business continuity plans are designed to mitigate more serious problems.

A ***disaster recovery plan (DRP)*** outlines the procedures to restore an organization's IT function in the event that its data center is destroyed by a natural disaster or act of terrorism. Organizations have three basic options for replacing their IT infrastructure, which includes not just computers, but also network components such as routers and switches, software, data, Internet access, printers, and supplies. The first option is to contract for use of a ***cold site***, which is an empty building that is prewired for necessary telephone and Internet access, plus a contract with one or more vendors to provide all necessary equipment within a specified period of time. A cold site still leaves the organization without the use of its information system for a period of time, so it is appropriate only when the organization's RTO is one day or more. A second option is to contract for use of a ***hot site***, which is a facility that is not only prewired for telephone and Internet access but also contains all the computing and office equipment the organization needs to perform its essential business activities. A hot site typically results in an RTO of hours.

A problem with both cold and hot sites is that the site provider typically oversells its capacity, under the assumption that at any one time only a few clients will need to use the facility. That assumption is usually warranted. In the event of a major disaster, such as Hurricane Katrina, that affects all organizations in a geographic area, however, some organizations may find that they cannot obtain access to their cold or hot site. Consequently, a third infrastructure replacement option for organizations with a very short RTO is to establish a second data center as a backup and use it to implement real-time mirroring.

A ***business continuity plan (BCP)*** specifies how to resume not only IT operations, but all business processes, including relocating to new offices and hiring temporary replacements, in the event that a major calamity destroys not only an organization's data center but also its main headquarters. Such planning is important, because more than half of the organizations without a DRP and a BCP never reopen after being forced to close down for more than a few days because of a disaster. Thus, having both a DRP and a BCP can mean the difference between surviving a major catastrophe such as Hurricane Katrina or 9/11 and going out of business. Focus 10-2 describes how planning helped NASDAQ survive the complete destruction of its offices in the World Trade Center on September 11, 2001.

Simply having a DRP and a BCP, however, is not enough. Both plans must be well documented. The documentation should include not only instructions for notifying appropriate staff and the steps to take to resume operations, but also vendor documentation of all hardware and software. It is especially important to document the numerous modifications made to default configurations, so that the replacement system has the same functionality as the original. Failure to do so can create substantial costs and delays in implementing the recovery process. Detailed operating instructions are also needed, especially if temporary replacements have to be hired. Finally, copies of all documentation need to be stored both on-site and off-site so that it is available when needed.

Periodic testing and revision are probably the most important components of effective disaster recovery and business continuity plans. Most plans fail their initial test because it is impossible

FOCUS 10-2 How NASDAQ Recovered from September 11

Thanks to its effective disaster recovery and business continuity plans, NASDAQ was up and running six days after the September 11, 2001, terrorist attack that destroyed the twin towers of the World Trade Center. NASDAQ'S headquarters were located on the 49th and 50th floors of One Liberty Plaza, just across the street from the World Trade Center. When the first plane hit, NASDAQ'S security guards immediately evacuated personnel from the building. Most of the employees were out of the building by the time the second plane crashed into the other tower. Although employees were evacuated from the headquarters and the office in Times Square had temporarily lost telephone service, NASDAQ was able to relocate to a backup center at the nearby Marriott Marquis hotel. Once there, NASDAQ executives went through their list of priorities: first, their employees; next, the physical damage; and last, the trading industry situation.

Effective communication became essential in determining the condition of these priorities. NASDAQ attributes much of its success in communicating and coordinating with the rest of the industry to its dress rehearsals for Y2K. While preparing for the changeover, NASDAQ had regular nationwide teleconferences with all the exchanges. This helped it organize similar conferences after the 9/11 attack. NASDAQ had already planned for one potential crisis, and this proved helpful in recovering from a different, unexpected, crisis. By prioritizing and teleconferencing, the company was able to quickly identify problems and the traders who would need extra help before NASDAQ could open the market again.

NASDAQ'S extremely redundant and dispersed systems also helped it quickly reopen the market. Executives carried more than one mobile phone so that they could continue to communicate in the event one carrier lost service. Every trader was linked to two of NASDAQ's 20 connection centers located throughout the United States. The centers are connected to each other using two separate paths and sometimes two distinct vendors. Servers are kept in different buildings and have two network topologies. In addition to Manhattan and Times Square, NASDAQ had offices in Maryland and Connecticut. This decentralization allowed it to monitor the regulatory processes throughout the days following the attack. It also lessened the risk of losing all NASDAQ'S senior management.

NASDAQ also invested in interruption insurance to help defer the costs of closing the market. All of this planning and foresight saved NASDAQ from losing what could have been tens of millions of dollars.

to fully anticipate everything that could go wrong. The time to discover such problems is not during an actual emergency, but rather in a setting in which weaknesses can be carefully and thoroughly analyzed and appropriate changes in procedures made. Therefore, disaster recovery and business continuity plans need to be tested on at least an annual basis to ensure that they accurately reflect recent changes in equipment and procedures. It is especially important to test the procedures involved in the transfer of actual operations to cold or hot sites. Finally, DRP and BCP documentation needs to be updated to reflect any changes in procedures made in response to problems identified during tests of those plans.

EFFECTS OF VIRTUALIZATION AND CLOUD COMPUTING A virtual machine is just a collection of software files. Therefore, if the physical server hosting that machine fails, the files can be installed on another host machine within minutes. Thus, virtualization significantly reduces the time needed to recover (RTO) from hardware problems. Note that virtualization does not eliminate the need for backups; organizations still need to create periodic "snapshots" of desktop and server virtual machines and then store those snapshots on a network drive so that the machines can be recreated. Virtualization can also be used to support real-time mirroring in which two copies of each virtual machine are run in tandem on two separate physical hosts. Every transaction is processed on both virtual machines. If one fails, the other picks up without any break in service.

Cloud computing has both positive and negative effects on availability. Cloud computing typically utilizes banks of redundant servers in multiple locations, thereby reducing the risk that a single catastrophe could result in system downtime and the loss of all data. However, if a public cloud provider goes out of business, it may be difficult, if not impossible, to retrieve any data stored in the cloud. Therefore, a policy of making regular backups and storing those backups somewhere other than with the cloud provider is critical. In addition, accountants need to assess the long-run financial viability of a cloud provider before their organization commits to outsource any of its data or applications to a public cloud.

Change Control

COBIT sections AI 6, AI 7, and DS 9 address different aspects of the critically important topic of change control. Organizations constantly modify their information systems to reflect new business practices and to take advantage of advances in information technology. ***Change control*** is the formal process used to ensure that modifications to hardware, software, or processes do not reduce systems reliability. In fact, good change control often results in overall *better* operating performance: careful testing prior to implementation reduces the likelihood of making changes that cause system downtime, and thorough documentation facilitates quicker "trouble-shooting" and resolution of any problems that do occur. Companies with a good change control process are also less likely to suffer financial or reputational harm from security incidents.

Effective change control procedures require regularly monitoring for unauthorized changes and sanctioning anyone who intentionally introduces such changes. Other principles of a well-designed change control process include the following:

- All change requests should be documented and follow a standardized format that clearly identifies the nature of the change, the reason for the request, the date of the request, and the outcome of the request.
- All changes should be approved by appropriate levels of management. Approvals should be clearly documented to provide an audit trail. Managers should consult with the CISO or other IT managers about the effects of the proposed changes on systems reliability.
- To assess the impact of the proposed change on all five principles of systems reliability, changes should be thoroughly tested prior to implementation in a separate, nonproduction environment, not the system actually used for daily business processes. (Virtualization technology can be used to reduce the costs of creating a separate testing and development system). As data from old files and databases are entered into new data structures, conversion controls are needed to ensure that the new data storage media are free of errors. The old and new systems should be run in parallel at least once and the results compared to identify discrepancies. Internal auditors should review data conversion processes for accuracy.
- All documentation (program instructions, systems descriptions, backup and disaster recovery plans, etc.) should be updated to reflect authorized changes to the system.
- "Emergency" changes or deviations from standard operating policies must be documented and subjected to a formal review and approval process as soon after implementation as practicable. All emergency changes need to be logged to provide an audit trail.
- "Backout" plans need to be developed for reverting to previous configurations in case approved changes need to be interrupted or abandoned.
- User rights and privileges must be carefully monitored *during* the change process to ensure that proper segregation of duties is maintained.

Probably the most important change control is adequate monitoring and review by top management to ensure that proposed and implemented changes are consistent with the organization's multiyear strategic plan. The objective of this oversight is to make certain that the organization's information system continues to effectively support its strategy. Many organizations create IT steering committees to perform this important monitoring function.

Summary and Case Conclusion

Jason's report assessed the effectiveness of Northwest Industries' controls designed to ensure processing integrity. To minimize data entry, and the opportunity for mistakes, Northwest Industries mailed turnaround documents to customers, which were returned with their payments. All data entry was done online, with extensive use of input validation routines to ensure the accuracy of the information entering the system. Managers reviewed output for reasonableness, and the accuracy of key components of financial reports was regularly cross-validated with independent sources. For example, inventory was counted quarterly, and the results of the physical counts were reconciled to the quantities stored in the system.

Jason was concerned about the effectiveness of controls designed to ensure systems availability, however. He noted that although Northwest Industries had developed a disaster recovery and business continuity plan, those plans had not been reviewed or updated for three years. Of even greater concern was the fact that many portions of the plan, including arrangements for a cold site located in California, had never been tested. Jason's biggest concern, however, related to backup procedures. All files were backed up weekly, on Saturdays, onto DVDs, and incremental backups were made each night, but no one had ever practiced restoring the data. In addition, the backups were not encrypted, and one copy was stored on-site in the main server room on a shelf by the door.

Jason also documented evidence of weaknesses related to change control. One point of concern was the finding that "emergency" changes made during the past year were not documented. Another was the fact that in order to save money, Northwest Industries gave programmers access to its transaction processing system to make changes, rather than using a separate testing and development system.

Jason concluded his report with specific recommendations to address the weaknesses he had found. He recommended that Northwest Industries immediately test its backup restoration procedures and encrypt its backup files. Jason also recommended testing the DRP and BCP plans. Another recommendation was to purchase a server that would use virtualization software to create a testing and development system and restrict programmers' access to only that virtual system. Finally, he suggested the CIO should assign someone to update the documentation to record the effects of "emergency changes" made during the past year and implement procedures to ensure that all future changes be documented. Jason felt confident that once those recommendations were implemented, management could be reasonably assured that Northwest Industries' information systems had satisfied the AICPA's Trust Services framework criteria and principles for systems reliability.

Key Terms

turnaround document 296
field check 296
sign check 296
limit check 296
range check 296
size check 296
completeness check 296
validity check 296
reasonableness test 296
check digit 297
check digit verification 297
sequence check 297
batch totals 297
financial total 297
hash total 297
record count 297
prompting 297
closed-loop verification 297
header record 297
trailer record 298
transposition error 298
cross-footing balance test 298
zero-balance test 298
concurrent update controls 298
checksum 299
parity bit 299
parity checking 299
fault tolerance 304
redundant arrays of independent drives (RAID) 304
uninterruptible power supply (UPS) 304
backup 305
recovery point objective (RPO) 305
recovery time objective (RTO) 305
real-time mirroring 305
incremental backup 305
differential backup 306
archive 306
disaster recovery plan (DRP) 307
cold site 307
hot site 307
business continuity plan (BCP) 307
change control 309

AIS IN ACTION

Chapter Quiz

1. Which of the following measures the amount of data that might be potentially lost as a result of a system failure?
   a. recovery time objective (RTO)
   b. recovery point objective (RPO)
   c. disaster recovery plan (DRP)
   d. business continuity plan (BCP)

2. Which data entry application control would detect and prevent entry of alphabetic characters as the price of an inventory item?
   a. field check
   b. limit check
   c. reasonableness check
   d. sign check

3. Which of the following controls would prevent entry of a nonexistent customer number in a sales transaction?
   a. field check
   b. completeness check
   c. validity check
   d. batch total

4. Which disaster recovery strategy involves contracting for use of a physical site to which all necessary computing equipment will be delivered within 24 to 36 hours?
   a. virtualization
   b. cold site
   c. hot site
   d. data mirroring

5. Which of the following statements is true?
   a. Incremental daily backups are faster to perform than differential daily backups, but restoration is slower and more complex.
   b. Incremental daily backups are faster to perform than differential daily backups, and restoration is faster and simpler.
   c. Differential daily backups are faster to perform than incremental daily backups, but restoration is slower and more complex.
   d. Differential daily backups are faster to perform than incremental daily backups, and restoration is faster and simpler.

6. Information that needs to be stored securely for 10 years or more would most likely be stored in which type of file?
   a. backup
   b. archive
   c. encrypted
   d. log

7. Which of the following is an example of the kind of batch total called a hash total?
   a. the sum of the purchase amount field in a set of purchase orders
   b. the sum of the purchase order number field in a set of purchase orders
   c. the number of completed documents in a set of purchase orders
   d. all of the above

8. Which of the following statements is true?
   a. "Emergency" changes need to be documented once the problem is resolved.
   b. Changes should be tested in a system separate from the one used to process transactions.
   c. Change controls are necessary to maintain adequate segregation of duties.
   d. All of the above are true.

9. Which of the following provides detailed procedures to resolve the problems resulting from a flash flood that completely destroys a company's data center?
   a. backup plan
   b. disaster recovery plan (DRP)
   c. business continuity plan (BCP)
   d. archive plan

10. Which of the following is a control that can be used to verify the accuracy of information transmitted over a network?
    a. completeness check
    b. check digit
    c. parity bit
    d. size check

Discussion Questions

10.1. Two ways to create processing integrity controls in Excel spreadsheets are to use the built-in Data Validation tool or to write custom code with IF statements. What are the relative advantages and disadvantages of these two approaches?

10.2. What is the difference between using check digit verification and using a validity check to test the accuracy of an account number entered on a transaction record?

10.3. For each of the three basic options for replacing IT infrastructure (cold sites, hot sites, and real-time mirroring), give an example of an organization that could use that approach as part of its DRP. Be prepared to defend your answer.

10.4. Use the numbers 10–19 to show why transposition errors are always divisible by 9.

10.5. What are some business processes for which an organization might use batch processing?

10.6. Why do you think that surveys continue to find that a sizable percentage of organizations either do not have formal disaster recovery and business continuity plans or have not tested and revised those plans for more than a year?

Problems

10.1. Match the following terms with the appropriate definition or example:

____ 1. Business continuity plan (BCP)	a. A file used to store information for long periods of time
____ 2. Completeness check	b. A plan that describes how to resume IT functionality after a disaster
____ 3. Hash total	c. An application control that verifies that the quantity ordered is greater than 0
____ 4. Incremental daily backup	d. A control that counts the number of odd or even bits in order to verify that all data were transmitted correctly
____ 5. Archive	e. An application control that tests whether a customer is 18 or older
____ 6. Field check	f. A daily backup plan that copies all changes since the last full backup
____ 7. Sign check	g. A disaster recovery plan that contracts for use of an alternate site that has all necessary computing and network equipment, plus Internet connectivity
____ 8. Change control	h. A disaster recovery plan that contracts for use of another company's information system
____ 9. Cold site	i. A disaster recovery plan that contracts for use of an alternate site that is prewired for Internet connectivity but has no computing or network equipment
____ 10. Limit check	j. An application control that ensures that a customer's ship-to address is entered in a sales order
____ 11. Zero-balance test	k. An application control that involves use of an account that should not have a balance after processing
____ 12. Recovery point objective (RPO)	l. An application control that involves comparing the sum of a set of columns to the sum of a set of rows
____ 13. Recovery time objective (RTO)	m. A measure of the length of time that an organization is willing to function without its information system
____ 14. Record count	n. A measure of the amount of data that an organization is willing to reenter or possibly lose in the event of a disaster
____ 15. Validity check	o. A batch total that does not have any intrinsic meaning
____ 16. Check digit verification	p. A batch total that represents the number of transactions processed

____ 17. Closed-loop verification	q. An application control that validates the correctness of one data item in a transaction record by comparing it to the value of another data item in that transaction record
____ 18. Parity checking	r. An application control that verifies that an account number entered in a transaction record matches an account number in the related master file
____ 19. Reasonableness test	s. A plan that describes how to resume business operations after a major calamity, such as Hurricane Katrina, that destroys not only an organization's data center but also its headquarters
____ 20. Financial total	t. A data entry application control that verifies the accuracy of an account number by recalculating the last number as a function of the preceding numbers
____ 21. Turnaround document	u. A daily backup procedure that copies only the activity that occurred on that particular day
	v. A data entry application control that could be used to verify that only numeric data are entered into a field
	w. A plan to ensure that modifications to an information system do not reduce its security
	x. A data entry application control in which the system displays the value of a data item and asks the user to verify that the system has accessed the correct record
	y. A batch total that represents the total dollar value of a set of transactions
	z. A document sent to an external party and subsequently returned so that preprinted data can be scanned rather than manually reentered.

10.2. Excel Problem

Enter the following data into a spreadsheet, and then perform the following tasks:

Employee Number	Pay Rate	Hours Worked	Gross Pay	Deductions	Net Pay
12355	10.55	38	400.90	125.00	275.90
2178g	11.00	40	440.00	395.00	45.00
24456	95.00	90	8550.00	145.00	8405.00
34567	10.00	40	400.00	105.00	505.00

a. Calculate examples of these batch totals:
   - A hash total
   - A financial total
   - A record count

b. Assume the following rules govern normal data:
   - Employee numbers are five digits in length and range from 10000 through 99999.
   - Maximum pay rate is $25, and minimum is $9.
   - Hours worked should never exceed 40.
   - Deductions should never exceed 40% of gross pay.

Give a specific example of an error or probable error in the data set that each of the following controls would detect:
   - Field check
   - Limit check
   - Reasonableness test
   - Cross-footing balance test

c. Create a control procedure that would prevent, or at least detect, each of the errors in the data set.

10.3. Excel Problem

The Moose Wings Cooperative Flight Club owns a number of airplanes and gliders. It serves fewer than 2,000 members, who are numbered sequentially from the founder, Tom Eagle (0001), to the newest member, Jacques Noveau (1368). Members rent the flying machines by the hour, and all must be returned on the same day. The following six records were among those entered for the flights taken on September 1, 2010:

Member #	Flight Date MM/DD/YY	Plane Used*	Takeoff Time	Landing Time
1234	09/10/10	G	6:25	8:46
4111	09/01/10	C	8:49	10:23
1210	09/01/10	P	3:42	5:42
0023	09/01/10	X	1:59	12:43
012A	09/01/10	P	12:29	15:32
0999	09/01/10	L	15:31	13:45

*C = Cessna, G = Glider, L = Lear Jet, P = Piper Cub

Required

a. Identify and describe any errors in the data.
b. For each of the five data fields, suggest one or more input edit controls that could be used to detect input errors.
c. Enter the data in a spreadsheet, and create appropriate controls to prevent or at least detect the input errors.
d. Suggest other controls to minimize the risk of input errors.

(SMAC adapted)

10.4. The first column in Table 10-3 lists transaction amounts that have been summed to obtain a batch total. Assume that all data in the first column are correct. Cases A through D each contain an input error in one record, along with a batch total computed from that set of records.

Required

For each case (a through d), compute the difference between the correct and erroneous batch totals, and explain how this difference could help identify the cause of the error.

TABLE 10-3 Data for Problem 10.4

	Correct Transactions	Case A	Case B	Case C	Case D
	$3,630.62	$3,630.62	$3,630.62	$3,630.62	$3,630.62
	1,484.86	1,484.86	1,484.86	1,484.86	1,484.86
	1,723.46	1,723.46	1,723.46	1,723.46	1,723.46
	9,233.25	9,233.25	9,233.25	9,233.25	9,233.25
	123.45	123.45	123.45	123.45	123.45
	7,832.44	7,832.44	1,832.44	7,832.44	7,832.44
	2,398.33	2,398.33	2,398.33	2,398.33	2,398.33
	3,766.24	3,766.24	3,766.24	3,766.24	3,766.24
	4,400.00	4,400.00	4,400.00	−4,400.00	4,400.00
	2,833.00	2,833.00	2,833.00	2,833.00	2,833.00
	1,978.95	1,987.95	1,978.95	1,978.95	1,978.95
	654.32	654.32	654.32	654.32	9,876.23
	9,876.23	9,876.23	9,876.23	9,876.23	2,138.10
	2,138.10	2,138.10	2,138.10	2,138.10	5,533.99
	5,533.99	5,533.99	5,533.99	5,533.99	
Batch total	$57,607.24	$57,616.24	$51,607.24	$48,807.24	$56,952.92

10.5. Excel Problem

Create a spreadsheet with the following columns:

- Plaintext character
- ASCII code (seven bits, binary number)
- First bit
- Second bit
- Third bit
- Fourth bit
- Fifth bit
- Sixth bit
- Seventh bit
- Number of bits with value = 1
- Parity bit for odd parity coding
- Parity bit for even parity coding

Required

a. Enter a-e, A-E, 0-9, ?, !,%, &, and ; in the plaintext column.
b. The ASCII column should convert the plaintext character to the binary code used by your computer.
c. The next seven columns should each display one bit of the ASCII code, beginning with the leftmost digit. (*Hint:* Excel provides text functions that can select individual characters from a string.)
d. The tenth column should sum the number of bits that have the value 1. (*Hint:* The text functions used to populate columns 3–9 return a text string that you will need to convert to a numeric value.)
e. Column 11 should have a 1 if the number in column 10 is odd, and 0 if the number in column 10 is even.
f. Column 12 should have a 1 if the number in column 10 is even, and a 0 if the number in column 10 is odd.

10.6. The ABC Company is considering the following options for its backup plan:

1. Daily full backups:
   - Time to perform backup = 60 minutes
   - Size of backup = 50 GB
   - Time to restore from backup = 30 minutes
2. Weekly full backups plus daily incremental backup:
   - Same requirements as option 1 to do a full backup on Friday, plus
   - Time to perform daily backup = 10 minutes
   - Size of daily backup = 10 GB
   - Time to restore each daily backup file = 5 minutes
3. Weekly full backups plus daily differential backup:
   - Same requirements as option 1 to do a full backup on Friday, plus
   - Time to perform daily backup = 10 minutes first day, growing by 5 minutes each day thereafter
   - Size of daily backup = 10 GB first day, growing by 10 GB each day
   - Time to restore differential backup file = 5 minutes first day, increasing by 2 minutes each subsequent day

Which approach would you recommend? Why?

10.7. Which control(s) would best mitigate the following threats?

a. The hours-worked field in a payroll transaction record contained the value 400 instead of 40. As a result, the employee received a paycheck for $6,257.24 instead of $654.32.
b. The accounts receivable file was destroyed because it was accidentally used to update accounts payable.
c. During processing of customer payments, the digit 0 in a payment of $204 was mistakenly typed as the letter "O." As a result, the transaction was not processed

correctly, and the customer erroneously received a letter that the account was delinquent.

d. A salesperson mistakenly entered an online order for 50 laser printers instead of 50 laser printer toner cartridges.
e. A 20-minute power brownout caused a mission-critical database server to crash, shutting down operations temporarily.
f. A fire destroyed the data center, including all backup copies of the accounts receivable files.
g. After processing sales transactions, the inventory report showed a negative quantity on hand for several items.
h. A customer order for an important part did not include the customer's address. Consequently, the order was not shipped on time, and the customer called to complain.
i. When entering a large credit sale, the clerk typed in the customer's account number as 45982 instead of 45892. That account number did not exist. The mistake was not caught until later in the week, when the weekly billing process was run. Consequently, the customer was not billed for another week, delaying receipt of payment.
j. A visitor to the company's Web site entered 400 characters into the five-digit Zip code field, causing the server to crash.
k. Two traveling sales representatives accessed the parts database at the same time. Salesperson A noted that there were still 55 units of part 723 available and entered an order for 45 of them. While salesperson A was keying in the order, salesperson B, in another state, also noted the availability of 55 units for part 723 and entered an order for 33 of them. Both sales reps promised their customer next-day delivery. Salesperson A's customer, however, learned the next day that the part would have to be back-ordered. The customer canceled the sale and vowed to never again do business with the company.
l. The warranty department manager was upset because special discount coupons were mailed to every customer who had purchased the product within the past three years, instead of to only those customers who had purchased the product within the past three months.
m. The clerk entering details about a large credit sale mistakenly typed in a nonexistent account number. Consequently, the company never received payment for the items.
n. A customer filled in the wrong account number on the portion of the invoice being returned with payment. Consequently, the payment was credited to another customer's account.
o. A batch of 73 time sheets was sent to the payroll department for weekly processing. Somehow, one of the time sheets did not get processed. The mistake was not caught until payday, when one employee complained about not receiving a paycheck.
p. Sunspot activity resulted in the loss of some data being sent to the regional office. The problem was not discovered until several days later, when managers attempted to query the database for that information.

10.8. MonsterMed Inc. (MMI) is an online pharmaceutical firm. MMI has a small systems staff that designs and writes MMI's customized software. The data center is installed in the basement of its two-story headquarters building. The data center is equipped with halon-gas fire suppression equipment and an uninterruptible power supply system.

The computer operations staff works a two-shift schedule, five days per week. MMI's programming staff, located in the same building, has access to the data center and can test new programs and program changes when the operations staff is not available. Programmers make changes in response to oral requests by employees using the system. Because the programming staff is small and the work demands have increased, systems and programming documentation is developed only when time is available. Backups are made whenever time permits. The backup files are stored in a locked cabinet in the data center. Unfortunately, due to several days of heavy rains, MMI's building recently experienced serious flooding that destroyed not only the computer hardware but also all the data and program files that were on-site.

Required

a. Identify at least five weaknesses in MonsterMed Inc.'s backup and DRP procedures.
b. Evaluate change controls at MonsterMed Inc.

(CMA exam, adapted)

10.9. Excel Problem

Create data validation rules in a spreadsheet to perform each of the following controls:
a. Limit check—that values in the cell are < 70
b. Range check—that values in the cell are between 15 and 65
c. Sign check—that values in the cell are positive
d. Field check—that values in a cell are only numeric
e. Size check—that the cell accepts no more than 40 characters of text
f. Reasonableness check—that the cell's value is less than 75% of the cell to its left
g. Validity check—that a value exists in a list of allowable values

10.10. Excel Problem

Creating and testing check digits.

Required

a. Create a spreadsheet that will take as input a five-digit account number, and calculate a check digit using this formula: (5 × left-most digit + 4 × next digit + 3 × third digit + 2 × fourth digit + fifth digit) modulus division by 7. (Modulus division returns the remainder—for example: 11 modulus division by 3 = 2). The check digit then becomes the sixth (right-most) digit in the account number. Your spreadsheet should look like this:

Check digits—creation and use

a. Creating check digits Formula = (5x left-most digit + 4x next digit + 3x third digit + 2x fourth digit + fifth digit) mod 7

Raw account#	First digit	Second digit	Third digit	Fourth digit	Fifth digit	Check digit calculation	Actual account #
12345	1	2	3	4	5	0	123450
12346	1	2	3	4	6	1	123461
12347	1	2	3	4	7	2	123472
12348	1	2	3	4	8	3	123483
12349	1	2	3	4	9	4	123494
12350	1	2	3	5	0	4	123504
12351	1	2	3	5	1	5	123515
12352	1	2	3	5	2	6	123526
12353	1	2	3	5	3	0	123530

b. Add another panel to the spreadsheet that takes as input a six-digit account number and uses the check digit formula in part a to test whether or not the account number is valid. Your solution should look like this:

b. Testing check digits

Account number	First digit	Second digit	Third digit	Fourth digit	Fifth digit	Check digit	Valid? (Y/N)
123530	1	2	3	5	3	0	Y
123534	1	2	3	5	3	4	N

10.11. For each of the following scenarios, determine whether the company's current backup procedures enable it to meet its recovery objectives, and explain why:
a. Scenario 1:
- Recovery point objective = 24 hours
- Daily backups at 3:00 A.M., process takes 2 hours
- Copy of backup tapes picked up daily at 8:00 A.M. for storage off-site

b. Scenario 2: Company makes daily incremental backups Monday through Saturday at 7:00 P.M. each night. Company makes full backup weekly, on Sunday at 1:00 P.M.
   - Recovery time objective = 2 hours
   - Time to do full backup = 3 hours
   - Time to restore from full backup = 1 hour
   - Time to make incremental daily backup = 1 hour
   - Time to restore each incremental daily backup = 30 minutes

c. Scenario 3: Company makes daily differential backups Monday through Friday at 8:00 P.M. each night. Company makes full backup weekly, on Saturdays, at 8:00 A.M.
   - Recovery time objective = 6 hours
   - Time to do full backup = 4 hours
   - Time to restore from full backup = 3 hours
   - Time to do differential daily backups = 1 hour on Monday, increasing by 30 minutes each successive day
   - Time to restore differential daily backup = 30 minutes for Monday, increasing by 15 minutes each successive day

Case 10-1 Ensuring Systems Availability

The *Journal of Accountancy* (available at www.aicpa.org) has published a series of articles that address different aspects of disaster recovery and business continuity planning:

1. J. A. Gerber and E. R. Feldman, "Is Your Business Prepared for the Worst?" *Journal of Accountancy* (April 2002): 61–64.
2. E. McCarthy, "The Best-Laid Plans," *Journal of Accountancy* (May 2004): 46–54.
3. R. Myers, "Katrina's Harsh Lessons," *Journal of Accountancy* (June 2006): 54–63.
4. S. Phelan and M. Hayes, "Before the Deluge—and After," *Journal of Accountancy* (April 2003): 57–66.

Required

Read one or more of these articles that your professor assigns, plus section DS 4 of COBIT version 4.1 (available at www.isaca.org), to answer the following questions:

1. What does COBIT suggest as possible metrics for evaluating how well an organization is achieving the objective of DS 4? Why do you think that metric is useful?
2. For each article assigned by your professor, complete the following table, summarizing what each article said about a specific COBIT control objective (an article may not address all 10 control objectives in DS 4):

COBIT Control Objective	Points Discussed in Article
DS 4.1	
DS 4.2	
DS 4.3	
DS 4.4	
DS 4.5	
DS 4.6	
DS 4.7	
DS 4.8	
DS 4.9	
DS 4.10	

Case 10-2 Change Controls

Read section AI 6 in version 4.1 of COBIT (available at www.isaca.org), and answer the following questions:

1. What is the purpose of each detailed control objective—why is it important?
2. How is each of the suggested metrics useful?

AIS IN ACTION SOLUTIONS

Quiz Key

1. Which of the following measures the amount of data that might be potentially lost as a result of a system failure?
   a. recovery time objective (RTO) (Incorrect. The RTO measures the time that an organization may have to function without its information system.)
   ▶ b. recovery point objective (RPO) (Correct. The RPO measures the time between the last data backup and the occurrence of a problem.)
   c. disaster recovery plan (DRP) (Incorrect. A DRP specifies the procedures to restore IT operations.)
   d. business continuity plan (BCP) (Incorrect. A BCP specifies the procedures to resume business processes.)

2. Which data entry application control would detect and prevent entry of alphabetic characters as the price of an inventory item?
   ▶ a. field check (Correct. Field checks test whether data are numeric or alphabetic.)
   b. limit check (Incorrect. A limit check compares an input value against a fixed number.)
   c. reasonableness check (Incorrect. A reasonableness check compares two data items to determine whether the values of both are reasonable.)
   d. sign check (Incorrect. A sign check determines whether a numeric field is positive or negative.)

3. Which of the following controls would prevent entry of a nonexistent customer number in a sales transaction?
   a. field check (Incorrect. A field check tests only whether data are numeric or alphabetic.)
   b. completeness check (Incorrect. A completeness check would ensure that a customer number was entered, but it does not test whether the customer number exists.)
   ▶ c. validity check (Correct. A validity check compares a customer number entered into a transaction record against the customer numbers that exist in the master file or database.)
   d. batch total (Incorrect. A batch total is used to verify completeness of data entry.)

4. Which disaster recovery strategy involves contracting for use of a physical site to which all necessary computing equipment will be delivered within 24 to 36 hours?
   a. virtualization (Incorrect. Virtualization is a strategy to make better use of resources by running multiple virtual machines on one physical host. It is not a disaster recovery strategy.)
   ▶ b. cold site (Correct.)
   c. hot site (Incorrect. A hot site is an infrastructure replacement strategy which contracts for use of a physical site that contains all necessary computer and network equipment.)

d. data mirroring (Incorrect. Data mirroring is a fault-tolerant backup strategy in which the organization maintains a second data center and all transactions are processed on both systems as they occur.)

5. Which of the following statements is true?
   ▶ a. Incremental daily backups are faster to perform than differential daily backups, but restoration is slower and more complex. (Correct.)
   b. Incremental daily backups are faster to perform than differential daily backups, and restoration is faster and simpler. (Incorrect. Incremental daily backups produce separate backup files for each day since the last full backup, making restoration more complex.)
   c. Differential daily backups are faster to perform than incremental daily backups, but restoration is slower and more complex. (Incorrect. Differential daily backups are slower than incremental daily backups, but restoration is faster and simpler because only the most recent differential daily backup and the last full backup files are required.)
   d. Differential daily backups are faster to perform than incremental daily backups, and restoration is faster and simpler. (Incorrect. Differential daily backups are slower to perform than incremental daily backups.)

6. Information that needs to be stored securely for 10 years or more would most likely be stored in which type of file?
   a. backup (Incorrect. Backups are for short-term storage; archives are for long-term storage.)
   ▶ b. archive (Correct.)
   c. encrypted (Incorrect. Long-term retention uses archives, which are usually not encrypted.)
   d. log (Incorrect. A log is part of an audit trail.)

7. Which of the following is an example of the kind of batch total called a hash total?
   a. the sum of the purchase amount field in a set of purchase orders (Incorrect. This is an example of a financial total.)
   ▶ b. the sum of the purchase order number field in a set of purchase orders (Correct. The sum of purchase order numbers has no intrinsic meaning.)
   c. the number of completed documents in a set of purchase orders (Incorrect. This is an example of a record count.)
   d. all of the above (Incorrect. Choices a and c are incorrect.)

8. Which of the following statements is true?
   a. "Emergency" changes need to be documented once the problem is resolved. (Incorrect. This statement is true, but so are b and c.)
   b. Changes should be tested in a system separate from the one used to process transactions. (Incorrect. This statement is true, but so are a and c.)
   c. Change controls are necessary to maintain adequate segregation of duties. (Incorrect. This statement is true, but so are a and b.)
   ▶ d. All of the above are true. (Correct.)

9. Which of the following provides detailed procedures to resolve the problems resulting from a flash flood that completely destroys a company's data center?
   a. backup plan (Incorrect. Backup plans focus solely on making a duplicate copy of files in the event that the original becomes corrupted because of hardware malfunctions, software problems, or human error.)
   ▶ b. disaster recovery plan (DRP) (Correct. A DRP focuses on restoring an organization's IT functionality.)
   c. business continuity plan (BCP) (Incorrect. A BCP focuses on restoring not only IT, but all aspects business processes.)
   d. archive plan (Incorrect. An archive plan deals with long-term retention of data.)

10. Which of the following is a control that can be used to verify the accuracy of information transmitted over a network?
    a. completeness check (Incorrect. A completeness check is a data input control to ensure that all necessary data are entered.)
    b. check digit (Incorrect. A check digit is a data input control designed to detect miskeying of account numbers.)
    ▶ c. parity bit (Correct. A parity bit is a communications control that counts the number of bits in order to verify the integrity of data sent and received.)
    d. size check (Incorrect. A size check is a data input control to ensure that the amount of data entered does not exceed the space set aside for it. Size checks are especially important for programs that accept input from users, because they can prevent buffer overflow attacks.)