Chapter 11

Internal Control and COSO Framework

■ Concept Checks

P. 339

1. Management typically has three broad objectives in designing effective internal controls.

    1. **Reliability of Reporting** While this objective relates to both external and internal reporting, we focus here on the reliability of external financial reporting. Management is responsible for preparing financial statements for investors, creditors, and other users. Management has both a legal and professional responsibility to be sure that the information is fairly presented in accordance with reporting requirements such as GAAP or IFRS. The objective of effective internal control over financial reporting is to fulfill these financial reporting responsibilities.

    2. **Efficiency and Effectiveness of Operations** Controls within an organization are meant to encourage efficient and effective use of its resources to optimize the company's goals. An important objective of these controls is accurate financial and non-financial information about the entity's operations for decision making.

    3. **Compliance with Laws and Regulations** Section 404 of the Sarbanes–Oxley Act requires all public companies to issue a report about the operating effectiveness of internal control over financial reporting. In addition to the legal provisions of Section 404, public, nonpublic, and not-for-profit organizations are required to follow many laws and regulations. Some relate to accounting only indirectly, such as environmental protection and civil rights laws. Others are closely related to accounting, such as income tax regulations and anti-fraud regulations such as the Foreign Corrupt Practices Act of 1977 and certain provisions of the Sarbanes–Oxley Act.

Concept Check - p. 339 (continued)

2. Section 404(a) of the Sarbanes-Oxley Act requires management of all public companies to issue an internal control report that includes the following:

- A statement that management is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting and
- An assessment of the effectiveness of the internal control structure and procedures for financial reporting as of the end of the company's fiscal year.

P. 348

1. The COSO *Internal Control – Integrated Framework* consists of the following five components:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

The control environment is the broadest of the five and deals primarily with the way management implements its attitude about internal controls. The other four components are closely related to the control environment. In the context of internal controls related to financial reporting, risk assessment is management's identification and analysis of risks relevant to the preparation of financial statements in accordance with accounting standards. Management implements control activities and creates the accounting information and communication system in response to risks identified as part of its risk assessment in order to meet its objectives for financial reporting. Finally, management periodically assesses the quality of internal control performance to determine that controls are operating as intended and that they are modified as appropriate for changes in conditions (monitoring). All five components are necessary for effectively designed and implemented internal control.

2. The updated COSO *Internal Control – Integrated Framework* includes seventeen broad principles that provide more guidance related to the five COSO components. The components and principles are listed together in Table 11-1. According to the COSO guidance, all of these seventeen principles must be present and functioning in order for controls to be effective. In assessing whether internal controls are designed and operating effectively, management would want to ensure that all of the principles are present and functioning. For example, in considering whether monitoring controls are designed and operating effectively, management would want to perform periodic evaluations of the monitoring controls and also ensure that identified deficiencies are being communicated to those who can remediate those deficiencies.

Concept Check (continued)

P. 355

1. *General controls* relate to all aspects of the IT function. They have a global impact on all software applications. Examples of general controls include controls related to the administration of the IT function; software acquisition and maintenance; physical and online security over access to hardware, software, and related backup; back-up planning in the event of unexpected emergencies; and hardware controls. *Application controls* apply to the processing of individual transactions. Examples of application controls include a programmed control that verifies that all time cards submitted are for valid employee ID numbers included in the electronically accessible employee master file; and a control that recomputes net pay from gross pay and deductions.

2. The typical duties often segregated within an IT function include systems development, computer operations, and data control. Systems development involves the acquisition or programming of application software. Systems development personnel work with test copies of programs and data files to develop new or improved application software programs. Computer operations personnel are responsible for executing live production jobs in accordance with a job schedule and for monitoring consoles for messages about computer efficiency and malfunctions. Data control personnel are responsible for data input and output control. They often independently verify the quality of input and the reasonableness of output. By separating these functions, no one IT employee can make changes to application software or underlying master files and then operate computer equipment to use those changed programs or data files to process transactions.

■ Review Questions

11-1 Management designs systems of internal control to accomplish three categories of objectives: reporting, operations, and compliance with laws and regulations. The auditor's focus in both the audit of financial statements and the audit of internal controls is on those controls related to the reliability of financial reporting plus those controls related to operations and to compliance with laws and regulations objectives that could materially affect financial reporting.

11-2 Management's assessment of internal control over financial reporting consists of two key characteristics. First, management must evaluate the design of internal control over financial reporting. Second, management must test the operating effectiveness of those controls. When evaluating the design of internal control over financial reporting, management evaluates whether the controls are designed to prevent or detect material misstatements in the financial statements.

11-2 (continued)

When testing the operating effectiveness of those controls, the objective is to determine whether the control is operating as designed and whether the person performing the control possesses the necessary authority and qualifications to perform the control effectively.

11-3 There are eight parts of the planning phase of audits: accept client and perform initial audit planning, understand the client's business and industry, perform preliminary analytical procedures, set preliminary judgment of materiality and performance materiality, identify significant risks due to fraud or error, assess inherent risk, understand internal control and assess control risk, and finalize overall audit strategy and audit plan. Understanding internal control and assessing control risk is therefore part seven of planning. Only finalizing the audit strategy and audit plan follow understanding internal control and assessing control risk.

11-4 PCAOB Auditing Standard 5 requires that the auditor issue a report on the effectiveness of internal control over financial reporting. To express an opinion on internal controls, the auditor obtains an understanding of and performs tests of controls related to *all* significant account balances, classes of transactions, and disclosures and related assertions in the financial statements. PCAOB Auditing Standard 5 requires the auditor's independent assessment of the internal controls' design and operating effectiveness.

11-5 When obtaining an understanding of internal control, the auditor must assess two aspects about those controls. First, the auditor must gather evidence about the *design* of internal controls. Second, the auditor must gather evidence about whether those controls have been *implemented*.

11-6 The COSO *Internal Control – Integrated Framework* is the most widely accepted internal control framework in the U.S. The COSO framework, updated in 2013, describes internal control as consisting of five components that management designs and implements to provide reasonable assurance that its control objectives will be met. Each component contains many controls, but auditors concentrate on those designed to prevent or detect material misstatements in the financial statements.

11-7 The control environment consists of the actions, policies, and procedures that reflect the overall attitudes of top management, directors, and owners of an entity about internal control and its importance to the entity. The control environment serves as the umbrella for the other four components (risk assessment, control activities, information and communication, and monitoring). Without an effective control environment, the other four are unlikely to result in effective internal control, regardless of their quality. However, all five components are necessary for effectively designed and implemented internal control.

11-8 The five categories of control activities are:

- Adequate separation of duties
  Example: The following two functions are performed by different people: processing customer orders and billing of customers.
- Proper authorization of transactions and activities
  Example: The granting of credit is authorized before shipment takes place.
- Adequate documents and records
  Example: Recording of sales is supported by authorized shipping documents and approved customer orders.
- Physical control over assets and records
  Example: A password is required before an entry can be made into the computerized accounts receivable master file.
- Independent checks on performance
  Example: Bill clerk verifies prices and quantities on sales invoices before they are sent to customers.

11-9 Separation of operational responsibility from record keeping is intended to reduce the likelihood of operational personnel biasing the results of their performance by incorrectly recording information.

Separation of the custody of assets from accounting for these assets is intended to prevent misappropriation of assets. When one person performs both functions, the possibility of that person's disposal of the asset for personal gain and adjustment of the records to relieve himself or herself of responsibility for the asset without detection increases.

11-10 An example of a physical control the client can use to protect each of the following assets or records is:

1. Computers should be in an area protected by security and should be protected from extreme temperatures. Access should be password-protected.
2. Cash received by retail clerks should be entered into a cash register to record all cash received.
3. Adequate backup copies of computerized accounts receivable records should be maintained and access to the master files should be restricted via passwords. Other accounts receivable records should be stored in a locked, fireproof safe.
4. Raw material inventory should be retained in a locked storeroom with a reliable and competent employee controlling access.
5. Perishable tools should be stored in a locked storeroom under control of a reliable employee.
6. Manufacturing equipment should be kept in an area protected by security and fire alarms and kept locked when not in use.

11-10 (continued)

7. Marketable securities should be stored in a safety deposit vault.

11-11 Independent checks on performance are internal control activities designed for the continuous internal verification of other controls. Examples of independent checks include:

- Preparation of the monthly bank reconciliation by an individual with no responsibility for recording transactions or handling cash.
- Recomputing inventory extensions for a listing of inventory by someone who did not originally do the extensions.
- The preparation of the sales journal by one person and the accounts receivable master file by a different person, and a reconciliation of the control account to the master file.
- The counting of inventory by two different count teams.
- The existence of an effective internal audit staff.

11-12 The most important internal control deficiency that permitted the defalcation to occur was the failure to adequately segregate the accounting responsibility of recording billings in the sales journal from the custodial responsibility of receiving the cash. Regardless of how trustworthy James appeared, no employee should be given the combined duties of custody of assets and accounting for those assets.

11-13 Entity level controls, such as the effectiveness of the board of directors' and audit committee's oversight, can have a pervasive affect on many different transaction-level controls. If entity-level controls are deemed to be deficient, then there is greater likelihood that transaction-level controls may be ineffective in their design or operation. In contrast, if entity-level controls are deemed to be highly effective, the auditor may be able to place greater reliance on those controls, which may provide an opportunity to reduce testing of transaction-level controls thereby increasing the efficiency of the audit procedures.

11-14 The proper installation of IT can lead to internal control enhancements by replacing manually performed controls with computer-performed controls. IT-based accounting systems have the ability to handle tremendous volumes of complex business transactions cost effectively. Computer-performed controls can reduce the potential for human error by replacing manual controls with programmed controls that apply checks and balances to each transaction processed. The systematic nature of IT offers greater potential to reduce the risk of material misstatements resulting from random, human errors in processing.

The use of IT-based accounting systems also offers the potential for improved management decisions by providing more and higher-quality information on a more timely basis than traditional manual systems. IT-based systems are usually administered effectively because the complexity requires effective organization, procedures, and documentation. That in turn enhances internal control.

11-15 When entities rely extensively on IT systems to process financial information, there are risks specific to IT environments that must be considered. Key risks include the following:

- *Reliance on the functioning capabilities of hardware and software.* The risk of system crashes due to hardware or software failures must be evaluated when entities rely heavily on IT to produce financial statement information.
- *Systematic versus random errors.* Due to the uniformity of processing performed by IT-based systems, errors in computer software can result in incorrect processing for all transactions processed. This increases the risk of many significant misstatements.
- *Unauthorized access.* The centralized storage of key records and files in electronic form increases the potential for unauthorized online access from remote locations.
- *Loss of data.* Centralized storage of data in electronic form increases the risk of data loss in the event the data file is altered or destroyed.
- *Visibility of audit trail*. The use of IT often converts the traditional paper trail to an electronic audit trail, eliminating source documents and paper-based journals and records.
- *Reduced human involvement.* The replacement of traditional manual processes with computer-performed processes reduces opportunities for employees to recognize misstatements resulting from transactions that might have appeared unusual to experienced employees.
- *Lack of traditional authorization.* IT-based systems can be programmed to initiate certain types of transactions automatically without obtaining traditional manual approvals.
- *Reduced segregation of duties.* The installation of IT-based accounting systems centralizes many of the traditionally segregated manual tasks under the authority of the IT function now that those functions are mainly performed by the computer.
- *Need for IT experience.* As companies rely on IT-based systems to a greater extent, the need for personnel trained in IT systems increases in order to install, maintain, and use systems.

11-16 In most traditional accounting systems, the duties related to authorization of transactions, recordkeeping, and custody of assets are segregated across three or more individuals. As accounting systems make greater use of IT, many of the tasks that were traditionally performed manually are now performed by the computer. As a result, some of the traditionally segregated duties, particularly authorization and recordkeeping, fall under the responsibility of IT personnel. To compensate for the collapsing of duties under the IT function, key IT tasks related to programming, operation of hardware and software, and data control are segregated. Separation of those IT functions restricts an IT employee's ability to inappropriately access software and data files in order to misappropriate assets.

11-17 If general controls are effective, there is an increased likelihood of placing greater reliance on automated application controls. Stronger general controls should lead to greater likelihood that automated application controls operate effectively and data files contain accurate, authorized, and complete information. If general controls are ineffective, there is a potential for material misstatement in each computer-based accounting application, regardless of the quality of automated application controls. If, for example, the systems development process is not properly controlled, there is a greater risk that unauthorized and untested modifications to accounting applications software have occurred that may have affected the automated control.

11-18 Because many companies that operate in a network environment decentralize their network servers across the organization, there is an increased risk for a lack of security and lack of overall management of the network operations. The decentralization may lead to a lack of standardized equipment and procedures. In many instances responsibility for purchasing equipment and software, maintenance, administration, and physical security often resides with key user groups rather than with a centralized IT function. Also, network-related software often lacks the security features, including segregation of duties, typically available in traditionally centralized environments because of the ready access to software and data by multiple users. In database management systems where many applications share the same data, controls can often be strengthened as data are more centralized and duplicate files can be eliminated. However, there are also increased risks in some cases given that multiple users, including individuals outside accounting, access and update data files. Without proper database administration and access controls, risks of unauthorized, inaccurate, and incomplete data files increase. Centralization of data also increases the need to properly back up data information on a regular basis.

11-19 An online sales ordering system poses many potential risks for an audit client. Risks that may exist include:

1. Customer data is susceptible to interception by unauthorized third parties.
2. The client company's data, programs, and hardware are susceptible to potential interception or sabotage by external parties.
3. An unauthorized third party may attempt to transact business with the client company.

These risks can be addressed by the use of firewalls, encryption techniques, and digital signatures. A *firewall* is a system of hardware and software that monitors and controls the flow of e-commerce communications by channeling all network connections through a control gateway. A firewall protects data, programs, and other IT resources from external users accessing the system through networks, such as the Internet. *Encryption techniques* are based on computer programs that transform a standard message into a coded (encrypted) form. One key (the public key) is used for encoding the message and the other key (the private key) is used to decode the message. Encryption

11-19 (continued)

techniques protect the security of electronic communication during the transmission process. Finally, the use of *digital signatures* can enhance internal controls over the online sales order system by authenticating the validity of customers and other trading partners who conduct business with the client company.

■ Multiple Choice Questions From CPA Examinations

11-20 a. (1) b. (1) c. (4)

11-21 a. (3) b. (3) c. (1)

■ Multiple Choice Questions From Becker CPA Exam Review

11-22 a. (4) b. (3) c. (2)

■ Discussion Questions and Problems

11-23

1.	d.	Information and communication
2.	c.	Control activities
3.	a.	Control environment
4.	b.	Risk assessment
5.	e.	Monitoring
6.	c.	Control activities
7.	d.	Information and communication
8.	c.	Control activities
9.	a.	Control environment
10.	b.	Risk assessment

11-24

	INTERNAL CONTROL	a. CONTROL ACTIVITY	b. TRANSACTION-RELATED AUDIT OBJECTIVE(S)
1.	Sales invoices are matched with shipping documents by the computer system and an exception report is generated.	Adequate documents and records	Occurrence
2.	Receiving reports are prenumbered and accounted for on a daily basis.	Adequate documents and records	Completeness Timing
3.	Sales invoices are independently verified before being sent to customers.	Independent checks on performance	Accuracy
4.	Payments by check are received in the mail by the receptionist, who lists the checks and restrictively endorses them.	Adequate separation of duties	Completeness
5.	Labor hours for payroll are reviewed for reasonableness by the computer system.	Independent checks on performance Proper authorization of transactions	Occurrence Accuracy
6.	Checks are signed by the company president, who compares the checks with the underlying supporting documents.	Adequate separation of duties Independent checks on performance	Occurrence Accuracy
7.	Unmatched shipping documents are accounted for on a daily basis.	Physical control over documents and records	Completeness Timing
8.	The computer system verifies that all payroll payments have a valid employee identification number assigned by the human resources department at the time of hiring.	Adequate separation of duties	Occurrence
9.	The accounts receivable master file is reconciled to the general ledger on a monthly basis.	Independent checks on performance	Posting and summarization

11-25

1. a. Adequate documents and records, and independent checks on performance.
   b. Transactions are recorded on the correct dates (cutoff).
   c. Carefully coordinate the physical count of inventory on the last day of the year with the recording of sales to make certain that counted inventory has not been billed and billed inventory has not been counted.

2. a. Adequate documents and records and independent checks on performance.
   b. Transactions are stated at the correct amounts (accuracy).
   c. Changes to the computer master file of prices are reviewed when the master file is updated.

3. a. Proper authorization of transactions and adequate documents and records.
   b. Recorded transactions exist (occurrence).
   c. Include a control in the accounts payable software that requires the input of a valid receiving report number before the software will process a payment on an accounts payable.

4. a. Adequate documents and records, physical control over assets and records, and independent checks on performance.
   b. Recorded transactions exist (occurrence).
   c. 1) Fence in the physical facilities and prohibit employees from parking inside the fencing.
      2) Require the accounting department to maintain perpetual inventory records and take physical counts of actual sides of beef periodically.

5. a. Adequate separation of duties.
   b. Recorded transactions exist (occurrence).
   c. Restrict the accounts payable clerk from being able to make changes to the approved vendor master file. Only allow purchasing personnel to input changes to that master file.

6. a. Independent checks on performance.
   b. Recorded transactions are stated at the correct amounts (accuracy).
   c. Counts by qualified personnel and independent checks on performance.

7. a. Proper authorization of transactions and activities.
   b. Transactions are stated at the correct amounts (accuracy).
   c. 1) Make sure the salesperson has a current price list.

11-25 (continued)

2) Require independent approval of all transactions, including the price, before shipment is made.

8. a. Adequate documents and records.
   b. Recorded transactions exist (occurrence).
   c. 1) Require that payments only be made on original invoices.
      2) Require a receiving report be attached to the vendor's invoice before a payment is made.

11-26 The criteria for dividing duties is to keep all asset custody duties with one person (Cooper). Document preparation and recording is done by the other person (Smith). Singh will perform independent verification. The two most important independent verification duties are the bank reconciliation and reconciling the accounts receivable master file with the control account; therefore, they are assigned to Singh. The duties should be divided among the three as follows:

Robert Smith:	†2	†4	†5	†7	†9	†11	14	16	17
James Cooper:	†1	†3	†6	†8	†10	†12	13		
Mohini Singh:	15	18							

11-27 A schedule showing the pertinent transaction-related management assertions and application controls for each type of misstatement is below and on the following page.

MISSTATEMENT	a. TRANSACTION-RELATED ASSERTION	b. COMPUTER-BASED CONTROLS
1. A customer number on a sales invoice was transposed and, as a result, charged to the wrong customer. By the time the error was found, the original customer was no longer in business.	■ Recorded transactions exist (occurrence) ■ Amounts and other data relating to recorded transactions and events have been recorded appropriately (accuracy)	■ Key entry verification ■ Check digit ■ Reconciliation to customer number on purchase order and bill of lading
2. A former computer operator, who is now a programmer, entered information for a fictitious sales return and ran it through the computer system at night. When the money came in, he took it and deposited it in his own account.	■ Recorded transactions exist (occurrence)	■ Input security controls over cash receipts records ■ Scheduling of computer processing ■ Controls over access to equipment ■ Controls over access to live application programs
3. A nonexistent part number was included in the description of goods on a shipping document. Therefore, no charge was made for those goods.	■ Existing transactions are recorded (completeness)	■ Preprocessing review ■ Programmed controls (e.g., compare part no. to parts list master file)
4. A customer order was filled and shipped to a former customer that had already filed bankruptcy.	■ Recorded transactions exist (occurrence)	■ Preprocessing authorization ■ Preprocessing review ■ Programmed controls (e.g., comparison to customer file)

11-27 (continued)

MISSTATEMENT	a. TRANSACTION-RELATED ASSERTION	b. COMPUTER-BASED CONTROLS
5. The sales manager approved the price of goods ordered by a customer, but he wrote down the wrong price.	■ Amounts and other data relating to recorded transactions and events have been recorded appropriately (accuracy)	■ Preprocessing review ■ Programmed controls (e.g., comparison to the online authorized price list)
6. A computer operator picked up a computer-based data file for sales of the wrong week and processed them through the system a second time.	■ Recorded transactions exist (occurrence) ■ Transactions are recorded in the correct accounting period (cutoff)	■ Correct file controls ■ Cutoff procedures ■ Programmed controls (e.g., check for sequence of dates)
7. For a sale, a data entry operator erroneously failed to enter the information for the salesman's department. As a result, the salesman received no commission for that sale.	■ Existing transactions are recorded (completeness)	■ Conversion verification (e.g., key verification) ■ Programmed controls (e.g., check field for completeness)
8. Several remittance advices were batched together for inputting. The cash receipts clerk stopped for coffee, set them on a box, and failed to deliver them to the data input personnel.	■ Existing transactions are recorded (completeness) ■ Transactions are recorded in the correct accounting period (cutoff)	■ Control totals reconciled to manual totals of all batches ■ Computer accounts for numerical sequence of batches submitted

11-28

PERSON 1	PERSON 2	PERSON 3	PERSON 4
a. ■ Systems analyst ■ Programmer	■ Computer operator	■ Librarian	■ Data control
b. ■ Systems analyst ■ Programmer	■ Computer operator	■ Librarian ■ Data control	N/A
c. ■ Systems analyst ■ Programmer ■ Data control*	■ Computer operator ■ Librarian*	N/A	N/A

* This solution assumes the data control procedures will serve as a check on the computer operator and will allocate work across both persons.

d. If all five functions were performed by one person, internal control would certainly be weakened. However, the company would not necessarily be unauditable, for two reasons: First, there may be controls outside the IT function that constitute effective control. For example, users may reconcile all input and output data on a regular basis. Second, the auditor of a non-public entity is not required to rely on internal control. He or she may take a substantive approach to the audit assuming adequate evidence is available in support of transactions and balances.

11-29 1. Wilcoxon Sports should strengthen several of its IT general controls. The fact that the programmer was able to access the current live version of the sales application program suggests that there are breakdowns in appropriate segregation of duties among IT personnel. Programmers should be restricted from access to actual software used in production. The librarian function should protect access to live versions of the programs and only provide access to operators that allows them to use actual live versions of software to process transactions.

Wilcoxon should consider strengthening its processes for authorizing and approving software changes. More extensive procedures should be implemented regarding requests and approvals for software changes. Only upon the presentation of adequate documentation and approvals should the librarian provide access of a test copy of the software programs to the programmers. Without adequate documentation and approvals, the programmers should not be granted access to software. Furthermore, the librarian should never accept revised programs back from the programmers when there is no supporting documentation that a change was authorized. Approvals for software changes should

11-29 (continued)

include user department approvals, such as those responsible for the sales function.

For larger IT functions, programmers are split into subgroups with some programmers only authorized to address programming issues for application software (e.g., the sales application) while other programmers are only authorized to address programming issues for systems software, such as operating software.

2. Strengthening IT general controls over program changes, restricting access to live software versions, and enhancing segregation of duties will significantly reduce the programmer's ability to make unauthorized changes to software as was done at Wilcoxon Sports. If all program changes must be accompanied by extensive documentation and approvals for those changes, it will be more difficult for programmers to make an unauthorized change.

   Furthermore, restricting programmer access to only test copies of software that have been approved for modification makes it much more difficult for programmers to implement a change in software without someone's knowledge. If the librarian only accepts revised programs for properly authorized changes, then the programmer will be prevented from sneaking a changed program back into live production.

   If programmer functions are separated among programmers such that only a subset is authorized to modify application programs and not system software, then it will require collusion among programmers to implement a change in application software that also requires modification to system software. That segregation would prevent situations like the one at Wilcoxon whereby the programmer was able to make unauthorized changes to both the sales application and the operating system software.

11-30

a. The strengths of Hardwood Lumber Company's computerized accounting system include the following:
   - Separate departments for systems programming, applications programming, operations, and data control.
   - Some employees have READ ONLY capabilities, and others have CHANGE or RUN capabilities.
   - The computer room is locked and requires a key-card for access which enhances security surrounding unauthorized access.
   - There is a librarian who is responsible for maintaining the library of program files.
   - Backup copies of program files and data files are maintained.
   - Programmers are restricted to READ ONLY access to all live application software program files.
   - Data control clerks have no access to software program files.

11-30 (continued)

b. Recommendations to improve Hardwood Lumber Company's Information Systems function:

- The Vice President of Information Systems (VP of IS) should report on a day-to-day basis to senior management (e.g., the president) and should not be under the authority of user personnel. This ensures that the IS function is not subordinate to a user function, which might inappropriately allocate IS resources to that user function's projects.
- The VP of IS should have access to the board of directors and should be responsible for periodically updating the board on significant IS projects. Perhaps, the board should create an IS Steering Committee to oversee IS activities (like the Audit Committee oversees the financial reporting process).
- Operations staff should not have responsibility for maintaining the operating software security features. This responsibility should be assigned to a more senior, trusted IS individual, such as the VP of IS.
- Video monitors should be examined continually. The actual monitors could be viewed on an ongoing basis by building security guards. Hardwood should consider taping what the cameras are viewing for subsequent retrieval in the event of a security breach.
- Hardwood may consider purchasing a vendor-developed access security software package to strengthen online security beyond the features currently provided by the operation software's security features.
- Restrict programmer access to test copies of software programs for only those programs that have been authorized for program change. Access to copies of other programs may not be necessary when those programs have not been authorized for change.
- Grant systems programmers access only to approved test copies of systems software, and grant application programmers access only to approved copies of application software.
- Consider hiring a systems analyst to coordinate all program development projects. Systems analysts can strengthen communications between user and programming personnel, and they can increase the likelihood that a strong systems development process is followed.
- Develop a weekly Job Schedule that outlines the order in which operators should process jobs. The VP of IS should review computer output to determine that it reconciles to the approved Job Schedule. This will increase the likelihood that only approved jobs are processed and that they are processed in the correct sequence.

11-30 (continued)

- Relocate the backup program and data storage to a physically secure room separate from the computer room but offsite to avoid having both the computer room and the backup data being destroyed in the event of damage to the building. Only grant the librarian access to this room. This will prevent the unauthorized removal of program and data files.
- Remove the librarian's CHANGE rights to program and data files. The librarian should not be able to make changes to those files. The librarian should only be able to copy the contents of those files.
- Consider purchasing a vendor-developed librarian software package to assist the librarian in maintaining complete and accurate records of secondary storage programs and data files.
- Make sure only user department personnel have the ability to authorize additions or changes to data files.

11-31 a. The COSO report notes that an organization's technology will continually evolve as the organization evolves. At the same time, cyber attackers are continually finding new ways of hacking information systems and exploiting weaknesses. It is challenging to prevent a cyberattack from occurring, but it is possible for an organization to plan and put in place security systems to the best of their ability.

b. At the control environment level, management and the board of directors need to set the tone that cyber security is a priority. The board of directors needs to be aware of cybersecurity issues. Regular communication between management and the board regarding information technology is necessary. Increasingly, companies are considering the need to have board members with information technology or cyber expertise.

c. The COSO report identifies the following five categories of perpetrators and motives:

- Nation states and spies: foreign nations attempting to steal national security information or other intellectual property
- Organized criminals: attempt to steal money or customer identity information
- Terrorists: individuals or groups attempting to launch cyberattacks to disrupt infrastructure such as financial institutions
- Hacktivists: individuals attempting to steal and disclose sensitive information to make a social or political statement
- Insiders: individuals inside the organization who may try to sell private information

11-31 (continued)

d. The report suggests that both preventive and detective controls need to be implemented. Preventive controls are designed to prevent a cyberattack from occurring, such as multiple firewalls. Controls designed to rapidly detect a cyberattack will allow management to react quickly in order to minimize damage. General controls as discussed in this chapter will also help to prevent and detect cyberattacks. The report also suggests there are IT-specific frameworks that organizations can rely on as well, such as COBIT (Control Objectives for Information and Related Technology).

■ Case

11-32 a. **Sales**

TRANSACTION-RELATED ASSERTION	CONTROL
Occurrence	■ Supervisor approves all invoices. ■ Accounts receivable clerk has no access to cash. ■ Monthly statements are sent to customers. ■ Supervisor approves all credit.
Completeness	■ Cash register is at the front of the store. ■ Sales clerks handle no cash. ■ Sales clerks summarize daily sales, which determine their commission. This summary is compared daily to total sales. ■ Sales transactions are used to update perpetuals and monthly physical inventory is taken.
Accuracy	■ Owner sets all prices. ■ Supervisor rechecks all calculations. ■ Accountant reconciles all computer totals to sales staff summary totals and supervisor's sales summary. ■ Monthly statements are sent to customers. ■ Computer is used to update records. ■ Monthly statements are sent. ■ The aged trial balance is compared to the general ledger.
Classification	None
Cutoff	■ Sales transactions are recorded daily.

11-32 (continued)

b. **Cash Receipts**

TRANSACTION-RELATED AUDIT OBJECTIVE	CONTROL
Occurrence	■ Monthly bank reconciliation is prepared. ■ Accounts receivable clerk compares duplicate deposit slip from bank to sales and cash receipts journal.
Completeness	■ Cash register is used for cash sales. ■ Cash collected on receivables is prelisted. ■ Supervisor deposits money in a locked box.
Accuracy	■ Supervisor recaps cash sales and compares totals to the cash receipts tapes. ■ Monthly bank reconciliation prepared. ■ Accounts receivable clerk compares duplicate deposit slip from bank to cash sales and cash receipts journal. ■ Monthly statements are sent to customers. ■ Computer is used to update records. ■ The aged trial balance is compared to the general ledger.
Classification	None
Cutoff	■ Cash is deposited daily.

c. **Sales and Cash Receipts**

Deficiencies

- Supervisor enters all sales in the cash register, recaps sales and cash, and compares the totals to the tapes. She also receives all invoices from sales clerks. (This deficiency is offset by the daily summary form prepared by sales clerks and used to calculate sales clerks' commissions.)
- Lack of accounting for a numerical sequence of sales invoices. (Partially offset by control totals used by comparing sales clerks' and supervisor's control totals.)
- No internal verification of key entry for customer name, date, and sales classifications on either cash receipts or sales.
- There is no internal verification of general totals, posting to accounts receivable master file, or posting to the general ledger.
- There is a lack of internal verification of all of the accounting work done by the accounts receivable clerk.