

# STUDY UNIT TEN

## RISK ASSESSMENT AND CONTROLS

10.1	Control Environment .....	1
10.2	Control Procedures .....	5
10.3	Foreign Corrupt Practices Act .....	12
10.4	Core Concepts .....	13

This study unit is the **first of three** on **internal controls**. The relative weight assigned to this major topic in Part 1 of the exam is **15%** at **skill level A** (two skill types required). The three study units are

Study Unit 10: Risk Assessment and Controls

Study Unit 11: Internal Auditing

Study Unit 12: Systems Controls and Security Measures

After studying the outlines and answering the multiple-choice questions, you will have the skills necessary to address the following topics listed in the IMA's Learning Outcome Statements:

### Part 1 – Section C.1 Risk assessment and controls

The candidate should be able to:

- a. demonstrate an understanding of risk assessment and the management of risk
- b. recognize how a company's organizational structure, policies, objectives, and goals, as well as its management philosophy and style, influence the scope and effectiveness of the control environment
- c. demonstrate an understanding of how the organizational structure defines the key areas of authority and responsibility
- d. recognize that the board of directors is responsible for ensuring that the company is operated in the best interest of shareholders
- e. recognize that internal controls are designed to provide reasonable assurance regarding achievement of an entity's objectives involving (i) effectiveness and efficiency of operations, (ii) reliability of financial reporting, and (iii) compliance with applicable laws and regulations
- f. identify reasons why personnel policies and procedures, particularly with the employment and promotion of competent personnel, are integral to an efficient control environment
- g. define and give examples of segregation of duties
- h. identify and explain why the following four types of functional responsibilities should be performed by different organizations or people: (i) authority to execute transactions, (ii) recording transactions, (iii) custody of assets involved in the transactions, and (iv) periodic reconciliations of the existing assets to recorded amounts
- i. demonstrate an understanding of the importance of independent checks
- j. identify examples of safeguarding controls
- k. recognize that the most visible safeguarding controls are designed and implemented to protect an organization's assets
- l. recognize that the use of prenumbered forms, as well as specific policies and procedures detailing who is authorized to receive specific documents, etc., is a means of control
- m. define inherent risk, control risk, and detection risk
- n. understand that risk encompasses the total dollar value of assets that are exposed to loss, as well as the probability that such a loss will occur
- o. recognize that, while controls designed to prevent fraud are important and make perpetration of fraud more difficult, they are not complete insurance against fraud
- p. identify the major internal control provisions of Foreign Corrupt Practices Act

### **10.1 CONTROL ENVIRONMENT**

## 1. The System of Internal Control

- a. Management accountants are interested in a broad range of controls. Thus, **SMA 2A**, *Management Accounting Glossary*, defines internal control as:

*The whole system of controls (financial and otherwise) established by management to carry on the business of the enterprise in an orderly and efficient manner, to ensure adherence to management policies, safeguard the assets, and ensure as far as possible the completeness and accuracy of the records.*

- b. The AICPA offers a similar perspective with this definition:

*Internal control is a process -- effected by an entity's board of directors, management, and other personnel -- designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations.*

- c. The proper design and operation of an organization's system of internal controls is the **responsibility of management**. **Section 404** of the **Sarbanes-Oxley Act of 2002** requires publicly traded companies to issue a report stating that
- 1) Management takes responsibility for establishing and maintaining the firm's system of internal controls, and
  - 2) The system has been functioning effectively over the reporting period.
- d. **Risk assessment** is the process whereby management identifies the organization's vulnerabilities.
- 1) All systems of internal control involve tradeoffs between cost and benefit. For this reason, no system of internal control can be said to be "100% effective."
  - 2) Organizations accept the fact that risk can only be **mitigated**, not eliminated. **Risk management** is the ongoing process of designing and operating internal controls that mitigate the risks identified in the organization's risk assessment.
- e. Two conceptual areas vital to any understanding of internal control are the control environment and control procedures.

2. The **control environment** reflects the "tone at the top." Thus, it encompasses the attitudes and actions of the board of directors and managers regarding the significance of control. It provides the discipline and structure for the achievement of the objectives of internal control by influencing the control consciousness of the people within the organization. According to the AICPA, the control environment has the following elements:

- a. **Integrity and ethical values.** Control effectiveness is limited by the integrity and ethical values of the people who design, implement, and monitor controls. Integrity and ethical values are essential because they affect all aspects of control. Ethical behavior results from the entity's standards, the way they are transmitted, and how they are reinforced. Hence, management should remove incentives for dishonest, illegal, or unethical behavior. Management also should communicate entity values and behavioral standards by means of policy statements and codes of conduct and by setting an example.
- b. **Commitment to competence.** Competence consists of the knowledge and abilities necessary for members of the organization to complete tasks. Thus, management should consider the competence required for particular tasks and how that relates to necessary knowledge and abilities.

- c. **Board of directors or audit committee participation.** Control consciousness is in large part a function of certain attributes of the board or audit committee: degree of independence from management, their experience and prestige, the commitment to oversight of activities, the propriety of their actions, the extent to which significant issues are discussed with management, and their relationship with internal and external auditors.
  - d. **Management philosophy and operating style.** Philosophy and operating style embrace such characteristics as the attitude toward business risk; the attitude and actions with respect to financial reporting, such as whether accounting estimates and the selection of accounting principles are appropriate; and attitudes toward activities of the information system, the accounting function, and employees.
  - e. **Organizational structure.** This framework should allow the organization to achieve its objectives by planning, executing, controlling, and monitoring appropriate activities. Key areas of authority and responsibility as well as appropriate lines of reporting are reflected in a relevant organizational structure. The structure should be suited to the entity's needs and be reflective of its size and activities.
  - f. **Assignment of authority and responsibility.** This element of the control environment pertains not only to authority and responsibility for operations but also to determination of reporting relationships and authorization of transactions. Other relevant concerns are the propriety of business practices, the qualifications of key employees, and the resources needed to execute duties. Assignment of authority and responsibility also encompasses efforts to ensure that employees know organizational objectives, how their interrelated activities contribute to achieving the objectives, and how and for what they will be accountable.
  - g. **Personnel policies and practices.** This element concerns, among other things, hiring, training, evaluating, promoting, and compensating employees. Thus, hiring standards that emphasize education, prior experience, past achievements, and evidence of integrity and ethical behavior display a commitment to employing people who are competent and trustworthy. Training policies should impart to employees a knowledge of their roles and responsibilities and expectations about their conduct and performance. Promotions based on periodic performance appraisals should reflect a commitment to rewarding merit.
3. A **board of directors** consists of inside members (such as officers and employees) and outside members. It is the governing authority of a corporation and is therefore responsible for establishing overall corporate policy. Thus, the directors have a **fiduciary duty** to the organization and its shareholders. They must exercise **reasonable care** in the performance of their duties, which entails being informed about and conversant with pertinent corporate information, attending meetings, analyzing corporate financial statements, etc.
- a. Directors also owe a **duty of loyalty**, which prohibits dealing with the corporation unless full disclosure is made or usurping any corporate opportunity without giving the entity the right of first refusal.
  - b. Under the **business judgment rule**, however, a director will not have personal liability for his/her conduct if (s)he acts in good faith; is not motivated by fraud, conflict of interest, or illegality; and is not guilty of gross negligence. Thus, honest errors of judgment do not result in liability.
    - 1) Moreover, a director may rely on information provided by an officer or an expert if the reliance is reasonable.

- c. Directors typically
  - 1) Select and remove officers
  - 2) Determine the capital structure
  - 3) Add, amend, or repeal bylaws
  - 4) Initiate fundamental changes, e.g., mergers or spinoffs, which must be approved by the shareholders
  - 5) Declare dividends
  - 6) Set the compensation of officers and management
- 4. An **audit committee** is a subcommittee made up of outside directors who are independent of management. Its purpose is to help keep external and internal auditors independent of management and to assure that the directors are exercising due care.
  - a. The role of an audit committee or an equivalent body in strengthening the position of both internal and external auditing is now widely recognized. The following are some of its characteristics and responsibilities:
    - 1) The appropriate governing authority should develop and approve a written charter describing the audit committee's duties and responsibilities.
    - 2) The audit committee should review the independence of the independent public accountant.
    - 3) Reports to shareholders or other stakeholders should include a letter from the chair of the audit committee describing its responsibilities and activities.
    - 4) The audit committee should monitor compliance with codes of conduct.
    - 5) The audit committee should have necessary resources available.
    - 6) The audit committee should oversee the regulatory reporting process.
    - 7) The audit committee should monitor instances in which management seeks second opinions on significant accounting issues.
  - b. Many stock exchanges require a listed organization to have an audit committee.
  - c. An audit committee composed of nonmanagement directors promotes the independence of internal as well as external auditors, especially when it selects the external audit firm and the chief audit executive (the person in the organization with responsibility for oversight of internal auditing activities). Thus, a strong audit committee insulates the auditors from influences that may compromise their independence and objectivity.
    - 1) An audit committee may also serve as a mediator of disputes between the auditors and management.
  - d. **Audit committee functions** include
    - 1) Selecting an external auditor and reviewing the audit fee and the engagement letter
    - 2) Reviewing the external auditor's overall audit plan
    - 3) Reviewing preliminary annual and interim financial statements
    - 4) Reviewing results of engagements performed by external auditors
    - 5) Approving the charter of the internal audit activity (IAA)
    - 6) Reviewing and approving the internal audit activity's plans and resource requirements and receiving a summary of the IAA's work schedule, staffing plan, and financial budget
    - 7) Directly communicating with the chief audit executive who regularly attends and participates in meetings
    - 8) Reviewing evaluations of risk management, control, and governance processes reported by the internal auditors

- 9) Receiving distributions of final engagement communications by the internal auditors as an entity able to ensure that engagement results are given due consideration
  - 10) Reviewing policies on unethical and illegal procedures
  - 11) Reviewing financial statements to be transmitted to regulatory agencies
  - 12) Reviewing observations of organization personnel
  - 13) Participating in the selection of accounting policies
  - 14) Reviewing the impact of new or proposed legislation or governmental regulations
  - 15) Reviewing the organization's insurance program
  - 16) Reviewing the external auditor's management letter
- e. External auditors have recognized the importance of reporting to audit committees. Among the matters that may be communicated are internal-control-related matters, significant accounting policies, management judgments and accounting estimates, significant audit adjustments, disagreements with management, and difficulties encountered during the audit.
- 1) One of the factors encompassed by the control environment component of internal control is participation by the board, audit committee, or other governing authority. As previously mentioned, the control consciousness of the entity is improved if the audit committee is independent, composed of experienced and respected people, extensively involved in scrutinizing entity activities, willing to raise and pursue difficult questions with management, and in close communication with the internal and external auditors.
  - 2) Fraud involving senior management or fraud that materially misstates the financial statements should be reported directly to the audit committee.
    - a) The auditors also should be assured that the audit committee is adequately informed about other illegal acts coming to their attention.

## 10.2 CONTROL PROCEDURES

1. **Control activities** are designed and placed in operation to **ensure that management's directives are executed**. Hence, they should include the requisite steps to respond to the risks that threaten the attainment of organizational objectives.
  - a. For this purpose, controls should be suitably designed to prevent or detect unfavorable conditions arising from **particular risk exposures**. They should also be placed in operation and operate effectively. If controls are not always in force, they cannot operate effectively no matter how effective their design.
  - b. Control procedures are implemented to **manage or limit risk** in accordance with the entity's risk assessments whenever risk exposures exist that threaten loss of assets or misstatements of accounting or management information.
  - c. **Risk** is the uncertainty of the occurrence of an event that could have an effect on the achievement of organizational objectives. Risk is measured in terms of consequences and likelihood.
    - 1) Accordingly, the **expected value** of a loss due to a risk exposure may be calculated if monetary estimates of potential losses and their probabilities can be made. This expected value is the maximum that should be spent on controls designed to minimize the risk.

- 2) Risk exposure should be evaluated and appropriate controls should be implemented with regard to
  - a) Reliability and integrity of financial and operational information
  - b) Effectiveness and efficiency of operations
  - c) Safeguarding of assets
  - d) Compliance with laws, regulations, and contracts
2. The **AICPA model** for internal control recognizes **four major areas** of control activities: performance reviews, information processing, segregation of duties, and physical controls. Of these, the last two are the most important for management accountants.
  - a. **Performance reviews** compare actual performance with budgets, forecasts, and prior period performance. When prepared by persons other than those under review, they embody an **independent check**. They may also compare sets of operating or financial data and provide analyses of the relationships and actions taken to detect and correct unfavorable conditions. Another form of review concerns the performance of an activity or function. An example is a bank's analysis of consumer loan approvals and collection by branch, region, or loan type.
  - b. **Information processing controls** concern the accuracy, completeness, or authorization of transactions. The two categories of information systems controls are general controls and application controls. See Study Unit 12.
3. **Segregation of duties** involves assigning different employees to perform functions such that an employee acting alone is prevented from committing an error or concealing a fraud in the normal course of his/her duties.
  - a. Four types of **functional responsibilities** should be segregated:
    - 1) The **authority to execute transactions**
    - 2) The **recording of transactions**
    - 3) **Custody of the assets** affected by the transactions
    - 4) **Periodic reconciliation** of the existing assets to recorded amounts
  - b. **EXAMPLES.** The following functions should all be vested in different persons or departments.
    - 1) In the **purchases-payables cycle**: the initiation of a purchase, receipt and checking in of the merchandise, authorization to pay the vendor, custody of the merchandise, record keeping for the merchandise, and verification that the amounts of the merchandise on hand match the amounts in the books.
    - 2) In the **payroll cycle**: authorization of pay rates and deductions, hiring and termination of employees, payroll preparation, check distribution, and reconciliation of checks cut and cleared to the payroll register and HR records.
    - 3) In the **production cycle**: planning production and inventory levels, inventory custody, inventory recording, cost accounting, and reconciliation of materials requisitions to production reports.
    - 4) In the **sales-receivables cycle**: authorization of customer credit levels, authorization of a sale to a customer, custody of product, custody of cash, record keeping, and reconciliation of accounts receivable records to cash receipts.
  - c. The objective of **safeguarding assets** requires that access be limited to authorized personnel. Access includes both **direct physical access** and **indirect access** through the preparation or processing of documents that authorize the use or disposition of assets.
    - 1) Access is required in normal operations, so limiting access to those authorized is the maximum feasible constraint.
    - 2) The number and competence of authorized personnel should be influenced by the nature of the assets and the related **susceptibility to loss** through errors and fraud. Limitation of direct access to assets requires appropriate physical segregation and protective equipment or devices.

- 3) Controls to safeguard assets are numerous. The following is by no means a complete list of examples:
  - a) The use of cash registers; also, establishment of a lockbox system for collecting cash receipts from customers, e.g., direct deposit in a bank, intact deposit of daily receipts, and custody of cash by the treasury function.
  - b) Controls to prevent improper granting of credit, approval of credit memos by persons other than sales agents, and approval of writeoffs of uncollectibles by a person independent of the credit manager or the accounts receivable function.
  - c) Use of **sequentially prenumbered forms** accounted for by an independent third party to permit detection of unrecorded and unauthorized transactions; omitting amounts from the copy of a purchase order sent to the receiving department to ensure a fair count of the goods received; requiring proper documentation, that is, a purchase order, supplier's invoice, and receiving report, before authorization of payment for goods received; and cancelation of vouchers and supporting documents to prevent duplicate payments.
  - d) Preparation of payroll from time cards approved by line supervisors; distribution of paychecks by the treasury function, not line supervisors; and custody of unclaimed checks by an independent party.
  - e) Custody of securities by the treasury function, the presence of at least two authorized persons when the safe deposit box is opened, recording and reconciliation of identifying information about securities, and registration in the name of the owner.
  - f) Controls over excess use of materials in production; custody of inventories by the storekeeper, with proper documentation of transfers; and perpetual inventory records.
  - g) Restriction of access to property, plant, and equipment and periodic inspections by internal auditing.
  - h) The controls over computer processing.
  - i) Physical measures taken to protect assets from natural disasters (e.g., floods, wind damage, or earthquakes).
- d. **Reconciliation of recorded accountability with assets.** The performance of this function by someone other than the person with custody of the assets is an important part of mitigating the risk of errors and fraud. It constitutes an **independent check**.
  - 1) A comparison revealing that the assets do not agree with the recorded accountability provides evidence of unrecorded or improperly recorded transactions.
    - a) The converse, however, does not necessarily follow. For example, agreement of a cash count with the recorded balance does not provide evidence that all cash received has been properly recorded.
  - 2) The frequency of such comparisons for the purpose of safeguarding assets depends on the nature and amount of the assets involved and the cost of making the comparison.
    - a) For example, it may be reasonable to count cash daily, but not reasonable to take a physical inventory at that interval.
    - b) However, a daily inventory of products in the custody of route sales reps, for example, may be necessary as a means of determining their accountability for sales. Similarly, the value and vulnerability of some products may make frequent complete inventories worthwhile.

4. **Physical controls** pertain to the security over tangible objects, such as assets and records. An example is the use of secured facilities. Physical controls also include authorization for access to computer programs and data and periodically counting actual amounts and comparing them with amounts shown on control records (see comparison of recorded accountability with assets in d. above).
5. **Compensating controls** replace the normal controls, such as segregation of duties, when the latter cannot feasibly be implemented. For example, in the finance and investment cycle, top management may authorize and execute investments and have access to the records, stock certificates, etc. The compensating control in this case is for at least two people to perform each function.
  - a. An alternative to performance of each function by at least two people is to provide oversight. Thus, the board may authorize an investment, with other functions (custody of stock certificates, management of the portfolio, and oversight of record keeping) performed by a top manager. Other compensating controls in the finance and investment cycle include periodic communications with the board, oversight by a committee of the board, and internal auditing's reconciliation of the securities portfolio with the recorded information.
6. The AICPA's **audit risk model** for the account balance or class of transactions level describes the components of audit risk, which is the risk that an auditor may unwittingly fail to modify his/her opinion on materially misstated financial statements. These components are defined as follows:
  - a. **Inherent risk (IR)** is the susceptibility of a financial statement assertion to material misstatement in the absence of related controls. This risk is greater for some assertions than for others, e.g., cash has a greater inherent risk than property, plant, and equipment.
  - b. **Control risk (CR)** is the risk that a possible material misstatement of an assertion will not be prevented or detected by the related controls in a timely manner. This risk depends on the effectiveness of the design and operation of those controls.
    - 1) However, control risk cannot be eliminated because of the **inherent limitations** of internal control, for example, the possibility of simple error or mistake due to faulty human judgment, the ability of management to override internal control inappropriately, the potential for circumventing internal control as a result of collusion by two or more people, or an unfavorable relationship of the cost of control to its benefits.
  - c. **Detection risk (DR)** is the risk that a material misstatement of an assertion will not be detected by the auditor, for example, because the auditor merely sampled the account balance or class of transactions, selected an inappropriate audit procedure, misapplied an audit procedure, or misinterpreted the audit results.
    - 1) The level of detection risk is the only one of the three subject to the auditor's direct control.
  - d. **Total audit risk (AR)** may be stated as follows:
 
$$AR = IR \times CR \times DR$$
7. **Fraud** differs from error because it is intentional. It typically involves pressures or incentives to engage in wrongdoing and a perceived opportunity to do so. Examples are fraudulent financial reporting and misappropriation of assets.
  - a. Internal controls are designed to, among other things, prevent fraud. However, because of the concealment aspects of fraudulent activity (e.g., collusion or falsification of documents), the controls cannot give absolute assurance that material fraud will be prevented or detected.



8. Sawyer and Dittenhofer, *Sawyer's Internal Auditing* (Altamonte Springs, FL: The Institute of Internal Auditors, 5th ed., 2003, pages 82-86), defines control and provides a description of the means of achieving control that is useful to management accountants as well as to internal auditors. Sawyer defines **control** as

*The employment of all the means devised in an enterprise to promote, direct, restrain, govern, and check upon its various activities for the purpose of seeing that enterprise objectives are met. These means of control include, but are not limited to, form of organization, policies, systems, procedures, instructions, standards, committees, charts of accounts, forecasts, budgets, schedules, reports, records, checklists, methods, devices, and internal auditing.*

- a. **Organization.** As a means of control, organization is an approved intentional structuring of roles assigned to people within the enterprise so that the enterprise can achieve its objectives efficiently and economically.
- 1) Responsibilities should be divided so that no one person will control all phases of any transaction.
  - 2) Managers should have the authority to take the action necessary to discharge their responsibility.
  - 3) Individual responsibility should always be clearly defined so that it can be neither sidestepped nor exceeded.
  - 4) An official who assigns responsibility and delegates authority to subordinates should have an effective system of follow-up for making sure that tasks assigned are properly carried out.
  - 5) The individuals to whom authority is delegated should be required to exercise that authority without close supervision. However, they should check with their superiors for exceptions.
  - 6) People should be held accountable to their superiors for the manner in which they have discharged their responsibilities.
  - 7) The organization should be flexible enough to permit changes in its structure when operating plans, policies, and objectives change.
  - 8) Organizational structures should be as simple as possible.
  - 9) Organization charts and manuals should be prepared that will help plan and control changes in, as well as provide better understanding of, the organization, chain of authority, and assignment of responsibilities.
- b. **Policies.** A policy is any stated principle that requires, guides, or restricts action. Policies should follow certain principles.
- 1) Policies should be clearly stated in writing in systematically organized handbooks, manuals, or other publications, and properly approved.
  - 2) Policies should be systematically communicated to all officials and appropriate employees of the organization.
  - 3) Policies must conform with applicable laws and regulations, and they should be consistent with objectives and general policies prescribed at higher levels.
  - 4) Policies should be designed to promote the conduct of authorized activities in an effective, efficient, and economical manner and to provide a satisfactory degree of assurance that the resources of the enterprise are suitably safeguarded.
  - 5) Policies should be periodically reviewed, and they should be revised when circumstances change.

- c. **Procedures.** Procedures are methods employed to carry out activities in conformity with prescribed policies. The same principles applicable to policies are also applicable to procedures. In addition,
  - 1) To reduce the possibility of fraud and error, procedures should be so coordinated that one employee's work is automatically checked by another who is independently performing separate prescribed duties. In determining the extent to which automatic internal checks should be built into the system of control, such factors as degree of risk, cost of preventive procedures, availability of personnel, operational impact, and feasibility should be considered.
  - 2) For nonmechanical operations, prescribed procedures should not be so detailed as to stifle the use of judgment.
  - 3) To promote maximum efficiency and economy, prescribed procedures should be as simple and as inexpensive as possible.
  - 4) Procedures should not be overlapping, conflicting, or duplicative.
  - 5) Procedures should be periodically reviewed and improved as necessary.
- d. **Personnel.** People hired or assigned should have the qualifications to do the jobs assigned to them. The best form of control over the performance of individuals is supervision. Hence, high standards of supervision should be established. The following practices help improve control.
  - 1) New employees should be investigated as to honesty and reliability.
  - 2) Employees should be given training and refresher courses that provide the opportunity for improvement and keep them informed of new policies and procedures.
  - 3) Employees should be given information on the duties and responsibilities of other segments of the organization so they may better understand how and where their jobs fit into the organization as a whole.
  - 4) The performance of all employees should be periodically reviewed to see whether all essential requirements of their jobs are being met. Superior performance should be given appropriate recognition. Shortcomings should be discussed with employees so that they are given an opportunity to improve their performance or upgrade their skills.
- e. **Accounting.** Accounting is the indispensable means of financial control over activities and resources. It furnishes a framework that can be fitted to assignments of responsibility. Moreover, it is the financial scorekeeper of the enterprise. The problem lies in what scores to keep. Here are some basic principles for accounting systems.
  - 1) Accounting should fit the needs of managers for rational decision making rather than the dictates of some textbook or canned check list.
  - 2) Accounting should be based on lines of responsibility.
  - 3) Financial reports of operating results should parallel the organizational units responsible for carrying out operations.
  - 4) Accounting should be such that controllable costs can be identified.

- f. **Budgeting.** A budget is a statement of expected results expressed in numerical terms. As a control, it sets a standard for input of resources and what should be achieved as output and income.
- 1) Those who are responsible for meeting a budget should participate in its preparation.
  - 2) Those responsible for meeting a budget should be provided with adequate information that compares budgets with actual events and shows reasons for any significant variances.
  - 3) All subsidiary budgets should tie into the overall budget for the enterprise.
  - 4) Budgets should set measurable objectives; they are meaningless unless managers know what they are budgeting for.
  - 5) Budgets should help sharpen the organizational structure because objective budgeting standards are difficult to set in a confused combination of subsystems. Budgeting is therefore a form of discipline and coordination.
- g. **Reporting.** In most organizations, management functions and makes decisions on the basis of reports it receives. Therefore, reports should be timely, accurate, meaningful, and economical. Here are some principles for establishing a satisfactory internal reporting system.
- 1) Reports should be made in accordance with assigned responsibilities.
  - 2) Individuals or units should be required to report only on those matters for which they are responsible.
  - 3) The cost of accumulating data and preparing reports should be weighed against the benefits to be obtained from them.
  - 4) Reports should be as simple as possible and consistent with the nature of the subject matter. They should include only information that serves the needs of the readers. Common classifications and terminology should be used as much as possible to avoid confusion.
  - 5) When appropriate, performance reports should show comparisons with predetermined standards of cost, quality, and quantity. Controllable costs should be segregated.
  - 6) When performance cannot be reported in quantitative terms, the reports should be designed to emphasize exceptions or other matters requiring management attention.
  - 7) For maximum value, reports should be timely. Timely reports based partly on estimates may be more useful than delayed reports that are more precise.
  - 8) Report recipients should be polled periodically to see if they still need the reports they are receiving or if the report could be improved.

### 10.3 FOREIGN CORRUPT PRACTICES ACT

1. The **Foreign Corrupt Practices Act (FCPA)**, enacted in 1977, had its origins in the Watergate investigations. The FCPA is designed to prevent secret payments of corporate funds for purposes that Congress has determined to be contrary to public policy.
  - a. The Act amends the Securities Exchange Act of 1934 to prohibit a domestic concern, including any person acting on its behalf, whether or not doing business overseas and whether or not registered with the SEC, from offering or authorizing corrupt payments to any
    - 1) Foreign official
    - 2) Foreign political party or official thereof
    - 3) Candidate for political office in a foreign country
  - b. Only political payments to foreign officials are prohibited. Payment to foreign business owners or corporate officers are not addressed by the FCPA.
  - c. **Corrupt payments** are payments for the purpose of inducing the recipient to act or refrain from acting so that the domestic concern might obtain or retain business.
    - 1) The FCPA prohibits a mere offer or promise of a bribe, even if it is not consummated.
    - 2) The FCPA prohibits payment of anything of value. De minimis gifts and tokens of hospitality are acceptable.
    - 3) Payments are prohibited if the person making them knew or should have known that some or all of them would be used to influence a governmental official.
  - d. Foreign officials do not include clerical or ministerial employees.
    - 1) **EXAMPLE:** Payments made to a clerk to expedite the processing of goods through customs may not be prohibited by the Act.
    - 2) Such payments are not prohibited as long as the recipient has no discretion in carrying out a governmental function.
    - 3) Payments that are allowed under the written law of the foreign country are also not prohibited.
  - e. Regardless of whether they have foreign operations, all public companies must make and keep **books, records, and accounts in reasonable detail** that accurately and fairly reflect transactions and dispositions of assets.
  - f. All public companies must devise and **maintain a system of internal accounting control** sufficient to provide reasonable assurance that
    - 1) Transactions are executed in accordance with management's general or specific authorization.
    - 2) Transactions are recorded as necessary to
      - a) Permit preparation of financial statements in conformity with generally accepted accounting principles (GAAP) or any other criteria applicable to such statements and
      - b) Maintain accountability for assets.
    - 3) Access to assets is permitted only in accordance with management's general or specific authorization.
    - 4) The recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.
  - g. The penalties for an individual for each criminal violation of the corrupt practices provisions are a fine of up to \$10,000 or imprisonment for up to 5 years, or both. A corporation may be assessed a fine of up to \$1,000,000 for violation of the same section. Fines imposed upon individuals may not be paid directly or indirectly by an employer.

- h. The implications of the Foreign Corrupt Practices Act of 1977 extend well beyond its anti-bribery provisions. All American businesses and business people are involved. Management is particularly affected. The responsibility for internal control is not new, but the potential for civil and criminal liabilities represents an added burden. The impact of the law and the threat its ambiguities pose may alter business operations. Management might decide to abandon direct selling operations in foreign countries in favor of the use of foreign agents in hopes that this might lessen their “reason to know.”
- i. A written code of ethics and conduct is a necessity. This code should be communicated and monitored by internal auditors for compliance. The code might include an explanation of the Foreign Corrupt Practices Act and its penalties. A firm may require written representations from employees that they have read and understood the provisions of the code. Written representations regarding compliance might also be requested at future times. Foreign agents should be made aware of the prohibitions of indirect payments.

## 10.4 CORE CONCEPTS

### Control Environment

- The proper design and operation of a company’s **system of internal control** are the **responsibility of management**.
- **Risk assessment** is the process whereby management identifies the organization’s vulnerabilities.
- The **control environment** encompasses the **attitudes and actions** of the board of directors and managers regarding the significance of control.
- An **audit committee** is a subcommittee of the board of directors whose purpose is to help **keep external and internal auditors independent of management**.

### Control Procedures

- **Control activities** are designed and placed in operation to ensure that **management’s directives are executed**.
- **Control procedures** are implemented to **manage or limit risk** in accordance with the entity’s risk assessments.
- The **AICPA model** for internal control recognizes **four major areas** of control activities: performance reviews, information processing, segregation of duties, and physical controls.
- Effectively segregating duties involves **keeping four functional responsibilities separate**: the authority to execute transactions, the recording of transactions, the custody of assets, and periodic reconciliation.
- The objective of **safeguarding assets** requires that access be limited to authorized personnel. Access includes both **direct physical access** and **indirect access** through the preparation or processing of documents.

### Foreign Corrupt Practices Act

- The **Foreign Corrupt Practices Act of 1977** was designed to prevent secret payments of corporate funds for purposes of bribing foreign officials, foreign political parties, or candidates for office in foreign countries.
- Under the Act, all public companies must devise and maintain a **system of internal accounting control**.