CHAPTER 3
INTERNAL CONTROL OVER FINANCIAL REPORTING: MANAGEMENT’S RESPONSIBILITIES AND IMPORTANCE TO THE EXTERNAL AUDITORS
LEARNING OBJECTIVES

1. Articulate the importance of internal control over financial reporting for organizations and their external auditors

2. Define internal control as presented in COSO’s updated *Internal Control, Integrated Framework* and identify the components of internal control

3. Describe the control environment component of internal control, list its principles, and provide examples of each principle
LEARNING OBJECTIVES

4. Describe the risk assessment component of internal control, list its principles, and provide examples of each principle

5. Describe the control activities component of internal control, list its principles, and provide examples of each principle

6. Describe the information and communication component of internal control, list its principles, and provide examples of each principle
LEARNING OBJECTIVES

7. Describe the monitoring component of internal control, list its principles, and provide examples of each principle

8. Identify management’s responsibilities related to internal control over financial reporting, including the factors management considers when assessing control deficiencies
THE AUDIT OPINION FORMULATION PROCESS

I. Making Client Acceptance and Continuance Decisions
   Chapter 14

II. Performing Risk Assessment
    Chapters 3, 7, and 9–13

III. Obtaining Evidence about Internal Control Operating Effectiveness
     Chapters 8–13 and 16

IV. Obtaining Substantive Evidence about Accounts, Disclosures and Assertions
    Chapters 8–13 and 16

V. Completing the Audit and Making Reporting Decisions
   Chapters 14 and 15

The Auditing Profession, the Risk of Fraud and Mechanisms to Address Fraud: Regulation, Corporate Governance, and Audit Quality
   Chapters 1 and 2

Professional Liability and the Need for Quality Auditor Judgments and Ethical Decisions
   Chapter 4

The Audit Opinion Formulation Process and A Framework for Obtaining Audit Evidence
   Chapters 5 and 6
• To achieve the objective of reliable financial reporting, organizations need to have effective controls in place
• Such controls were not in place at Chesapeake Petroleum and Supply, Inc.
  • The CFO had authorizing and signing control over company checks and exclusive control over petty cash
  • He pled guilty to embezzling more than $2.7 million from the company
PROFESSIONAL JUDGMENT IN CONTEXT - IMPORTANCE OF INTERNAL CONTROL FOR SAFEGUARDING ASSETS

• Why is internal control over financial reporting important to an organization? (LO 1)
• How does internal control help an organization achieve reliable financial reporting? (LO 1)
• Why does an external auditor need to know about a client’s internal control? (LO 1)
• What is internal control over financial reporting, and what are its components? (LO 2)
• What type of control is segregation of duties, and what risks is that control intended to mitigate? (LO 5)
LEARNING OBJECTIVE 1

ARTICULATE THE IMPORTANCE OF INTERNAL CONTROL OVER FINANCIAL REPORTING FOR ORGANIZATIONS AND THEIR EXTERNAL AUDITORS
IMPORTANCE OF INTERNAL CONTROL OVER FINANCIAL REPORTING

- Internal control helps:
  - Mitigate risks of not achieving organizational objectives
  - Provide confidence regarding reliability of financial information
  - Reduce occurrence of unforeseen circumstances
  - Improve quality of information
• Reliable Insurance Co. introduced an insurance policy to provide supplemental coverage to Medicare benefits for the elderly

• The company’s internal control system failed to record claims on a timely basis
  • It underpriced the policies and misrepresented its financial condition to shareholders and lenders

• It led to:
  • Unreliable financial statements
  • Failure of the business
IMPORTANCE OF INTERNAL CONTROL TO THE EXTERNAL AUDIT

• Auditors are required to identify and assess risks of material misstatement due to fraud or error
  • For this, the auditor needs to understand the company’s internal controls to determine appropriate audit procedures

• **Integrated audit**: Occurs when an auditor provides an opinion on:
  • The effectiveness of the client’s internal control over financial reporting and
  • The financial statements
DEFINE INTERNAL CONTROL AS PRESENTED IN COSO'S UPDATED **INTERNAL CONTROL, INTEGRATED FRAMEWORK** AND IDENTIFY THE COMPONENTS OF INTERNAL CONTROL
INTERNAL CONTROL, INTEGRATED FRAMEWORK

• Most widely used internal control framework
• Published by COSO (Committee of Sponsoring Organizations)

COSO’s updated *Internal Control, Integrated Framework*

• Comprehensive framework of internal control
• Used to assess effectiveness of:
  • Internal control over financial reporting
  • Controls over operational and compliance objectives
COSO defines **internal control** as a process:

- Effected by an entity’s board of directors, management, and other personnel
- Designed to provide reasonable assurance regarding achievement of objectives relating to operations, reporting, and compliance
EXHIBIT 3.1 - COSO FRAMEWORK FOR INTERNAL CONTROL
COMPONENTS OF INTERNAL CONTROL

• **Risk assessment**: Process for identifying and assessing risks that may affect organizations from achieving objectives

• **Control environment**
  • Set of standards, processes, and structures that provides the basis for carrying out internal control across the organization
  • Includes the tone at the top regarding importance of:
    • Internal control
    • Expected standards of conduct
COMPONENTS OF INTERNAL CONTROL

• **Control activities**: Actions established by policies and procedures
  - Help ensure that management’s directives regarding internal control are carried out

• **Information and communication**
  - Information can come from internal and external sources
  - Communication is the process of providing, sharing, and obtaining necessary information
COMPONENTS OF INTERNAL CONTROL

- **Monitoring**: Helps determine whether the controls are present and continuing to function effectively
- Effective internal controls need to:
  - Be effectively designed and implemented
  - Operate effectively
ENTITY-WIDE CONTROLS

- Operate across an entity and affect multiple processes, transactions, accounts, and assertions
  - Controls related to control environment
  - Controls over management override
  - Organizations’ risk assessment process
  - Centralized processing and controls
  - Controls to monitor results of operations
  - Controls over period-end financial reporting process
  - Policies that address business control and risk management practices
TRANSACTION CONTROLS

• Control activities implemented to mitigate transaction processing risk
• Affect certain processes, transactions, accounts, and assertions
  • Do not have an entity-wide effect
LEARNING OBJECTIVE 3

DESCRIBE THE CONTROL ENVIRONMENT COMPONENT OF INTERNAL CONTROL, LIST ITS PRINCIPLES, AND PROVIDE EXAMPLES OF EACH PRINCIPLE
## EXHIBIT 3.2 - INTERNAL CONTROL COMPONENTS AND PRINCIPLES

<table>
<thead>
<tr>
<th>Components</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. The organization demonstrates a commitment to integrity and ethical values.</td>
</tr>
<tr>
<td></td>
<td>2. The board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control.</td>
</tr>
<tr>
<td></td>
<td>3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</td>
</tr>
<tr>
<td></td>
<td>4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</td>
</tr>
<tr>
<td></td>
<td>5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</td>
</tr>
<tr>
<td></td>
<td>7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</td>
</tr>
<tr>
<td></td>
<td>8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.</td>
</tr>
<tr>
<td></td>
<td>9. The organization identifies and assesses changes that could significantly impact the system of internal control.</td>
</tr>
</tbody>
</table>
## EXHIBIT 3.2 - INTERNAL CONTROL COMPONENTS AND PRINCIPLES

<table>
<thead>
<tr>
<th>Components</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Activities</td>
<td>10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</td>
</tr>
<tr>
<td></td>
<td>11. The organization selects and develops general control activities over technology to support the achievement of objectives.</td>
</tr>
<tr>
<td></td>
<td>12. The organization deploying control activities through policies that establish what is expected and in procedures that put policies into action.</td>
</tr>
<tr>
<td>Information and</td>
<td>13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.</td>
</tr>
<tr>
<td>Communication</td>
<td>14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.</td>
</tr>
<tr>
<td></td>
<td>15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</td>
</tr>
<tr>
<td></td>
<td>17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.</td>
</tr>
</tbody>
</table>
COSO COMPONENT: CONTROL ENVIRONMENT

- Foundation for all other components of internal control
- A strong control environment protects against risks related to reliability of financial statements
- Examples of control environment deficiencies
  - Low level of control consciousness within an organization
  - Audit committee not having independent members
  - Absence of an ethics policy within an organization
In the case of HealthSouth, it did not matter that the organization had a code of ethics for its employees.

The company and its board were dominated by the management.

The unwritten message was stronger than any written message: “Do what we want you to do or lose your job.”

This illustrates that a weak control environment enables fraud to occur.
COMMITMENT TO INTEGRITY AND ETHICAL VALUES - COSO PRINCIPLE 1

• Demonstrated through the tone set by the board and management

• Organizations should have:
  • Standards of conduct regarding expectations for integrity and ethical values
  • Processes in place to determine if individuals are performing in accordance with expected standards of conduct
  • Processes for identifying and addressing any deviations in expected conduct
The weak control environment at NutraCea led to other material weaknesses in internal control.

Management failed to properly analyze, account for, and record significant sales contracts for proper revenue recognition.

Management failed to retain the resources to:
- Analyze significant transactions
- Prepare financial statements
- Respond to regulatory comments in a timely manner
BOARD OF DIRECTORS EXERCISES OVERSIGHT RESPONSIBILITY - COSO PRINCIPLE 2

• Board of directors includes various committees
  • Audit committee oversees management
  • Compensation committee
    • Reviews and approves compensation of top officers
    • Oversees organization’s benefit plans
    • Makes recommendations regarding board compensation

• Board of directors is required to exercise objective oversight for the development and performance of internal control
BOARD OF DIRECTORS EXERCISES OVERSIGHT RESPONSIBILITY - COSO PRINCIPLE 2

• The board should have:
  • Sufficient knowledge and skills to fulfill its oversight responsibilities
  • Sufficient number of independent members to ensure the board’s objectivity
### MANAGMENTS ESTABLISH STRUCTURE, AUTHORITY, AND RESPONSIBILITY - COSO PRINCIPLE 3

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Board</strong></td>
<td>- Retains authority over decisions</td>
</tr>
<tr>
<td></td>
<td>- Reviews management’s assignments</td>
</tr>
<tr>
<td><strong>Senior Management</strong></td>
<td>- Establishes directives, guidance, and controls</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>- Guides and facilitates senior’s directives</td>
</tr>
<tr>
<td><strong>Personnel</strong></td>
<td>- Understand internal control requirements</td>
</tr>
<tr>
<td><strong>Outsourced Service Providers</strong></td>
<td>- Follow management’s scope of authority and responsibility for all nonemployees engaged</td>
</tr>
</tbody>
</table>
Commitment towards competence is demonstrated through policies and procedures to:

- Attract
- Train
- Mentor
- Evaluate
- Retain employees
ORGANIZATION ENFORCES ACCOUNTABILITY - COSO PRINCIPLE 5

• Individuals held accountable for internal control responsibilities
• Accountability mechanisms
  • Establishing and evaluating performance measures
  • Providing appropriate incentives and rewards
LEARNING OBJECTIVE 4

DESCRIBE THE RISK ASSESSMENT COMPONENT OF INTERNAL CONTROL, LIST ITS PRINCIPLES, AND PROVIDE EXAMPLES OF EACH PRINCIPLE
COSO COMPONENT - RISK ASSESSMENT

Internal sources of risk
- Changes in management responsibilities
- Changes in internal information technology
- Poorly conceived business model

External sources of risks
- Economic recessions decrease product or service demand
- Increase in competition
- Changes in regulation that make the business model unsustainable
- Changes in the reliability of source goods that reduce profitability
SPECIFIES RELEVANT OBJECTIVES - COSO PRINCIPLE 6

• When specifying the objectives of reliable financial reporting, management should take steps for financial reporting to reflect underlying transactions and events
  • Financial reporting objectives should be consistent with accounting principles
  • Management should consider level of materiality when specifying objectives
IDENTIFIES AND ANALYZES RISK - COSO PRINCIPLE 7

- Appropriate levels of management need to be involved in the identification and analysis of risk
- Risk identification should include both internal and external factors
  - External - Economic changes that may impact barriers to competitive entry
  - Internal - Change in management responsibilities that could affect the way certain controls operate
ASSESSES FRAUD RISK - COSO
PRINCIPLE 8

• Risks related to misappropriation of assets and fraudulent financial reporting

• Assessment of fraud risk considers:
  • Ways in which the fraud could occur
  • Fraud risk factors that impact financial reporting
  • Incentives and pressures that might lead to fraud
  • Opportunities for fraud
  • Personnel who might engage in or rationalize fraud activities
AUDITING IN PRACTICE - INEFFECTIVE INTERNAL CONTROL OVER FINANCIAL REPORTING LEADS TO EMBEZZLEMENT AT CITIGROUP

• A mid-level accountant in Citigroup’s office embezzled about $19 million from the company
  • He transferred money from various Citigroup accounts to his personal bank account by making adjusting journal entries from interest expense accounts and debt adjustment accounts to Citigroup’s main cash accounts
  • To conceal the transactions, he used a false contract number in the reference line of the wire transfer
IDENTIFIES AND ANALyzES SIGNIFICANT CHANGE - COSO PRINCIPLE 9

• As internal and external conditions change, an organization’s internal controls need to change
  • Example - The introduction of new information system technologies

• An organization needs a process for identifying and assessing changes in internal and external factors that can affect its ability to produce reliable financial reports
LEARNING OBJECTIVE 5

DESCRIBE THE CONTROL ACTIVITIES COMPONENT OF INTERNAL CONTROL, LIST ITS PRINCIPLES, AND PROVIDE EXAMPLES OF EACH PRINCIPLE
COSO COMPONENT: CONTROL ACTIVITIES

- Ensure that management’s directives regarding controls are accomplished
- Performed within processes
- Performed at all levels of an organization
SELECTS AND DEVELOPS CONTROL ACTIVITIES - COSO PRINCIPLE 10

- No universal set of control activities applicable to all organizations
  - Organizations select and develop control activities that are specific to the risks they identify during risk assessment
EXHIBIT 3.3 - TRANSACTION PROCESSING UNDER CONTROL ACTIVITIES

- Application controls (also referred to as transaction controls): Activities implemented to mitigate transaction processing risk that affect only certain processes, transactions, accounts, and assertions.
TRANSACTION PROCESSING UNDER CONTROL ACTIVITIES

- Control objectives desired by an organization
  - Recorded transactions exist and have occurred
  - All transactions are recorded
  - Transactions are properly valued
  - Transactions are properly presented and disclosed
  - Transactions relate to rights or obligations of the organization
Accounting estimates should be based on underlying processes and data that have been successful in providing accurate estimates in the past.

Controls should be built around the processes to provide reasonable assurance that:

- The data are accurate
- The estimates are faithful to the data
- The underlying estimation model reflects current economic conditions and has proven to provide reasonable estimates in the past.
TRANSACTION PROCESSING UNDER CONTROL ACTIVITIES

- Controls over adjusting, closing, and other unusual entries
  - Documented support for all entries
  - Reference to underlying supporting data with a well-developed transaction trail
    - **Transaction trail**: Records that allow auditors to trace transactions from origination through final disposition, or vice versa
  - Review by CFO or controller
AUTOMATED AND MANUAL TRANSACTION CONTROLS

• Application controls mitigate risks, whether automated or manual

• **Input controls**
  • Designed to ensure that:
    • Authorized transactions are correct and complete
    • Only authorized transactions can be input
AUTOMATED AND MANUAL TRANSACTION CONTROLS

• Types of inputs controls
  • Input validation tests (also referred to as edit tests): Built into an application to examine input data for obvious errors
  • Self-checking digits: Developed to test for transposition errors associated with identification numbers
    • Operate by computing an extra digit, or several digits, that are added into a numeric identifier
AUTOMATED AND MANUAL TRANSACTION CONTROLS

• **Processing controls**
  • Designed to ensure that:
    • Correct program used for processing
    • All transactions are processed
    • Transactions update appropriate files

• **Output controls**
  • Designed to ensure that:
    • All data are completely processed
    • Output is distributed only to authorized recipients
• **Segregation of duties**: Protect against risk that individuals may collude to conceal a fraud
  • Requires that a minimum of two employees be involved such that one does not have:
    • Authority and ability to process transactions
    • Custodial responsibilities
• **Physical controls over assets**: Protect and safeguard assets from accidental or intentional destruction and theft
OTHER IMPORTANT CONTROL ACTIVITIES

- **Preventive controls**: Designed to prevent occurrence of a misstatement
  - Most cost efficient
- **Detective controls**: Designed to discover errors that occur during processing
SELECTS AND DEVELOPS GENERAL CONTROLS OVER TECHNOLOGY - COSO PRINCIPLE 11

• General computer controls (also referred to as technology general controls or information technology controls): Pervasive control activities that affect multiple types of information technology systems
  • Include manual or automated control activities over:
    • Technology infrastructure
    • Security management
    • Technology acquisition, development, and maintenance
TECHNOLOGY INFRASTRUCTURE

- Provides the support for information technology to function effectively
- Control activities are necessary to check the technology for any problems and take corrective action
- Other control activities related to infrastructure
  - Backup procedures
  - Disaster recovery plans
SECURITY MANAGEMENT

• Control activities that limit access to technologies
• Security control activities protect from inappropriate and unauthorized access
  • Considerations in security management related to user access:
    • Data item access limited to those who are directly involved
    • Ability to change, modify, or delete a data item restricted to those with authorization
SECURITY MANAGEMENT

• Ability to identify and verify any potential users as authorized or unauthorized for the data item and function requested
• A security department should actively monitor attempts to compromise the system and prepare periodic reports to those responsible for the integrity and access of data
METHODS USED BY ORGANIZATIONS TO DEVELOP TECHNOLOGIES

• In-house - An organization should have:
  • Polices on documentation and approval requirements
  • Authorization of change requests
  • Appropriate protocols and testing of changes made
• Packaged software - An organization should have policies regarding selecting and implementing these packages
• Outsource arrangements
DEPLOYS THROUGH POLICIES AND PROCEDURES - COSO PRINCIPLE 12

• Policies should:
  • Outline what is expected
  • Establish clear responsibility and accountability

• Procedures should:
  • Put policies into action
  • Be performed diligently, consistently, and by appropriate and competent personnel in a timely manner
DESCRIBE THE INFORMATION AND COMMUNICATION COMPONENT OF INTERNAL CONTROL, LIST ITS PRINCIPLES, AND PROVIDE EXAMPLES OF EACH PRINCIPLE
COSO COMPONENT - INFORMATION AND COMMUNICATION

- Information - Required by an organization from internal and external sources to carry out its internal control responsibilities
- Communication
  - Process of providing, sharing, and obtaining information internally
  - Requires two-way communication with external parties
USES RELEVANT INFORMATION - COSO
PRINCIPLE 13

• Identify and obtain internal and external information to:
  • Support internal control
  • Achieve objective of reliable financial reporting
Internal communication of information occurs throughout organizations through:

- Periodic newsletters
- Posters in the break rooms
- Formal communications from senior management

Whistleblower function - Special line of communication needed for anonymous or confidential communications
COMMUNICATES EXTERNALLY - COSO PRINCIPLE 15

• Two-way communication with external parties
  • Shareholders
  • Business partners
  • Customers
  • Regulators

• External communication should include messages regarding:
  • Importance of internal control
  • Organization’s values and culture
LEARNING OBJECTIVE 7

DESCRIBE THE MONITORING COMPONENT OF INTERNAL CONTROL, LIST ITS PRINCIPLES, AND PROVIDE EXAMPLES OF EACH PRINCIPLE
COSO COMPONENT - MONITORING

• Process that provides feedback on effectiveness of each of the five components of internal control
• For its accomplishment, managers select either of the following or a combination of both
  • Mix of ongoing evaluations
  • Separate evaluations
• Requires that identified deficiencies in internal control be communicated to the personnel concerned with follow-up action taken
CONDUCTS ONGOING AND/OR SEPARATE EVALUATIONS - COSO PRINCIPLE 16

- **Ongoing evaluations**: Procedures built into the normal recurring activities of an entity
  - Computerized monitoring undertaken by organizations to review large volume of transactions
- **Separate evaluations**: Conducted periodically by:
  - Objective management personnel
  - Internal auditors
  - External consultants
EVALUATES AND COMMUNICATES DEFICIENCIES - COSO PRINCIPLE 17

• Control deficiencies identified need to be communicated to appropriate personnel to take appropriate corrective actions on a timely basis.
LEARNING OBJECTIVE 8

IDENTIFY MANAGEMENT’S RESPONSIBILITIES RELATED TO INTERNAL CONTROL OVER FINANCIAL REPORTING, INCLUDING THE FACTORS MANAGEMENT CONSIDERS WHEN ASSESSING CONTROL DEFICIENCIES
DOCUMENTATION OF INTERNAL CONTROL

• Provide clarity and communication of standards and expectations
• Can be either paper or electronic

Advantages
• Help train new personnel
• Serve as a reference tool for all employees
• Provide evidence that the controls are operating
• Enable proper monitoring activities
• Support reporting on internal control effectiveness
DOCUMENTATION OF INTERNAL CONTROL

- Used by external auditors to understand client’s internal control system
  - Documents supporting management’s assessment as an audit evidence required
- Documents required for supporting financial transactions
  - Authorization of transactions
  - Existence of transactions
  - Support for journal entries
  - Financial commitments made
GUIDELINES FOR DEVELOPING RELIABLE DOCUMENTATION

- Prenumbered paper or computer-generated documents facilitate control of, and accountability for, transactions
- Timely preparation
  - Improves credibility and accountability of documents
  - Decreases rate of errors on all documents
- Authorization of a transaction
- Transaction trail
  - Tracing a transaction from its origination through to its final disposition, or vice versa
IMPORTANT ASPECTS OF ELECTRONIC TRANSACTION TRAIL

• Unique identification of transaction
• Date and time of transaction
• Individual responsible for the transaction
• Location from which the transaction originated
• Details of the transaction
• Cross-reference to other transactions
• Authorization or approval of the transaction
REPORTING ON INTERNAL CONTROL OVER FINANCIAL REPORTING

• Sarbanes-Oxley Act of 2002 requires public company management to annually report on the design and operating effectiveness of controls

• Guidelines provided by U.S. Securities and Exchange Commission (SEC) require:
  • Suitable criteria be used as the benchmark in assessing internal control effectiveness
  • The five internal control components be viewed as part of an integrated system in making the assessment
EXHIBIT 3.6 - STEPS IN MANAGEMENT’S EVALUATION OF INTERNAL CONTROL OVER FINANCIAL REPORTING

1. Identify Financial Reporting Risks and Controls Implemented to Mitigate those Risks
   - Identify financial reporting risks
   - Identify controls that mitigate financial reporting risks
   - Assess design effectiveness (possibly via walkthroughs)

2. Evaluate the Operating Effectiveness of Internal Control over Financial Reporting
   - Select and perform testing procedures to evaluate the operating effectiveness
   - Document operating effectiveness

3. Provide Report on Effectiveness of Internal Control over Financial Reporting
   - Evaluate control deficiencies
   - Provide public disclosure of management report, including any material weaknesses
EVALUATING INTERNAL CONTROL
OVER FINANCIAL REPORTING

• Management identifies significant risks to reliable financial reporting
  • **Significant account**: Possibility of material misstatement without considering effect of internal controls
  • **Relevant assertion**: Judgment in valuing an account without considering effect of internal controls
EVALUATING INTERNAL CONTROL OVER FINANCIAL REPORTING

• Management conducts a walkthrough to focus on design and operating effectiveness of controls
  • **Walkthrough**: Process whereby management follows a transaction from origination through organization’s processes until it is reflected in organization’s financial records
    • Includes a combination of:
      • Inquiry
      • Observation
      • Inspection of documentation making up transaction trail
      • Reperformance of controls
EXHIBIT 3.7 - EXAMPLES OF APPROACHES TO MANAGEMENT TESTING OF OPERATING EFFECTIVENESS OF CONTROL

<table>
<thead>
<tr>
<th>Control to Be Tested</th>
<th>Possible Management Testing Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>As part of the organization’s risk assessment process, formal forecasts are prepared and updated during the year to reflect changes in conditions, estimates, or current knowledge. The organization has a documented and approved disaster recovery plan, which includes off-site storage controlled by a third-party vendor. The organization has a policy requiring that a revenue recognition review be performed by the revenue accountant before revenue from complex contracts is recorded. Surveys of internal users of financial reports are conducted to obtain information on user satisfaction with the reliability and timeliness of the reporting.</td>
<td>Obtain and review the most recent corporate budget, including current forecasts. Inquire of those that are responsible for preparing and updating the forecasts. Review disaster recovery plan and third-party vendor contract. Confirm off-site storage arrangement with third-party vendor. Obtain evidence of approval of the disaster recovery plan. Review the policy. For selected transactions, review documentation that substantiates the review or reperform the review. Obtain and review user surveys. Interview users.</td>
</tr>
</tbody>
</table>
ASSESSING INTERNAL CONTROL DEFICIENCIES

• Control deficiency: Shortcoming in internal controls such that objective of reliable financial reporting may not be achieved
  • Design deficiency - Control necessary to meet control objective missing
  • Operation deficiency - Properly designed control does not operate as designed
ASSESSING INTERNAL CONTROL DEFICIENCIES

• Categories of control deficiencies:
  
• **Material weakness**
  
  • A deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a *reasonable possibility* that a *material* misstatement of the company’s annual or interim financial statements will not be prevented or detected on a timely basis.
Categories of control deficiencies:

- **Significant deficiency**
  - A deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company’s financial reporting
  - Not needed to be reported to external users
  - Not included in management’s report on internal control effectiveness
EXHIBIT 3.8 - EXAMPLES OF MATERIAL WEAKNESSES IN INTERNAL CONTROL

• Weaknesses in the design of controls

• Absence of appropriate segregation of duties over important processes
• Absence of appropriate reviews and approvals of transactions, accounting entries, or systems output
• Inadequate controls to safeguard assets
• Absence of controls to ensure that all items in a population are recorded
• Inadequate processes to develop significant estimates affecting the financial statements, for example, estimates for pensions, warranties, and other reserves
• Undue complexity in the design of the processing system that obfuscates an understanding of the system by key personnel
• Inadequate controls over access to computer systems, data, and files
• Inadequate controls over computer processing
• Inadequate controls built into computer processing
EXHIBIT 3.8 - EXAMPLES OF MATERIAL WEAKNESSES IN INTERNAL CONTROL

- Weaknesses in the operation of controls

- Independent tests of controls at a division level indicate that the control activities are not working properly; for example, purchases have been made outside of the approved purchasing function
- Controls fail to prevent or detect significant misstatements of accounting information
- Misapplication of accounting principles
- Credit authorization processes overridden by the sales manager to achieve sales performance goals
- Reconciliations (a) not performed on a timely basis or (b) performed by someone independent of the underlying process
- Testing reveals evidence that accounting records have been manipulated or altered
- Evidence of misrepresentation by accounting personnel
- Computerized controls leading to items identified for nonprocessing systematically overridden by employees to process the transactions
- The completeness of a population, for example, prenumbered documents or reconciling items logged on to the computer with those processed, not accounted for on a regular basis
DIFFERENCES BETWEEN MATERIAL WEAKNESSES AND SIGNIFICANT DEFICIENCIES

- Professional judgment used by management in assessing the identified control deficiencies
- Severity of a deficiency depends on:
  - Magnitude of the potential misstatement resulting from the deficiency
  - Whether there is a reasonable possibility that the organization’s controls will fail to prevent, or detect and correct a misstatement
- Consideration of specific facts and circumstances surrounding the identified deficiency