Sarbanes Oxley Audit Committee Requirements
Audit Committee Member Independence

• Member may not:
  – Accept any consulting, advisory or other compensatory fees
  – Be affiliated with the issuer or any subsidiary thereof
    • Includes family members
    • Defines “Affiliates” for the purpose of determining independence
Determination and Disclosure of Audit Committee Financial Expert

• Disclosure of whether the audit committee includes at least one audit committee “financial expert”

• Financial expert defined as:
  – An individual who possesses all of the following:
    • An understanding of financial statements and GAAP
    • The ability to assess application of GAAP as it relates to accounting for estimates, accruals and reserves
    • Experience preparing, auditing, analyzing or evaluating financial statements that are generally comparable to the registrant’s or experience actively supervising those engaged in such activities
    • An understanding of internal controls and procedures for financial reporting
    • An understanding of audit committee functions
Audit Committee Financial Expert (continued)

• Financial experts attributes may be acquired by:
  – Education and experience as a
    • Principal; financial officer, principal accounting officer, controller, public accountant or auditor or
    • Experience in one or more positions that involve the performance of similar functions
  – Experience actively supervising a principal officer, principal accounting officer, controller, public accounts, auditor, or person performing similar functions
  – Experience overseeing or assessing the performance of companies or public accountants with respect to the preparation, auditing, or evaluation of financial statements
  – Other relevant experience
Auditor Communications with Audit Committees

- Required additional communications between auditors and audit committees:
  - Critical accounting policies
    - Relate to those policies that are most important to the portrayal of the company's financial condition and results and that require management’s most difficult, subjective, or complex judgments
    - To include an assessment of management’s disclosures and any proposed modifications by the accountants that were not included by management
  - Alternative accounting treatment related to material items that have been discussed with management
  - Other material written communications between the auditor and management
Interaction with Independent Auditor

• Interaction with Independent Auditor
  – Required Communications
  – External auditor responsibilities under GAAS
  – Company’s significant accounting policies
  – Management judgments and accounting estimates
  – Audit adjustments
  – External auditor judgments about the quality of company’s accounting principles
  – Disagreements with management
  – Consultations with the accountants
  – Major issues discussed with management prior to retention
  – Difficulties encountered in performing the audit
Whistle-blower Procedures

• Audit committees are required to establish procedures for:
  – Handling of complaints received by the company regarding accounting, internal controls or auditing matters
  – The confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters

• Management needs to inform employees and others of the confidential disclosure options
  – Employee handbooks
  – Orientation
  – Postings
  – Intranet sites

• Management needs to establish mechanisms to validate the representation of receipts from third-party vendor, email box, etc.
  – Designees should be given responsibility for investigating complaints and reporting back to the audit committee
A code of ethics is a written standard that is reasonably designed to detect wrongdoing and promotes:

- Honest and ethical conduct
- Full, fair, accurate, timely and understandable disclosure in reports
- Compliance with applicable governmental laws, rules and regulations
- Prompt internal reporting of code violations
- Accountability for adherence

Reporting requirements include:

- Disclosure of whether code of ethics exists for the principal executive officer, principal financial officer, principal accounting officer or controller, or their equivalents; if one does not exist, disclosure of why not
- Code of ethics to be made publicly available
- Changes or waivers of the code of ethics to be disclosed within five business days via Form 8-K or the company’s Website
Control Certifications and Attestation

• The certifying officers:
  – Are responsible for establishing and maintaining disclosure control and procedures
  – Have designed such disclosures controls and procedures to ensure that material information is made known to them
  – Have evaluated the effectiveness of the issuer’s disclosure controls and procedures within 90 days prior to the filing date of the report
  – Have presented in their report conclusions about the effectiveness of their disclosure controls and procedures
Control Certifications and Attestation (continued)

• The certifying officers have disclosed to the issuer's audit
  – All significant deficiencies in the design or operation of internal control over financial reporting
  – Any fraud, whether or not material, that involves management or other employees who have a significant role in internal control

• The certifying officers have indicated in the report whether there were significant changes in internal control subsequent to the date of their evaluation, including any corrective actions taken
Control Certifications and Attestation (continued)

• Definitions of internal controls
  – Disclosure controls and procedures
    • Controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files under the act is recorded, processed, summarized, and reported within the time periods specified in the commission’s rules and forms
  – Internal controls over financial reporting
    • Internal control over financial reporting includes those policies and procedures that pertain to an entity’s ability to initiate, record, process, and report financial data consistent with the assertions embodied in either annual or interim financial statements
Control Certifications and Attestation (continued)

• The chief executive officer and the chief financial officer must certify in each periodic report containing financial statements:
  – The periodic report containing the financial statements fully complies with the requirements of section 13 (a) or 15 (d) of the Securities Exchange Act of 1934 and that the information contained in the periodic report presents fairly, in all material respects, the financial condition and results of operations of the issuer
Control Certifications and Attestation – Audit Committee Considerations

• Understand process used by management to prepare certifications

• Encourage establishment of a disclosure committee responsible for:
  – Determining appropriateness of disclosures in drafts of all publicly disseminated information
  – Overseeing the process by which disclosures are created and reviewed
  – Identifying what constitutes a significant deficiency and material weakness in the designer operation of internal control
  – Ensuring that the CEO and CFO are aware of material information that could affect disclosures
  – Reviewing significant control deficiencies to determine appropriateness of disclosure
Committee of Sponsoring Organizations (COSO)

An Integrated Framework
What is Internal Control?

- Internal control means different things to different people

- Authoritative guidance defines Internal Control* as a process designed to provide reasonable assurance regarding the achievement of business objectives.

- Internal control has three main objectives:
  - To promote effectiveness and efficiency of operations
  - To ensure reliability of financial reporting
  - To maintain compliance with applicable laws and regulations
• In short, internal control helps an entity get to where it wants to go and avoid the pitfalls and surprises that may occur along the way.
Why is Internal Control Important?

**Operations**
- Promotes efficiency and effectiveness of operations through standardized processes
- Ensures the safeguarding of assets through control activities

**Financial**
- Promotes integrity of data used in making business decisions
- Assists in fraud prevention and detection through the creation of an auditable trail of evidence

**Compliance**
Helps maintain compliance with laws and regulations through periodic monitoring
Internal Control Myths

• Some people have unrealistic expectations about what internal control can do…

Myth #1: Internal control can ensure an entity’s success and provide absolute reliability of financial reporting and regulatory compliance.

– Effective internal control can only help an entity achieve its objectives. It cannot change a poor manager into a good one.
– An internal control system, no matter how well conceived and operated, can provide only reasonable assurance.
Myth #2: Internal control serves as a substitute for management.
- While internal control is integrated into the business management processes of planning, executing and monitoring, it is a tool used by management, not a substitute for it.

Myth #3: Internal control can protect an organization from errors in decision making, collusion of two or more people and management ability to override the system.
- The likelihood of occurrence of such events is affected by limitations inherent in all internal control systems.
Select Events in the Evolution of Internal Control

- **1970**: Mid-1970s Watergate Scandal and Investigation
- **1977**: Foreign Corrupt Practices Act (FCPA)
- **1980**: Early-1980s Increased Focus on Internal Control and Compliance
- **1985**: National Commission on Fraudulent Financial Reporting – Treadway Commission
- **1990s – 2000**: Continued Focus on Internal Control, Risk Management and Responsibilities (Blue Ribbon Commission, Competency Framework for Internal Audit, Others)
- **2000**: 1990s – 2000 Continued Focus on Internal Control, Risk Management and Responsibilities (Blue Ribbon Commission, Competency Framework for Internal Audit, Others)
- **2002**: Sarbanes-Oxley Act of 2002
How it All Began

• The SEC and the Watergate special prosecutor focus on internal controls during the mid-1970s.
  – Corporations were making illegal payments, including political contributions and bribes to government officials.

• The result of the SEC and Watergate investigations was the Foreign Corrupt Practices Act (FCPA) of 1977.
  – The underlying theme of this act was that sound internal control should provide an effective deterrent to illegal payments.

• This provided the foundation for increasing focus on the control environment and the process of internal control in the early-1980s.
  – Industry-specific and for organizations in general

• The National Commission on Fraudulent Financial Reporting, known as the Treadway Commission, was created in 1985.
  – Identify the causal factors of fraudulent financial reporting
  – Make recommendations to reduce its incidence
The Evolution Continues

• The Treadway Commission issued the Report on Fraudulent Financial Reporting.
  – Emphasized the control environment, codes of conduct, and competent and involved audit committees.
  – Called for sponsoring organizations to integrate the various concepts and develop a common reference point. The result was the Committee of Sponsoring Organizations or COSO.
    • COSO incorporated learnings from other existing authoritative sources (e.g., CoCo, Cadbury, Turnbull, etc.)

• COSO developed and published practical, broadly accepted criteria for establishing internal control and evaluations of effectiveness.
    • Outlined the roles and responsibilities of management
    • Established a means to monitor, evaluate and report on internal control
Ongoing Focus on Internal Control

• Federal Sentencing Guidelines
  – Used by the criminal justice system, effectively reduces white-collar crime penalties for entities with appropriate compliance related internal controls.

• Blue Ribbon Commission
  – Focused on strengthening the independence of audit committees, defining its accountability and on improving its effectiveness.
  – Issued report in 1999 outlining 10 recommendations and requirements for audit committees.
  – The rules are enforced by the SEC, NASD, NYSE, AICPA.

• Competency Framework for Internal Auditing (CFIA)
  – Issued by Institute for Internal Auditors, copyright 1999.
  – Defined the valued-added role of the internal audit department of the future.
  – Internal audit will provide assurance about risk exposure and control strategies.

• Sarbanes-Oxley Act
  – Requires executive responsibility for effectiveness of internal control infrastructures
  – Mandates the quarterly certification of, and annual attestation to, the effectiveness of internal controls infrastructures
The COSO Internal Control – Integrated Framework

- COSO offers an integrated framework that defines internal control by five interrelated components:
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information & Communication
  - Monitoring
Control Environment

• The **control environment** is the control consciousness of an organization; it is the environment in which people conduct business activities and fulfill their control obligations.

• The control environment includes both intangible and tangible elements:
  – Integrity and ethical values
  – Commitment to competence
  – Governance and organization structure
  – Management philosophy and operating style
  – Assignment of authority and responsibility
  – Human resource policies and practices

• An effective control environment exists when employees understand their responsibilities, authority, and are committed to acting ethically.

• Management influences an organization’s control environment through setting the standard through actions and effectively communicating written polices and procedures, a code of ethics, and standards of conduct – “tone at the top.”
Risk Assessment

- **Risk assessment** starts with identifying risks associated with business objectives linked through all levels of the organization.

- **Entity wide**
  - The cornerstone for effective control, entitywide objectives provide guidance on what the entity wants to achieve
  - Should be consistent with budget, strategy, and business plans

- **Activity level**
  - Align with entitywide objectives but differ in that they relate directly to goal setting with specific targets and deadlines
  - Provides guidance for management focus

- **Risk assessment requires evaluation of external and internal factors and the impact on operations, financial reporting, and compliance.**

- **May employ techniques for risk identification, assessment, and management.**
  - Control Self Assessment (CSA), Enterprise Risk Management (ERM), Risk and Control Assurance (RCA), questionnaires, and many others
Control Activities

- **Control activities** are policies and procedures that help to ensure that actions identified to manage risks are executed and timely.

- The control activities should be embedded within the operations of the business and used to manage risks to reasonable levels. Focuses on *prevention, detection, correction*.

- Types of control activities:
  - Approvals, authorizations, and verifications (e.g. delegation of authority)
  - Direct functional or activity management (e.g. reconciliations)
  - Review of performance indicators (e.g. KPIs, metrics)
  - Security of assets (e.g. physical controls)
  - Segregation of duties (e.g. custody - authority - recording)
  - Information systems controls (e.g. security access)

- Disciplinary action should be established, communicated, and consistently administered for noncompliance.
Information and Communication

- **Information and communication** requires that relevant external and internal information be identified, captured, processed, and communicated throughout the organization in a timely manner.

- Provided through various formal and informal means.
  - Verbal communication (e.g. meetings, feedback)
  - Written communication (e.g. policies, procedures, job descriptions)
  - Demonstrated through actions (e.g. management sets example)

- The integrity of information quality is imperative for making business decisions.
  - Requires internal control mechanisms to provide reasonable assurance that information is **appropriate, current, timely, accurate, and accessible**.

- Mangement's responsibilities:
  - Employee duties and responsibilities should be communicated
  - Communication across the organization should be fluid – up, down, and laterally across the organization
  - Channels of communication with customers, suppliers, and other external parties should be open
Monitoring

• The purpose of monitoring is to determine whether internal control is adequately designed, executed, effective, and adaptive.

• Internal control performance should be assessed over time through ongoing monitoring of operations and separate periodic evaluations.

• Scope and frequency of monitoring activities depend on significance of risks being controlled and importance of controls in reducing risks.

• Monitoring activities should be built into normal, recurring operating activities of an organization.

• Deficiencies found should have defined escalation path for reporting and follow-up and accountability for corrective action.
Linking Internal Control and Risk Management

**RISK**
Possibility of an adverse event that may negatively affect the ability of an organization to achieve its objectives.

**RISK MANAGEMENT**
Process to increase confidence in the ability of an organization to anticipate, prioritize, and overcome obstacles to the attainment of its goals.

**INTERNAL CONTROL**
A process designed to provide reasonable assurance regarding the achievement of business objectives.

- Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations
Roles and Responsibilities

• Executive Management
  – Sets the standard for the control environment
  – Maintains ultimate accountability for internal control and risk management enterprise wide
  – Supports control and risk management activities throughout the organization

• Operating Management
  – Directly responsible and accountable for business operations effectiveness and internal control related to business objectives
  – Periodically assesses and asserts on risk management and control environment
  – Develops and implements action plans for improvement

• Finance Management
  – Involved in financial implications of operating management responsibilities
  – Provides guidance to design, establishment, execution, and monitoring of adequate internal controls
Roles and Responsibilities (continued)

- **Internal Audit**
  - Provides support for risk and control assessment activities
  - Monitors exposure of the organization and makes recommendations relating to risk and control activities
  - Designs internal audit plan based on strategic risk assessment
  - Tests adequacy and effectiveness of controls
  - Challenges and validates management control environment assertions
  - Reports independent findings and provides recommendations

- **Audit Committee**
  - Focuses board attention
  - Evaluates overall risk exposure
  - Reviews adequacy of overall control environment
  - Provides oversight and advice

- **External Audit**
  - Evaluates the effectiveness of internal control to determine the scope of external audit procedures
  - Issues management commentary reports
  - Issues an opinion on the consolidated financial statements
  - Reviews control environment and uses results of risk assessments as input to develop external audit plan