Internal controls are designed with costs versus benefits in mind. It would be expensive for an organization to attempt to ensure that 100% of errors or fraud would be prevented, or detected and corrected. In addition, employee collusion or management override would be difficult to control. Thus, internal controls are designed to provide reasonable, but not absolute, assurance regarding achievement of an entity's objectives. Auditors assess the inherent risk, control risk, and planned detection risk in order to gain a basis for determining the acceptable audit risk for a particular area and design their testing procedures accordingly. These tests provide reasonable assurance that there are no material weaknesses in the internal control structure.

The passage of the Sarbanes-Oxley Act increased the cost of compliance for the external audit function tremendously. The PCAOB approved PCAOB Auditing Standard No. 5 in order to provide guidance to management and the external auditor in complying with Section 404 requirements. The standard requires auditors to perform their internal control assessment using a top-down, risk assessment (TDRA) approach. TDRA is a hierarchical approach that applies specific risk factors to determine the scope of work and evidence required in the assessment of internal controls.

The FCPA mandates that public companies make and keep books, records, and accounts that, in reasonable detail, accurately and fairly reflect the transactions and disposition of the company's assets. In addition, the company must devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:

- Transactions are executed in accordance with management's general or specific authorization.
- Transactions are recorded as necessary to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and to maintain accountability for assets.
- Access to assets is permitted only in accordance with management's general or specific authorization.
- The recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.

COSO's Internal Control - Integrated Framework.

A. Control environment: Refers to the standards, processes, and structures that provide the basis for internal control across the organization. It reflects the tone at the top of the organization regarding the importance of internal control including expected standards of conduct. The updated 2013 COSO Framework sets forth five principles that are fundamental to establishing an effective control environment. Those principles include:

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight responsibility.
3. Management establishes structures, reporting lines, and appropriate authorities and responsibilities throughout the organization in pursuing organizational objectives.
4. The organization demonstrates a commitment to attracting, developing, and retaining competent individuals in alignment with organizational objectives.
5. The organization enforces accountability for internal control responsibilities.

B. Risk assessment: The risk assessment component of the COSO Framework (as updated in 2013) involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. A precondition to risk

assessment is the establishment of objectives, linked at different levels of an entity. Four fundamental principles are associated with the risk assessment component of the 2013 updated COSO Framework. They include:

1. The organization must specify objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
2. The organization must identify risks to the achievement of its objectives across the entity and analyze risks as a basis for determining how risks should be managed.
3. The organization must consider the potential for fraud in assessing risks to the achievement of objectives.
4. The organization must identify and assess changes that could significantly impact the internal control system.

C. **Control activities:** Control activities include the policies and procedures that help ensure that management's directives to mitigate risks are carried out effectively. These activities are performed at all levels of an organization at various stages with business processes and across the technology environment. There are three fundamental principles associated with the Control Activities component of the 2013 updated COSO Framework. They are as follows:

1. The organization needs to select and develop control activities that contribute to the mitigation of risks to acceptable levels.
2. The organization needs to select and develop general control activities over technology.
3. The organization needs to deploy control activities through policies that set forth what is expected and procedures that put policies into action.

D. **Information and communication:** The information and communication component of the COSO Framework (as updated in 2013) focuses on providing, sharing, and obtaining necessary information through continual communication. Communication should be both internal and external. Internal communication is disseminated throughout the organization and enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations. Three fundamental principles are outlined in the 2013 updated COSO Framework as it relates to information and communication:

1. The organization obtains and uses relevant, quality information to support the functioning of internal control.
2. The organization internally communicates information regarding internal control.
3. The organization communicates with external parties regarding matters affecting the functioning of internal control.

E. **Monitoring activities:** Monitoring activities address the ongoing evaluations and/or separate evaluations to assess whether an organization's internal controls are present and functioning. In this regard, the 2013 updated COSO Framework sets forth two key principles:

1. The organization conducts ongoing and/or separate evaluations to assess whether internal controls are present and functioning.
2. The organization evaluates and communicates internal control deficiencies in a timely manner to parties responsible for taking corrective action.