DEFINITION
Internal controls are defined as follows:

Internal control is a process, affected 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:

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

The key concepts behind this definition are:

- Internal control is a *process*. It is a means to an end, not an end in itself.
- Internal control is affected by *people*. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

This definition is provided by the Committee of Sponsoring Organizations (of the Treadway Commission) and can be found at www.coso.org.

WHO IS RESPONSIBLE FOR INTERNAL CONTROLS?
Everyone has some level of responsibility for internal controls. This includes management, faculty, staff and students.

Management is responsible for creating and maintaining a culture of compliance. This includes establishing policies and procedures that ensure that adequate controls are in place and that these guidelines are followed.

Operating personnel affect internal controls by carrying out their duties in accordance with established policies and procedures. They also are responsible for reporting breakdowns in internal controls to their supervisor, internal audit, financial controls or other appropriate personnel.

Every employee in the organization is responsible for ensuring that established internal controls are followed and applied.

FIVE COMPONENTS OF INTERNAL CONTROLS
Control Environment is the "tone at the top" of the organization that includes the management philosophy and operating style, culture of compliance, and institutional values and ethics.

Risk Assessment is the identification of goals and objectives for the institution including financial, regulatory, process and strategic areas and the subsequent identification of any

barriers for achieving any of these goals. Risks are then examined for seriousness based on likelihood of occurrence and impact to the organization.

Control Activities are the policies and procedures that are put in place to mitigate risks to acceptable levels.

Information and Communication is the concept that information is available to management and employees in a timely and usable form in order for them to effectively execute their responsibilities and affect good control over the organizations activities. This information must travel up, down and across the organization.

Monitoring is the assessment of internal control performance over time to determine whether control is adequately designed, properly executed, and effective.

TYPES OF CONTROL ACTIVITIES

Control activities can be preventative or detective.

Preventative control activities are designed to avoid errors and irregularities *before* they happen. They often require extensive thought when building them into a business process but require less ongoing work once they are implemented and functioning. They prevent "bad" things from happening and avoid the needs for error detection, correction and rework. They are less costly than detective controls.

Examples of preventative controls include:
- *Approvals and authorizations* – Review of a transaction and its supporting documentation by appropriate personnel prior to recording it in the system of record.
- *Segregation of duties* - Duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. For instance, responsibilities for authorizing transactions, recording them and handling the related asset are divided.
- *Safeguarding of assets* - Equipment, inventories, securities, cash and other assets are secured physically, and periodically counted and compared with amounts shown on control records. Access is restricted to those with authority to handle them.
- *Information Processing Controls* - A variety of controls are performed to check accuracy, completeness and authorization of transactions. Data entered are subject to edit checks or matching to approved control files. Numerical sequences of transactions are accounted for, and file totals are controlled and reconciled with prior balances and control accounts. Development of new systems and changes to existing ones are controlled, as is access to data, files and programs. Access to systems is controlled by passwords.

Detective control activities are designed to find errors or irregularities *after* they happen. These are activities that are usually on the back end of a process to verify that the transaction was handled appropriately.

Examples of detective controls include:
- *Reconciliations* - Comparisons are made between similar records maintained by different persons to verify transaction details.
- *Supervisory reviews* - Managers running functions or activities review performance reports. They may relate different sets of data - operating or financial - to one another, together with analyses of the relationships.

- *Physical inventory counts* – Comparisons are made between the inventories on hand and the accounting records to determine discrepancies.
- *Audits* – Internal and external audits are both examples of detective controls that verify that information presented in reports are supported by sufficient evidence that the transaction did occur.