DELINEATION OF INTERNAL CONTROL AND ENTERPRISE RISK MANAGEMENT

- Enterprise Risk Management (ERM) is an effective way to handle SOX section 404. According to COSO, ERM is more than internal control. Its ultimate goal is the creation of value for stakeholders.
- Risk analysis provides a basis for the design and implementation of an effective system of internal control for an entire business entity.
- Risk analysis must be conducted in all business processes: management, operation, information, and compliance.
- The most critical business process is the management process that focuses on strategies and objectives. It may entail strategic and decision risks. Internal control must be established to counteract this area of business risk; otherwise, financial reports will likely be manipulated. (This area of internal control has not been addressed by either COSO or the PCAOB.)
- Risks in the operation process and the compliance process, if not detected and prevented, may also contribute to information risks. Separate internal controls are needed to control operation and compliance activities. (This area of internal control has not been emphasized by the accounting profession.)
- Risks in the information process lie primarily with those estimates for some financial variables that are subject to manipulation.
- Internal control is no panacea for detecting major business problems. An effective system of internal control can provide only reasonable assurance that an entity's strategic and other ensuing objectives will be achieved.