

Module 2 – Overview of Internal Control over Financial Reporting

Handout 1 – COSO Enterprise Risk Management Cube

In May 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued the *Internal Control – Integrated Framework*. The framework was designed to define internal control and to provide a standard against which organizations could assess control systems and implement improvements. In September 2004, COSO issued the *Enterprise Risk Management – Integrated Framework*. The new framework addresses internal control within enterprise risk management. Internal control is encompassed within and is an integral part of enterprise risk management. Enterprise risk management is broader than internal control, however, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk.

Internal Control – Integrated Framework remains in place for organizations and others reviewing internal control on a standalone basis and should continue to be used. However, organizations may decide to look to the enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.

The *Enterprise Risk Management – Integrated Framework* (pictured below) consists of four objectives that an entity should strive to achieve. It contains eight components, which represent what is needed to achieve the stated objectives. The relationship between objectives and components is depicted in the form of a three-dimensional cube. The four objective categories – strategic, operations, reporting, and compliance – are represented by vertical columns. The eight components are represented by horizontal rows. An entity’s units are represented by the third dimension. This depiction portrays the ability to focus on the entirety of an entity’s enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.



Module 2 – Overview of Internal Control over Financial Reporting

Handout 1 – COSO Enterprise Risk Management Cube

Objectives

- **Strategic** – high-level goals, aligned with and supporting its mission
- **Operations** – effective and efficient use of its resources
- **Reporting** – reliability of reporting
- **Compliance** – compliance with applicable laws and regulations.

Components

- **Internal Environment**– The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity’s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting**– Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.
- **Event Identification**– Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.
- **Risk Assessment**– Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk Response**– Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
- **Control Activities** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and Communication**– Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- **Monitoring** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.