

Overview of Risk Assessment and Internal Controls

Presented by Mary Beth Saenz

What are Risks?

- **In the most simplified form possible – risks are best described as:**

“What could go wrong”

- **Uncertainty about the future creates risk.**

Risk/Event

- ***Event*** – an incident or occurrence (internal or external source) that affects achievement of objectives. Events can have either a negative impact or a positive impact. (Risk or opportunity)
- ***Risk*** – the possibility that an event will occur and adversely affect the achievement of objectives. (COSO)

Risk Assessment/Risk Management

- ***Risk assessment*** – the process of identifying, sourcing, and evaluating individual risks and the interrelationships between risks.
- **The risk assessment process typically consists of:**
 - Evaluation of available data
 - Application of judgment
 - **Significance**
 - **Likelihood**
 - Formulation of risk responses

Risk Assessment/Risk Management

- ***Risk management*** – includes risk assessment as well as the activities associated with managing risk, including:
 - Policies
 - Processes
 - Competencies
 - Reporting
 - Methodologies
 - Systems

Risk/Performance Assessment

- ***Risk assessment*** is a forward-looking activity applied to future possible events to identify potential impact on the achievement of objectives and the likelihood of occurrence over a defined time.
- ***Performance assessment*** is a retrospective activity applied to evaluate the performance of a unit, a process, or a function against a pre-determined target or standard over a stated period of time.
- **Both apply to objectives**
- **The link between the two is: Risk tolerance**

Risk Tolerance/Risk Appetite

- ***Risk tolerance*** is defined (by COSO) as “the acceptable level of variation relative to the achievement of a specific objective.” (NOTE – this term is often used interchangeably with “risk threshold” or “risk limit”)
- ***Risk appetite*** is the amount of risk an entity is willing to accept in pursuit of value. It reflects the entity’s risk management philosophy.
- Risk appetite is strategic, risk tolerance is tactical.

ERM – Where does it fit?

- **ERM – Enterprise Risk Management**
- **Summarized by COSO:**

Enterprise risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy-setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events affecting the entity and manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board
- Geared to the achievement of objectives in one or more separate but overlapping categories – it is “a means to an end, not an end in itself.”

COSO (1992) Definition of Internal Control

- **It is a PROCESS**
- **effected by PEOPLE**
- **providing REASONABLE ASSURANCE**
- **regarding the ACHIEVEMENT OF OBJECTIVES**

Types of Risks

Based on ERM

- *Environment risk*
- *Process risk*
- *Information for decision-making risk*

Types of Risks – Environment Risk

- ***Environment risk*** – arises when external forces can affect the entity's performance, or make its choices regarding its strategies, operations, organizational structure or financing obsolete or ineffective.

Types of Risks – Process Risk

- ***Process risk*** – arises when internal processes do not achieve the objectives they were designed to achieve in supporting the entity's business model.

Types of Risks – Information Risk

- ***Information for decision-making risk***
– arises when information used to support business decisions is incomplete, out of date, inaccurate, late or simply irrelevant to the decision-making process.

Previous Risk Types

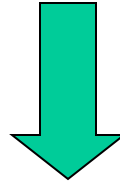
- ***Financial*** – associated with the financial structure of the organization, including the financial systems and transactions
- ***Operational*** – associated with your business' operational and administrative procedures
- ***Strategic*** – associated with operating in a particular industry
- ***Compliance*** – associated with the need to comply with laws and regulations

Focus of Risk Management

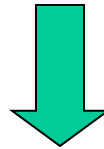
- **Risk management is focused on protecting the assets of an organization.**
- **Originally, this was limited to physical and financial assets.**
- **With ERM, the scope of risk management is enterprise-wide and the application of risk management is targeted to enhancing as well as protecting both tangible and intangible assets.**
- ***Assets* in this case being used to refer to all “sources of value” for the organization.**

Risk Management Process

Goals & Objectives



Activities



Risks



Controls

Five Categories of Assets Representing Sources of Value

- **Physical Assets**
- **Financial Assets**
- **Customer Assets**
- **Employee/Supplier Assets**
- **Organizational Assets**

Risk Assessment

- **Systematic (documented) assessment process**
- **Consideration of potential fraud schemes and scenarios**
- **Assessment of risk at company-wide, significant business unit, and significant account (process) level**
- **Evaluation of the likelihood and significance of each risk to the organization**
- **Testing of effectiveness of risk assessment process by internal audit**
- **Documented oversight by the audit committee, including the consideration of the risk of management override**

Physical Assets – Potential events

- **Unauthorized use**
- **Inefficient use**
- **Catastrophic loss**
- **Unacceptable costs**

Financial Assets – Potential Events

- **Poor economic performance**
- **Lack of economic sources of debt or equity capital**
- **Unacceptable losses**
- **Unexpected losses**
- **Inefficient use**

Employee/Supplier Assets – Potential Events

- **Talent shortages**
- **Work stoppages**
- **Loss of morale**
- **Poor supplier performance**
- **Excessive costs & lead time**
- **Poor quality**

Organizational Assets – Potential Events

- **Lack of leadership**
- **Unclear or obsolete strategies**
- **Lack of institutional learning**
- **Ineffective/inefficient processes**
- **Illegal acts**
- **Poor knowledge sharing**
- **Obsolete systems**
- **Inadequate information for decision-making**
- **Security breach**

Create a Risk Footprint

- **Identify mission, goals, and objectives**
- **Brainstorm Activities**
- **Consolidate into Processes**
- **Prioritize processes**
- **Brainstorm risks for each process**
- **Assign Impact and Probability values**
- **Construct the Risk Footprint**

Prioritize Processes

- **Rank the processes by their risk potential (the process that presents the most risks overall to the one with the least risk overall)**
 - This is a subjective evaluation based upon the combined knowledge of the workshop participants

Valuing Impact and Probability of Risks

- **Impact: Effect on achievement of goals & objectives**
 - High – “showstopper”
 - Medium – inefficient and extra work
 - Low – no effect
- **Probability: Likelihood of the risk happening**
 - High – will happen frequently
 - Medium – will happen infrequently
 - Low – will seldom happen

How to Value Impact

- **Develop a list of consequences to the organization if a risk were to become a reality (Every organization has a finite number of potential consequences)**
- **Value the effect on the organization for each consequence (high, medium, or low)**
- **The Impact value of an identified risk is the value of its highest potential consequence**

Example Impact Valuation

- **Activity: Own an Automobile**
 - Consequence (with Value to Owner)
 - **Loss of Asset** **Medium**
 - **Death/Major Injury** **High**
 - **Minor Injury** **Low**
 - **Criminal penalty** **High**
 - Risk (with associated consequence & value)
 - **Fender Bender (Minor Injury)** **L**
 - **DWI (Criminal penalty or D/I)** **H**
 - **Theft (Loss of asset)** **M**

How to Value Probability

- **Based on controls present**
 - Designed
 - Implemented
 - Level

Choose Risk Response

- **Management, not auditor, decision**
- **Decide Risk Tolerance for every risk**
 - This is usually dictated by assigned Impact value
- **Decide on appropriate strategy for every risk based upon risk tolerance**
 - This is usually dictated by assigned Impact value and the cost of the mitigation strategy

Risk Response Strategies

- **Accept – no mitigation**
- **Avoid – do not do the activity**
- **Transfer – contract out/manage contract**
- **Control – internal mitigation actions**
- **Exploit – do something else**

Risk Footprint Usage

- **Management uses the footprint to allocate resources to managing risks that can affect the achievement of goals and objectives**
- **Internal Audit uses the footprint to provide governance and executive management with appropriate level of assurance on all identified risks**

Level 1 Controls (Execution Controls)

- **Embedded in day-to-day operations**
 - Policies and procedures
 - Segregation of Duties
 - Reconciliations/Comparisons
- **Performed on every event/transaction**
- **Performed by the generators of the event/transaction**
- **Performed in 'real time', as the event/transaction is executed**

Level 2 Controls (Supervisory Controls)

- **Re-application of operating controls**
 - Supervisory Review; Quality Assurance; Self Assessment
- **Performed very soon after the generation of the event/transaction**
- **Performed by line management or staff positions who do not originate the event/transaction**
- **Performed on a sample of the total number of events/transactions**

Level 3 Controls (Oversight Controls)

- **Exception reports, status reports, analytical reviews, variance analysis**
- **Performed by representatives of executive management**
- **Performed on information provided by supervisory management**
- **Performed within a short period (weeks/months) after the event/transaction is originated**

Level 4 Controls (Internal Audit Controls)

- **Audit of the design of controls not the operation of controls**
- **Performed either before the event/transaction is originated or long after**
- **Performed by staff with no involvement in the operations**
- **Performed on individual events/transactions for discovery only**

Create Control Footprints

- **Construct a control footprint matrix for each activity on the risk footprint**
 - Risk Axis (horizontal axis) contains the prioritized risks taken electronically from the risk footprint
 - Control Axis (vertical axis) contains all the control steps that should be present
 - Place an “X” in each cell where a control step operates on a risk
- **Identify the level of each control step listed**

Control Footprint Usage

Indicates

- Most important controls for ensuring compliance with contracts
- Under or over control
- Optimal control mixture

Create Monitoring Plans

- **Include all of the control steps that operate on the critical (RED) risks (and YELLOW risks if desired)**
- **Place Level 1 Controls with associated Level 2 and 3 Controls first**
- **Place Level 1 Controls with associated Level 2 Controls next**
- **Place Level 1 Controls with no Level 2 or 3 Controls last**

Monitoring Plan Usage by Managers: On-going Monitoring

- **Use the Monitoring Plan to check compliance**
- **Check each Level 3 control, then the associated Level 2 Control to validate they were performed**
- **If unable to validate the performance of a Level 3 or a Level 2 control, perform detailed check of transactions for associated Level 1 control**
- **If Level 3 and Level 2 controls are validated, only perform discovery sampling of “stand-alone” Level 1 controls**

Monitoring Plan Use of Audit Program Development

- **Step 1 - Validate all Level 3 controls and their associated Level 2 controls & Level 1 controls first**
- **Step 2 - Validate all Level 2 controls and their associated Level 1 controls next**
- **Step 3 - Validate Level 1 controls that have no Level 2 or Level 3 controls last**

COSO Components

- **Internal Environment**
- **Risk Assessment**
 - Event (Risk) Identification (ERM)
 - Risk Assessment (ERM)
 - Risk Response (ERM)
- **Control Activities**
- **Information and Communication**
- **Monitoring**

Control Activities

- **Controls in any areas identified as posing a higher risk of fraudulent activity (revenue recognition, expenditure classification, non-standard journal entries)**
- **Controls over the financial reporting process**
- **Controls over management override**
- **Controls (manual or automated) over computer-generated information**

Control Activities Deficiency

- **Can not map specific control activities to identified risks!!**

Information & Communication

- **Antifraud program and policies must be appropriate, timely, current**
- **Must be properly disseminated so that employees understand their responsibilities**
- **Must contain an effective means of communicating upstream**

Information & Communication Deficiencies

- **Non-existent training on code of ethics**
- **Sharing of information regarding fraud risks, controls activities, and remediation is non-existent or seriously defective**
- **Management fails to consider the risk of computer-based and processed information**

Monitoring

- **Ongoing**
 - Built into the normal, recurring operating activities of the organization
 - Includes regular management and supervisory activities and other actions of personnel in reviewing the activities carried out by others
- **Periodic – Independent evaluations (audits) depend upon**
 - Changes in the entity and their associated risks
 - Competence and experience of individuals performing controls
 - Results of ongoing monitoring

Monitoring Deficiencies

- **Possibility of fraud in day-to-day operations not monitored**
- **I/A does not adequately address fraud risk in annual audit plan**
- **I/A does not include knowledgeable and experienced fraud professionals**