ERM, Internal Control & You

SVPBS Presentation
December 6, 2012
Troy Janes, PhD, CPA
Agenda

- How did we end up with this ERM and internal control stuff?
- What’s the difference between ERM and internal control?
- How does this affect me?
Where did it all come from?
Where did it all come from?

- 1985
  National Commission on Fraudulent Financial Reporting (aka Treadway Commission)

- 1992
  *Internal Control – Integrated Framework*
Where did it all come from?

- 2004

*Enterprise Risk Management – Integrated Framework*
Definition of Internal Control

“…a process...designed to provide reasonable assurance...regarding achievement of (the entity’s) objectives on:

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

(Source: Internal Control-Integrated Framework. 2011. COSO.)
Components of Internal Control
Definition of ERM

“… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Components of ERM
Internal Environment

- Establishes a philosophy regarding risk management. It recognizes that unexpected as well as expected events may occur.

- Establishes the entity’s risk culture.

- Considers all other aspects of how the organization’s actions may affect its risk culture.
Objective Setting

• Is applied when management considers risks strategy in the setting of objectives.

• Forms the risk appetite of the entity — a high-level view of how much risk management and the board are willing to accept.

• Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite.
Event Identification

- Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives.

- Addresses how internal and external factors combine and interact to influence the risk profile.
Risk Assessment

• Allows an entity to understand the extent to which potential events might impact objectives.

• Assesses risks from two perspectives:
  - Likelihood
  - Impact

• Is used to assess risks and is normally also used to measure the related objectives.
Risk Response

- Identifies and evaluates possible responses to risk.

- Selects and executes response based on evaluation of the portfolio of risks and responses.
  - avoiding
  - accepting
  - reducing
  - sharing
Control Activities

- Policies and procedures that help ensure that the risk responses, as well as other entity directives, are carried out.

- Occur throughout the organization, at all levels and in all functions.

- Include application and general information technology controls.
Management identifies, captures, and communicates pertinent information in a form and timeframe that enables people to carry out their responsibilities.

Communication occurs in a broader sense, flowing down, across, and up the organization.
Monitoring

Effectiveness of the other ERM components is monitored through:

- On-going monitoring activities
- Separate evaluations
- A combination of the two
A strong system of internal control is essential to effective enterprise risk management.
COSO Components of Internal Control

- Control Environment
- Risk Assessment
- Information and Communication
- Control Activities
- Monitoring
Control Environment

- Demonstrates commitment to integrity and ethical values
- Exercises oversight responsibility
- Establishes structure, authority and responsibility
- Demonstrates commitment to competence
- Enforces accountability
“Fraud and the Tone at the Top” video is available from the Association of Certified Fraud Examiners (acfe.org) free Fraud Videos Library
Risk Assessment

- Specifies suitable objectives
- Identifies and analyzes risk
- Assesses fraud risk
- Identifies and analyzes significant change
Fraud Risk Factors

Opportunity

Incentive Pressure

Rationalization Attitude
Information and Communication

- Generates/obtains quality information to support the other components of control
- Communicates information internally
- Communicates information externally
Control Activities

- Selects and develops control activities
- Selects and develops general controls over technology
- Deploys through policies and procedures
Control Activities

- Performance reviews
- Information processing
- Physical controls
- Segregation of duties
Segregation of Duties

**FIGURE 7.2**
Establishing Accountability for Assets

- A Maintains
- C Reconciliation of Assets: Held by A to Records, Maintained by B at Reasonable Intervals
- B Maintains
- C Independent Record
Monitoring

- Conducts ongoing and/or separate evaluations
- Evaluates and communicates deficiencies
Limitations of Internal Control

Even the most well-designed controls can fail.

http://www.youtube.com/watch?v=ol4ukdjxdUM
Limitations of Internal Control

- Errors may arise from misunderstandings of instructions, mistakes of judgment, fatigue, etc.
- Controls that depend on the segregation of duties may be circumvented by collusion
- Management may override the structure
- Compliance may deteriorate over time
Internal Control Activity

- Think of a way to steal something.
- Consider:
  - Failure in which components of internal control would allow you to get away with it?
  - What control activity would keep you from getting away with it?
Internal Control Activity

- Disclaimer:
  - This is NOT a criminal training exercise!
  - The goal is to assess risks and determine ways to control risk!
What’s this got to do with me?

“Everyone in an entity has some responsibility for enterprise risk management.”

What can I do?

- Know your role
- Don’t be Kramer
- Be alert
- Communicate
Blowing the Whistle

- Whistleblower rewarded
  - [http://www.cnbc.com/id/48986257](http://www.cnbc.com/id/48986257)

- Now everyone wants to do it
  - [Chicago Tribune article](http://www.chicagotribune.com)
Whistleblower Hotline

- Communication Hotline?
- [http://www.purdue.edu/hotline/](http://www.purdue.edu/hotline/)
- 1-866-818-2620
What’s this got to do with me?

“Everyone in an entity has some responsibility for enterprise risk management.”

Questions?
Comments?
Rebuttals?
Hopefully this is not how you feel…