Central Kentucky Chapter
AGA
April 13, 2017

Enterprise Risk Management

A Personal Approach

presented by

Dr. Jannett D. Bradford, CGFM

Southeast Regional Vice President

AGA

OVERVIEW

- COSO
- IC Framework 1992
- IC Framework 2013
- ERM Framework 2004
- Circular A-123 Update July 2016
- ERM Up-Close and Personal

The Committee of Sponsoring Organizations (COSO)

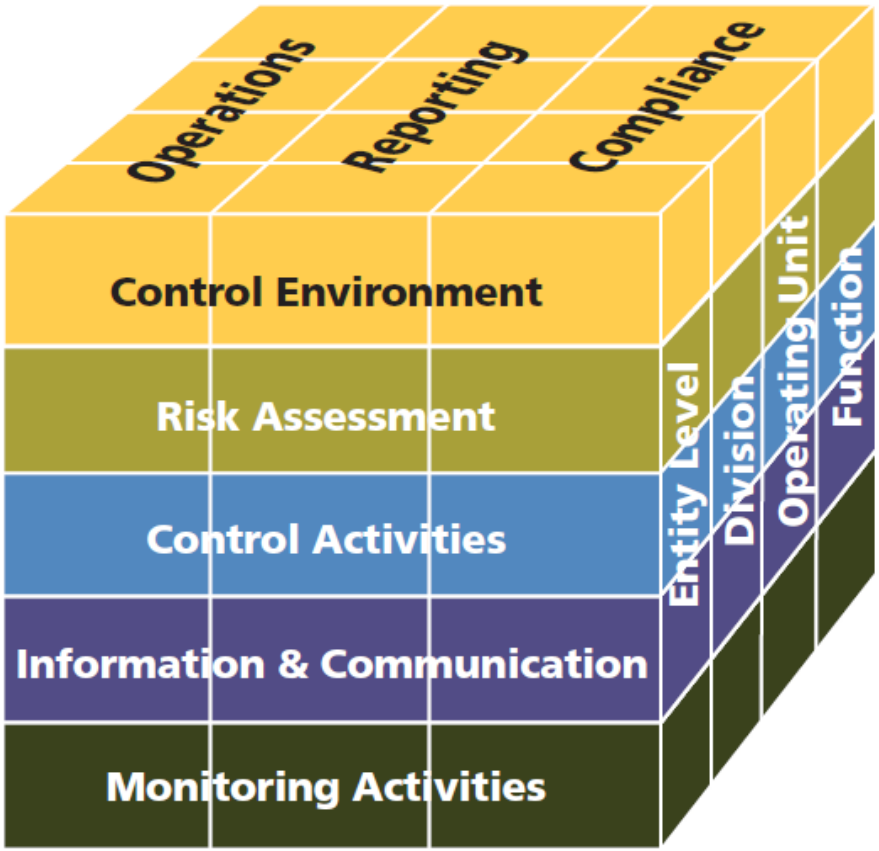
- COSO organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting
- COSO sponsored jointly by five major US professional associations
  - American Accounting Association (AAA)
  - American Institute of Certified Public Accountants (AICPA)
  - Financial Executives International (FEI)
  - Institute of Internal Auditors (IIA)
  - Institute of Management Accountants (IMA)
- *Internal Control –Integrated Framework* published September 1992

AGA
COASTAL GEORGIA CHAPTER

Internal Control Framework 1992

AGA
COASTAL GEORGIA

Internal Control Framework 2013



Changes from 1992 to 2013

- Expansion of the scope of reporting objectives beyond financial information
- Changes in business and operating environment are considered
- Formalization of fundamental concepts into 17 principles
- Points of focus included that highlight important characteristics of the 17 principles

Changes from 1992 to 2013 (cont'd)

- Additional approaches and examples added
- Explicit consideration given to outsourced service providers and other third parties affecting internal control
- Explicit consideration of the potential for fraud in risk assessment
- Specific principle related to IT

Principles

- The 17 principles enable effective operation of the five components and of the overall process.
- Specific controls are not prescribed.
- Management identifies and oversees the execution of controls that impact or influence the principles.

Principles (continued)

- Control Environment (5)
  - The organization demonstrates a commitment to integrity and ethical values.
- Risk Assessment (4)
  - The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- Control Activities (3)
  - The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Principles (continued)

- Information & Communication (3)
  - The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
  - The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.
- Monitoring Activities (2)
  - The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Points of Focus

- Points of focus represent important characteristics associated with the principles.
- Control Environment Principle 1:
  - The organization demonstrates a commitment to integrity and ethical values.
- Four points of focus for control environment principle 1:
  - Sets the Tone at the Top.
  - Establishes Standards of Conduct.
  - Evaluates Adherence to Standards of Conduct.
  - Addresses Deviations in a Timely Manner.

Financial Scandals - 1998 forward

- 1998: Waste Management of Houston, reported $17B in fake earnings

- 2001: Enron of Houston failed to report huge debts
  - Shareholders lost $74B
  - Employees and investors lost retirement savings
  - Many employees lost their jobs

- 2002: Worldcom
  - Inflated earnings by as much as $11B
  - 30,000 jobs lost
  - Investors lost about $180B

Financial scandals (cont'd)

- 2002: Tyco, New Jersey-based blue chip Swiss securities company
  - CEO Dennis Kozlowski and former CFO Mark Swartz stole $150M
  - Inflated company income by $500M
  - Kozlowski threw his wife a $2M birthday party, with appearance by Jimmy Buffett

- 2003: HealthSouth, largest publicly traded healthcare company in US
  - Inflated earnings by $1.4B to meet stockholder expectations
  - CEO Richard Scrushy sold $75M in stock the day *before* the company posted a huge loss
  - Served 70 months for bribing Alabama Governor Don Siegelman
  - Plaintiffs awarded $2.88B civil judgment

Financial scandals (cont'd)

- 2003: Freddie Mac, Federally-backed mortgage financing giant
  - $5B in earnings misstated
  - Discovered as part of SEC investigation
  - Fannie Mae, the other Federally-backed mortgaged financing company also caught in a scandal about 1 year later

Enterprise Risk Management (ERM) Framework 2004

- *Enterprise Risk Management – Integrated Framework*
  - COSO initiated project in 2001
  - Purpose: Develop readily usable framework to enable management to evaluate and improve their organization's enterprise risk management
  - ERM incorporates the internal control framework
    - Not intended to replace internal control framework
- Definition

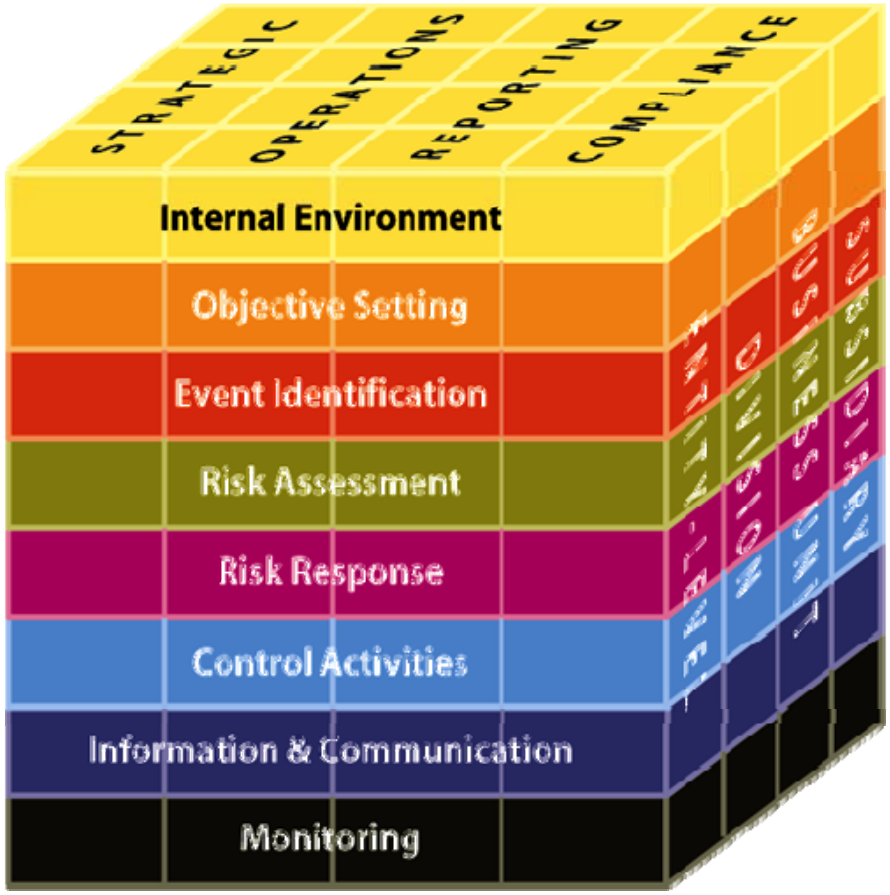
  ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding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

ERM Framework 2004 (continued)

- A *process*
- *Effected by people*
- *Applied in strategy setting*
- *Applied across the enterprise*
- *Risk appetite*
- *Provides reasonable assurance*
- *Achievement of objectives*

AGA
COASTAL GEORGIA CHAPTER

ERM Framework 2004 (continued)



OMB Circular A-123 Update Jul 2016

- Formerly the Circular on Internal Control
- Now, Management's Responsibility for Enterprise Risk Management and Internal Control
- ERM implementation effective FY 2017, which began October 1, 2016
- Federal executive agencies encouraged to establish a Risk Management Council to provide governance for the risk management function
- Emergence of the Chief Risk Officer
- Agencies must maintain a risk profile

OMB Circular A-123 Update Jul 2016 (cont'd)

Agency risk profile must include

- Identification of Objectives
- Identification of Risk
- Inherent Risk Assessment
- Current Risk Response
- Residual Risk Assessment
- Proposed Risk Response
- Proposed Action Category

Internal Environment
AGA Code of Ethics

- Revised at 2016 PDT in Anaheim in July
- Code sets minimum expected level of behavior and creates expectation: AGA members and CGFMs will do the right thing in any given situation.
- Code of Ethics defines our “Internal Environment”
- Code covers four facets
  - The Public Interest
  - Objectives
  - Principles
  - Professional Conduct

The Public Interest

The public expects us to be trustworthy and we should be accountable in the public interest. We should

- Abide by the expectations, standards, and rules of the position, and seek necessary information to interpret and apply them.
- Accept personal responsibility for the foreseeable consequences of action(s) and inaction.
- Take into account the long-term interest of the government and its citizens.

Objectives

Government financial management professionals should work at the highest standards of professionalism, attain the highest levels of performance and meet the public interest requirement. To accomplish this, four basic needs must be met:

- Credibility: Be believable and trustworthy
- Professionalism: Act with skill, good judgment, and polite behavior expected of one trained to do a job well
- Quality of Service: Highest standards of performance
- Confidence: Instill in others a full and strong believe that ethics govern your actions

Principles

- Integrity: Be straightforward and honest
- Objectivity: Be fair; do not allow prejudice, bias, conflict of interest or influence of others affect your decision-making
- Professional Competence and Due Care: Perform job duties with diligence; maintain professional knowledge and skills to work effectively and efficiently
- Confidentiality: Do not disclose or use any confidential information without proper, specific authority, or a legal or professional right or duty to disclose

Professional Conduct

1. Obey the law.
2. Conduct yourself with integrity, dignity, and respect for others.
3. Transmit and use confidential information only for the purpose intended, not for personal gain or advantage, nor to the disadvantage of others.
4. Adhere to the standards of conduct of your employer and any professional associations or organizations of which you are a member.

Professional Conduct (cont'd)

5. Perform duties of your position and supervise the work of your subordinates with the highest degree of professional care.
6. Render opinions, observations or conclusions for official purposes only after appropriate consideration of the pertinent facts.
7. Exercise diligence, objectivity, and honesty in your professional activities, including utilization and management of funds.
8. Avoid any activity that creates or gives the appearance of impropriety.

Risk Assessment

- Inherent and Residual Risk
- Likelihood: The possibility that a given event will occur
- Impact: The effect of the event
- Risk Score: Likelihood times Impact

Risk Assessment (continued)

- Likelihood scale:
  - 1 – Very Low
  - 2 – Low
  - 3 – Moderate
  - 4 – High
  - 5 – Very High
- Impact scale:
  - 1 – Insignificant
  - 2 – Minor
  - 3 – Moderate
  - 4 – Major
  - 5 - Catastrophic

Risk Assessment (continued)

- For an event that is highly likely (4) to occur but the impact is minor (2), then its risk score is 8.
- If the event is highly likely (4) to occur but the impact is catastrophic (5), then its risk score is 20.
- For this set of likelihood and impact values, the higher the score, the greater the risk.

Risk Assessment (continued)

- Likelihood scale:
  - 1 – Very High
  - 2 – High
  - 3 – Moderate
  - 4 – Low
  - 5 – Very Low
- Impact scale:
  - 1 – Catastrophic
  - 2 – Major
  - 3 – Moderate
  - 4 – Minor
  - 5 - Insignificant

Risk Assessment (continued)

- For an event that is highly likely (2) to occur but the impact is minor (4), then its risk score is 8.
- If the event is highly likely (2) to occur but the impact is catastrophic (1), then its risk score is 2.
- For this set of likelihood and impact values, the lower the score, the greater the risk.

Risk Response

- *Avoidance*. Exit the activities giving rise to risk.
- *Reduction.* Take action to reduce the risk likelihood, impact, or both.
- *Sharing.* Transfer or otherwise share a portion of the risk.
- *Acceptance.* Take no action to affect the likelihood or impact of risk.

Summary

- COSO Frameworks
  - 1992 Internal Control
  - 2004 ERM
  - 2013 Internal Control Updated
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
- The Internal Environment: AGA Code of Ethics
- Risk Assessment
- Risk Response