Enterprise Risk Management: Benefits, Adoption, Integration

Central Ohio AGA Professional Development Training
October 31, 2018

Charles T. Saunders, PhD, CIA, CFE, CCSA, CRMA, CPA (OH inactive)
Franklin University
Columbus, Ohio

A Few Examples of Governmental Risks

1. Environmental health (Sabogal & Hubbard, 2015)
2. Influenza pandemic (Steinhardt (GAO), 2009)
3. Municipal finance (Ponton & Darcy, 2006)
4. Credit ratings (Greer, 2016)
5. Economics of public health services (Jacobs et al., 2011)
6. Local government performance (Murray & Dollery, 2005)
7. Information, information systems, technology (Davis, 1998)
8. Risks related to employment, human resources, benefits (Campagna & Schriesheim, n.d.)
9. Complexity of rules, regulations, laws, jurisdiction (Ostermann & Aymonin, 2004)
10. Weather and disaster preparedness (Oppelaar, 2007)
11. Climate change (Poyar & Beller-Simms, 2010)
12. Risks that are unique to the public sector (Hofmann, 2008)
13. Environmental risks (Jung, 2002)
14. Pension plans (U. S. GAO, 2010)
15. Absence of awareness of risk, risk management (Meyer & Solomon, 1984)

What's at risk? What Have You Got to Lose? Here Are Some Considerations:

1. What is the total "human" value of your organization (consider all possible impacts)?
2. Where is the "non-human" value in your organization?
3. What is the value (i.e., balance sheet amounts) of that?
4. How much can you reasonably afford to lose?
5. How could that value be lost?
6. How big would a "catastrophic" loss be? Puts you out of business? A "show stopper"(temporary, prolonged, long-term, permanent)?
7. What impact would a loss in your organization have on other organizations? People? Programs?
8. Other than material loss, what are other related loss impacts: Reputation? Social? Political? Public? Customers? Suppliers?
9. Is loss foreseeable? Inevitable? Preventable? Manageable? Insurable? Recoverable?
10. Are preventive measures, adequate insurance, and recovery plans in place?

The "Big Question":

How Do You Know???

Renewed Perspective a Potential Benefit of Enterprise Risk Management…

"These aren't our real numbers, but darn it, they're the numbers we deserve!" (Source: Harvard Business Review)

COSO Definition – Internal Control

- A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations.

Enterprise Risk Management Definitions – Then and Now

- COSO (original): Enterprise Risk Management 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.
- COSO (2017): Enterprise Risk Management is the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value. ERM emphasizes its focus on managing risk through:
  - Recognizing culture
  - Developing capabilities
  - Applying practices
  - Integrating with strategy-setting and performance
  - Managing risk to strategy and business objectives
  - Linking to value

ERM Risk Management Principles – Categories – 1 of 5

(Committee of Sponsoring Organizations of the Treadway Commission, 2017)

❖Governance & Culture

1. Exercises Board Risk Oversight
2. Establishing Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

ERM Risk Management Principles – Categories – 2 of 5
(Committee of Sponsoring Organizations of the Treadway Commission, 2017)

- Strategy and Objective-Setting
  6. Analyzes Business Context
  7. Defines Risk Appetite
  8. Evaluates Alternative Strategies
  9. Formulates Business Objectives

ERM Risk Management Principles – Categories – 3 of 5
(Committee of Sponsoring Organizations of the Treadway Commission, 2017)

- Performance
  10. Identifies Risk
  11. Assesses Severity of Risk
  12. Prioritizes Risk
  13. Implements Risk Responses
  14. Develops Portfolio View

ERM Risk Management Principles – Categories – 4 of 5
(Committee of Sponsoring Organizations of the Treadway Commission, 2017)

- **Review & Revision**
  15. Assesses Substantial Change
  16. Reviews Risk and Performance
  17. Pursues Improvement in Enterprise Risk Management

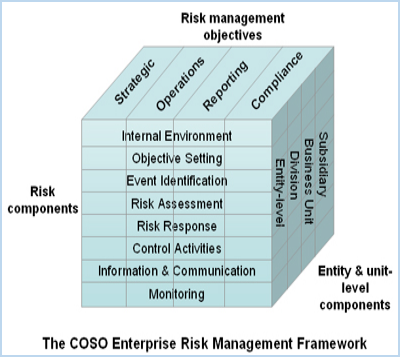
ERM Risk Management Principles – Categories – 5 of 5
(Committee of Sponsoring Organizations of the Treadway Commission, 2017)

- **Information, Communication, & Reporting**
  18. Leverages Information and Technology
  19. Communicates Risk Information
  20. Reports on Risk, Culture, and Performance

COSO Frameworks

- Internal Control

- ERM



The COSO Enterprise Risk Management Framework

Prevention: Risk Assessment (Girgenti & Hedley, 2011, pp. 123 - 137)

1. Design Considerations
2. Identify Business Units, Locations, or Processes to Assess
3. Inventory and Categorize Fraud and Misconduct Risks
   1. Interviews
   2. Documentation Reviews
   3. Focus Groups
   4. Risk Rating
4. Weigh the Likelihood of the Risk (e.g., Fraud or Loss Occurrence)
5. Assess the Potential Significance of the Risk (Financial and Non-financial)
6. Remediate Risks through Control Optimization

Prevention: Codes of Conduct, Communication, and Training (Girgenti & Hedley, 2011, pp. 141 - 142)

1. Design Fundamentals
   1. Who should design and implement a code?
   2. What types of standards should a code contain?
   3. When and to whom should the code be communicated?
   4. Where should the code be rolled out?
   5. How should a code's effectiveness be evaluated?
2. Design and development:
   1. Develop and prioritize list of key risk areas, relevant policies
   2. Consistency of provisions with existing policies and procedures
   3. Determine gaps among related policies and procedures
   4. Test the code for readability, realistic, relevance
   5. Develop realistic, illustrative Q and A
   6. Obtain approval of final document – senior management, board

Prevention: Codes of Conduct, Communication, and Training (cont.) (Girgenti & Hedley, 2011, pp. 142 - 154)

Features of a well-designed code include:

- High-level endorsement
- Mission, vision, values
- Avoid "legalese" and authoritarian tone
- Translate code into local languages
- Practical guidance
- Visually inviting format
- Internal reporting mechanisms
- Enforcement mechanisms
- Code content
- Code organization
- Adjunct topical guidance
- Code distribution
- Code certification
- Evaluate code's effectiveness
- Communications and training
  - ✓ Organizational imperative
  - ✓ Cost (spend the money!)
  - ✓ Legislative imperative
  - ✓ Compliance program annual report
- Leadership education and training
- Tone at the top—and the middle!

Effective Communication and Training Strategy (Girgenti & Hedley, 2011, pp. 154 - 159)

1. Strategy
   a. General awareness training
   b. Topic-specific training
   c. Refresher training
2. Content
   a. Integrate organizational values
   b. Publicize reporting mechanisms
   c. Use realistic examples
   d. Track attendance
   e. Ensure readability
   f. Provide translations
3. Get the message to stick – use multiple communication methods, including:
   - Internal & external mail
   - Group or town hall meetings
   - Articles in newsletters
   - Speeches by senior executives
   - Bulletin board postings
   - Voice mail messages
   - Letters and memos
   - Code of conduct
   - Paycheck stuffers

Effective Communication and Training Strategy (Girgenti & Hedley, 2011, pp. 154 - 159) (con't.)

3. More multiple communication methods:
   - Videos, posters, cafeteria table cards
   - Wallet cards with hotline number and core values
   - Vary training methods (different learning patterns, keep training interesting and fresh)
4. Follow-up to Evaluate Effectiveness – <u>Always!</u> (examples):
   - Before/after analysis of hotline calls
   - Survey to measure comprehension
   - Effectiveness survey – communications, training vehicles, learning facilitation processes
   - Just ask! Use informal feedback channels – and pay attention, especially to trends!

References

Committee of Sponsoring Organizations of the Treadway Commission (2017). *Enterprise Risk Management: Integrating with Strategy and Performance*. Durham, NC: COSO.

Girgenti, R.H. & Hedley, T.P. (2011). *Managing the risk of fraud and misconduct*. New York: McGraw-Hill.