Enterprise Risk Management: A Practical Approach

Presented by:
Ellen M. Labita, CPA, Partner, Not-for-Profit Services
Baker Tilly Virchow Krause, LLP
Ellen.Labita@bakertilly.com
631-719-3232
Agenda

- Overview of Enterprise Risk Management
- ERM Process
- Risk Assessment
- Infrastructure / Ongoing Process
Risk management failures in history

1637: The tulip bulb craze
1720: The South Sea bubble
1989: The S&L crisis
1995: The Barings Bank derivatives scandal
2001: Enron
2002: WorldCom
2008: Housing collapse
2010: Gulf oil spill
2012: JP Morgan, Knight Capital
Risk is the *possibility* of an event occurring that will *impact* the achievement of an organization’s mission and objectives.

**WHY IS THERE AN INCREASED EMPHASIS ON RISK?**
What is ERM?

COSO definition – 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 model

Source: COSO, *Enterprise Risk Management – An Integrated Framework*
Why implement ERM: The Value Proposition

• Broaden view of risk to address how it affects strategic plan and sustainability
• Optimize the cost of risk management
• Improve business performance
• Improve process efficiency
• Enhance governance
Tips for Implementing ERM

- Get started
- Keep it simple and doable
- Remember that risk is constantly changing
Keys to Success

- Support of and from the top
- Use incremental steps
- Focus on key risks
- Leverage existing resources
- Build on existing risk management activities
- Embed ERM into the business culture
- Ongoing updates
Steps for ERM

- Determine ERM leadership and working group
- Define risk appetite
- Conduct enterprise-wide risk assessment
- Implement plan for high priority risks
- Inventory/advance risk management infrastructure and reporting
- Continuous update
Conducting Risk Assessment

- Identify risks
- Prioritize risks
Types of Risk

- Fraud
- Operations
- Finance
- Compliance
- Technology
- Strategy
- Reputation
Identify Risks

- Brainstorm potential risks at a strategic entity-wide level

- Alternatively, use an outside, objective party to interview key Board Members and Management and draft an initial set of priorities
Prioritize Risks

- Prioritize risks based on significance (i.e., potential impact) and likelihood (i.e., chance of occurrence)
- Use a risk map as a roadmap for discussions and oversight
- Risks with the biggest potential impact and highest likelihood of occurrence are the top priority
Risk Mapping
Sample Risk Map

High Impact / Moderate Likelihood

- Legal and Regulatory Environment
- Business Continuity Planning and Disaster Recovery
- Information Retention and Institutional Knowledge
- Governance Effectiveness
- Employee Conduct
- Accounting Systems/Financial Reporting

High Impact / High Likelihood

- Data Security and Privacy
- Funding Cuts/ Budgeting
- Program Safety
- Media/Social Media
- Growth
- Management Succession

Moderate Impact / Moderate Likelihood

Moderate Impact / High Likelihood

- Strategy
- Operations
- Compliance
- Reputation
- Technology
Implement for High Priority Risks

• Clarify who is responsible for developing, implementing, and managing risk management plans
  • Who “owns” each risk and is responsible for developing plans?
  • The CEO/ED has ultimate responsibility for risk management in an organization
• Develop responses/plans to manage and mitigate risk, and monitor results
  • This should include determining what risk management activities are already in place and weighing cost/benefit of risk reduction proposals
Risk Response

- Avoid the risk
- Seek an opportunity and exploit the risk
- Remove the source of risk
- Change the likelihood
- Change the consequences
- Share the risk with another party
- Retain the risk
Key Questions

Was the risk assessment process comprehensive?

Are conclusions related to strategic risk appropriate?

Are problems and solutions presented and discussed within a comprehensive context of competing priorities and resources?

Are solutions transparently vetted in terms of alternative approaches?

Are solutions discussed and decided based on risk/return characteristics?

Do solutions address enterprise-wide risks?

Are resources being allocated to key strategic risks and strategies to protect the organization and help achieve goals?
Risk Management
Infrastructure and Reporting

- Assess risk management capabilities
- Develop/enhance infrastructure to reach the desired state of ERM
- Develop reporting plan/requirements
ERM is a journey, not a destination!