Fear, Uncertainty, Doubt

However,

ERM = Manageable

OK, Back to The Bonadio Group Standard…

Enterprise Risk Management

An Overview on Key Controls

Big firm capability. Small firm personality.

THE BONADIO GROUP

CPAs, Consultants & More

We Will Cover

- Why ERM
- ERM COSO basics
- Tangible benefits in an ERM Program
- Stakeholder Communication
- Building an ERM Program
- Key Takeaways
- What to Do Now

Definitions

- NPI – Non-Public Information
- PII – Personally Identifiable Information
- PHI – Protected Health Information
- FTC – Federal Trade Commission
- ITGC – Information Technology General Controls
- ISP – Internet Service Provider
- CSIRT – Computer Security Incident Response Plan
- E-Banking – Electronic Banking
- SOC Report – Service Organization Control Report
- Cybersecurity – protections against the criminal or unauthorized use of electronic data
- VPN – Virtual Private Network
- BCP – Business Continuity Plan
- DRP – Disaster Recovery Plan
- BIA – Business Impact Analysis
- IPS – Intrusion Prevention Software/System
- IoT – Internet of Things
- BOT – Automated program that runs over the Internet
- DDoS – Distributed Denial-of-Service attack
- Phishing – email/internet “pick pocketing”
- ISP – internet service provider
- Blockchain – open, distributed ledger transactions in a verifiable and permanent way
- BA – Business Associate

Why ERM

- Creation of a more risk aware culture for the organization
- Consistent risk reporting
- Improved focus and perception on risk
- Competent use of resources
- Effective synchronization of regulatory and compliance matters
- Creates collaborations between risk management and Internal Audit
- Supports value creation through risk management

Why ERM

- Cybercrime will exceed ***$2 Trillion*** by 2019: top threat to infrastructure, productivity, and revenue in every industry
- Fraud and error losses average 5.8% of revenue
- Third-Party Risk is advancing rapidly in our increasingly collaborative business landscapes
- From day-to-day operational choices to the essential trade-offs in the boardroom, dealing with uncertainly in business choices is a part of our organizational lives
- If you don't measure it you cannot accurately assess the risk

Why ERM

Stay out of the News

- CEO of New York's Oldest Credit Union Faces Fraud and Embezzlement Charges
- Equifax has spent $242.7 million on its data breach so far
- NY OSC Annual Report on Audits of State Agencies and Public Authorities
- ECMC spends millions to recover from ransomware attack
- Uber Faces Stricter FTC Oversight After Concealing Breach

ERM COSO basics

- 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
  - ✓ A tool to manage risks within your unique risk appetite
  - ✓ A method that provides reasonable assurance regarding the achievement of entity objectives

ERM COSO basics

- ERM
  - ✓ Assesses where value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day
  - ✓ Includes a response process that reduces the likelihood of downside outcomes and increases the upside
  - ✓ Is managed to improve collaboration, trust, and information sharing
- COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management

Benefits of an ERM Program

- Helps organizations deal efficiently with known and potential events that create uncertainty
- Per COSO “Good risk management and internal control are necessary for long term success of all organizations”
- COSO 2013 enhanced the framework’s content and relevance in an increasingly complex business environment so that organizations can attain better value from enterprise risk management
- Helps remove the “Black Swans”

COSO ERM 2013

- Framework focused on fewer components (five)

- Uses focused call-out examples to emphasize key points (> 30)
- Follows the business model versus an isolated risk management process

COSO ERM 2013

- 20 key principles within each of the five components

Governance & Culture

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

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

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

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

COSO ERM 2013

- ERM considers activities at all levels of the organization as an interactive ongoing process

COSO ERM 2013

- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy

COSO ERM 2013

- Builds links to internal control:
  - The document does not replace the Internal Control –Integrated Framework
  - The two frameworks are distinct and complementary
  - Both use a components and principles structure
  - Aspects of internal control common to enterprise risk management are not repeated
  - Some aspects of internal control are developed further in this framework

Stakeholder Communication

- All entities operate in environments where factors such as globalization, technology, restructurings, changing markets, competition, and regulation create uncertainty
- Uncertainty creates risks; ERM allows entities to manage risks to within their risk appetite
- Risk Management allows entities to provide maximum value to stakeholders with reasonable assurance that risks outside their risk appetite will be prevented
- ERM will help prevent future business failures and scandals

Stakeholder Communication

- Company correctly utilizing ERM will satisfy the requirements set forth by almost all regulations requiring measurable internal controls.
- ERM expands on internal controls by focusing on risk from a portfolio perspective
- ERM requires that strategic objectives align with **operations**, **reporting**, and **compliance** objectives.
- ERM discusses the concept of potential events and it recognizes that events can have positive and negative effects.

Stakeholder Communication

- Risk assessment is a more detailed process under ERM. It looks risk on a residual and inherent basis, and describes how a risk can create multiple risks across an entity.
- Risk response options are more detailed under ERM.
- ERM stresses that in some cases control activities themselves serve as a risk response.
- COSO has used the Internal Control- Integrated Framework as a foundation in the creation their Enterprise Risk Management- Integrated Framework

Building the ERM Program

- Find your Leadership Team
- Identify and engage your SME's
- Build consensus on the three ERM pillars
  - ✓ Risk governance: The governance structure reflects the oversight and accountability for risk issues, from individual roles and responsibilities to management committee structures and oversight by the board of directors. The design and implementation of the risk governance structure, including policies, reporting and escalation practices, impact ERM and risk-informed decision-making.

Building the ERM Program

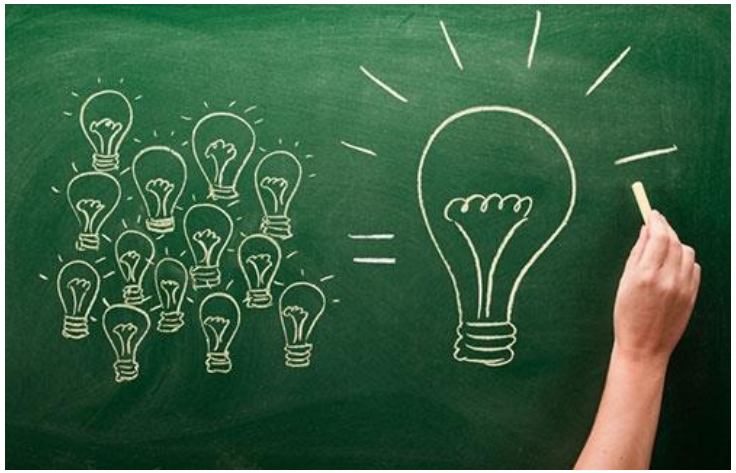
- ✓ Risk appetite: A risk appetite statement articulates the risks an organization is willing to undertake in the pursuit of business objectives. It presents an opportunity for management to clarify to the board and the rest of the organization the nature and extent of acceptable risks in executing the strategy.
- ✓ Risk culture: The keystone that holds things together, culture provides a source of strength or weakness for the organization. An actionable risk culture helps balance the inevitable tension between (a) creating enterprise value through the strategy and driving performance on the one hand and (b) protecting enterprise value through risk appetite and managing risk on the other hand. In effect, risk culture balances the push between strategy and risk appetite.

Building the ERM Program

- Integrate the needed Internal and External factors
  - ✓ Business model complexity
  - ✓ Availability and quality of resources and data.
  - ✓ Known and emerging market trends
  - ✓ Industry regulations
  - ✓ External stakeholder expectations
  - ✓ Unexpected events

Building the ERM Program

- Focus on the big picture
  - Identify and prioritize enterprise risks
  - Quantify, proactively manage and monitor top risks
  - Integrate risk and opportunity analysis into strategy-setting and planning
  - Implement a robust risk appetite framework
  - Disseminate a risk-based mindset across the organization



WHAT TO DO NOW!

Key Takeaway

- Learn the 2013 Standard
- Involve upper management and SME's
- Focus on the big picture
- Measure performance over time
- Understand that an effective ERM program is a differentiator
- It is not one and done
- Let your risk appetite determine your scope
- A risk not measured cannot be controlled

Questions?

Thank You!

Big firm capability. Small firm personality.

THE BONADIO GROUP

CPAs, Consultants & More