April 16 & 17, 2019

Enterprise Risk Management and the Board

Trust earned.
FreedMaxick®

Sanath Rajapakse
Director, Risk Advisory
sanath.rajapakse@freedmaxick.com

Bruce Rumbold
Managing Consultant, Risk Advisory
bruce.rumbold@freedmaxick.com

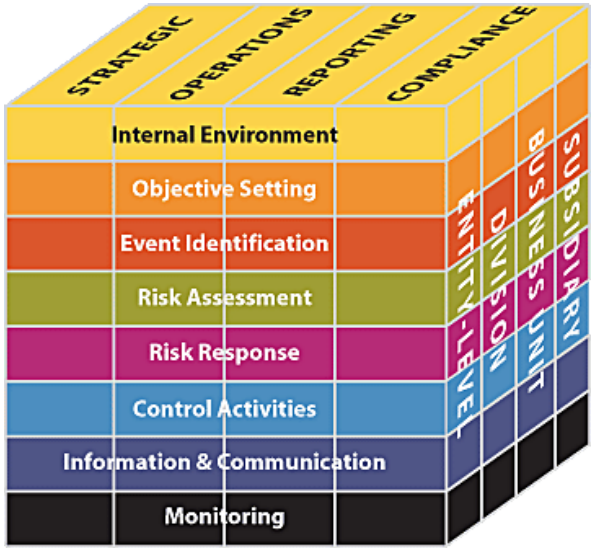
Introduction

Agenda

- ERM History
- ERM Today / Committee of Sponsoring Organizations (COSO Framework)
- COSO Performance Principles
- Governance
- High Performance Boards
- Regulatory Environment
- Trending – ESG Model
- What's Next – Risk Culture

History

- Dates to the 1970s
- Risk management circle of elements – assessment, control, financing and communication. Mostly concerned with transfer of risk via insurance.
- Evolved with the advent of derivative financial products and COSO 2004
- Other drivers:
  - Transparency
  - Financial disclosures
  - Security and technology (Cybersecurity)
  - Business continuity
  - Regulatory compliance



Credit: Committee of Sponsoring Organizations of the Treadway Commission

ERM Today

From the Society of Actuaries (SOA.org)

- The process of coordinated risk management that places a greater emphasis on cooperation among departments to manage the organization's full range of risks as a whole. A framework for effectively managing uncertainty, responding to risk and harnessing opportunities.
- The goal of ERM is to better understand the shock resistance of the enterprise to its key risks.
- COSO 2017 (20 ERM Components and Principles)[1]

  Governance & Culture ● Strategy / Objectives
  Performance ● Review / Revise ● Communicate

1 Credit: Committee of Sponsoring Organizations of the Treadway Commission

ERM Today

COSO'S MISSION [1]

COSO's Mission is "To provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations."

COSO'S FUNDAMENTAL PRINCIPLE [1]

Good risk management and internal control are necessary for long term success of all organizations

1 Committee of Sponsoring Organizations of the Treadway Commission

COSO 2017 Principles[1]

20 key principles within each of the five components

GOVERNANCE & CULTURE	STRATEGY & OBJECTIVE SETTING	PERFORMANCE	REVIEW & REVISION	INFORMATION, COMMUNICATION, & REPORTING
1. Exercises Board Risk Oversight	6. Analyzes Business Context	10. Identifies Risk	15. Assesses Substantial Change	18. Leverages Information and Technology
2. Establishes Operating Structures	7. Defines Risk Appetite	11. Assesses Severity of Risk	16. Reviews Risk and Performance	19. Communicates Risk Information
3. Defines Desired Culture	8. Evaluates Alternative Strategies	12. Prioritizes Risks	17. Pursues Improvement in Enterprise Risk Management	20. Reports on Risk, Culture, and Performance
4. Demonstrates Commitment to Core Values	9. Formulates Business Objectives	13. Implements Risk Responses		
5. Attracts, Develops, and Retains Capable Individuals		14. Develops Portfolio View		

1 Committee of Sponsoring Organizations of the Treadway Commission

COSO 2017 – Performance Principles

Identification • Assessment • Response • Communication

Identification

- Who is conducting and enterprise risk assessment?
- Are all of the categories of risk considered?
- Is there a way to remove silos when considering operational risks
- Is there a risk register?

Credit: Committee of Sponsoring Organizations of the Treadway Commission

COSO 2017 – Performance Principles

Identification • Assessment • Response • Communication

Assessment

- Are all of the risks assessed for likelihood and impact.
- Is velocity a factor?
- How do you measure?
- Right mix of KRI?
- Are risks prioritized?

Credit: Committee of Sponsoring Organizations of the Treadway Commission

COSO 2017 – Performance Principles

Identification • Assessment • Response • Communication

Response

- Mitigate
- Transfer
- Accept
- Stop

Credit: Committee of Sponsoring Organizations of the Treadway Commission

COSO 2017 – Performance Principles

Identification • Assessment • Response • Communication

Communication

- Finding the right balance of information and reporting formats
- How often does the Board / Committee interact with the CRO / CAE?
- Is this an open and honest communication?
- Is there a report on mitigation efforts?
- Do risk ratings change during the year?
- Do you receive enough information to provide proper **oversight** of the risk function?
- Turning KRI into KPI

Credit: Committee of Sponsoring Organizations of the Treadway Commission

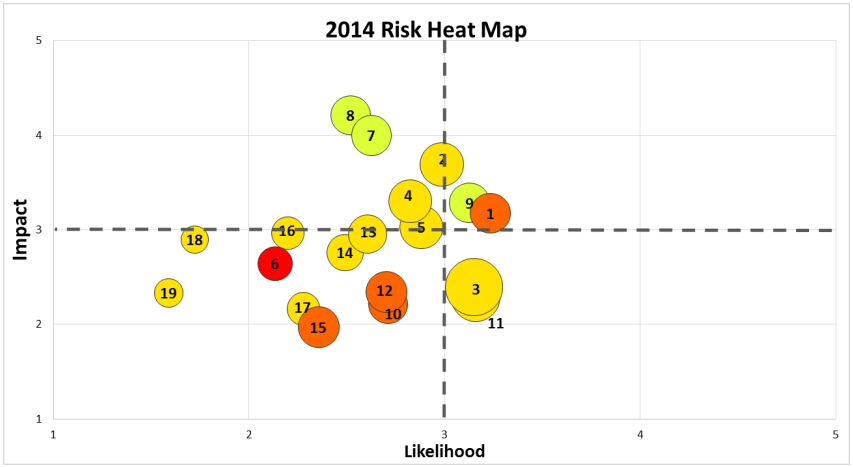
Reporting Examples

Strategic Risk Summary

Risk Category	Risk Exposure Dec	May Changes	Trajectory: Holding	OpCo2	OpCo3	OpCo4	OpCo5	OpCo6
Portfolio			⇨	⇨	⇨	⇨	⇨	⇨
Organizational Culture & Structure			⇨	⇨	⇨	⇨	⇨	
Legal				⇨	⇨			
Key Regulatory			⇧	⇧	⇧	⇧	⇨	⇨
Political/Other Regulatory				⇨	⇩			⇨
Internal Systems & Infrastructure				⇨				
Innovation				⇨	⇨	⇨	⇨	⇨
Competitive				⇩	⇨	⇨		⇨
Business Performance				⇩	⇨	⇨	⇨	⇨
Retail Programs				⇨	⇨	⇨		⇨
Reputation/Trans-formation Agenda			⇨					

Legend: ⇧ Significant Increase ⇧ Moderate Increase ⇨ No Change ⇩ Decrease

High | Medium/High | Medium | Low



INHERENT RISK

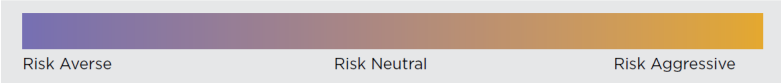
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	11	16	20	23	25
Likely	7	12	17	21	24
Possible	4	8	13	18	22
Unlikely	2	5	9	14	19
Rare	1	3	6	10	15

Impact

Rank	Key Risk	Inherent	Appetite	Target	4Q14	1Q15	2Q15	3Q15	4Q15	Trend
1	Quality Measures	High	ML	M	M	MH	M	M	M	→
2	Medicare Revenue Optimization / Profitability	High	M	ML	MH	MH	MH	MH	MH	→
3	Assess and Manage Margin Sources	MH	ML	ML	MH	MH	M	M	M	→
6	Data & Application Security	MH	ML	ML	MH	MH	MH	MH	MH	→
7	Vendor Management	MH	ML	ML	M	M	M	M	M	→
8	Strategy Development & Alignment	M	ML	ML	L	ML	ML	ML	ML	→
11	Federal & State Healthcare Reform and Regulatory Compliance & Implementation	M	ML	ML	M	M	ML	ML	ML	→
12	Medical Care / Trend Management	M	ML	ML	ML	ML	ML	ML	ML	→
15	Provider Network Management	ML	L	L	ML	ML	L	L	L	→

Governance – Providing Oversight

- Risk *Appetite* / *Tolerance* – what risk level can we cope with in pursuit of our objectives
- Risk appetite statement:
  - Is it a "*statement*"?
  - How is it communicated and **enforced**?
- Risk *Capacity*
- Strategic Objectives – balance between opportunities (risk taking) and threats (risk aversion)



- Do you let risk drive your Strategic Objectives or vice versa?
- Does your product mix align with risk tolerance?
- Is it communicated throughout the organization?

Governance – Structure

Committee Structure

- Does the board have a Risk Committee?
- What is the meeting cadence?
- Are the members qualified?
- How much time does the Committee Chair spend with the CRO and CAE?
- Is the CRO independent of operating units
- Is the risk assessment a living document

High Performance Boards

- Own the strategy
- Build the top team
- Match reward to performance
- Ensure financial viability
- Match risk with return
- Manage corporate reputation
- Drive effective board process

OTHER THOUGHTS

- Ethos of transparency and trust
- Be intentional about recruitment and development
- Set standards and measure performance
- Let the committees due the work
- Agenda driven
- Lose the conflicts

Regulatory environment

What is the current environment?

- It always depends…

Banks should expect continued focus on risk management at the Board and Senior Management level.

FRB Guidance for large financial institutions (LFIs)

- Effectiveness of a Bank's Board of Directors
- Management of business lines and independent risk management and controls
- Recovery planning

Regulatory environment

Risk Based Approach – similar to a review of your Compliance Management System

- Is the bank's risk appetite aligned with operations
- *Example:* is the bank's stated risk preference low while holding derivative securities and granting risky mortgages?

Capital and Liquidity

- Regulators always focus on this but will be reviewing operating units for risk tolerance that is aligned with objectives and risk preferences
- Is there transparency at the Board level? Are you capturing discussions in the minutes? Is it clear that all parties are engaged?

What's next?

ESG - Environmental, Social and Governance

- A model for sustainability
- Currently in use by the investment community / ratings agencies

Environment

Least important for a financial institution but are your buildings LEED certified? Have you tried to go paperless? Would you rather lend to the coal industry or for solar and wind?

Social

How do you help the planet. Are you a socially conscious bank? Are we a great place to work? Are we diverse? Are we using social media properly? What do we do for our community?

Governance

Board composition, culture and entity level controls.
Is there a diversity of skills, tenure, age, gender and ethnicity?

What's Next

RISK CULTURE

We've been talking for 30 years and don't have an answer.

Institute of Risk Management Framework

Credit: Institute of Risk Management

Questions?