Item 3: Committee Education – Sustainable Governance and Enterprise Risk Management

Raina Rose Tagle, CPA, CISA, CIA
Partner and National Practice Leader
Governance, Risk and Compliance Services
Baker Tilly

Finance & Audit Committee Meeting

ERCOT Public
October 10, 2016

BAKER TILLY

Candor. Insight. Results.

Sustainable Governance and Enterprise Risk Management

ERCOT
October 10, 2016

Raina Rose Tagle, CPA, CISA, CIA
Partner and National Practice Leader,
Governance, Risk and Compliance Services

Objectives

BAKER TILLY

Candor. Insight. Results.

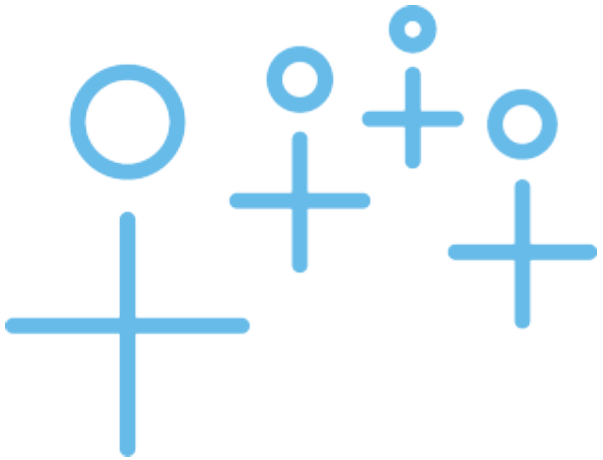
Enable reflection and idea generation regarding evolution and clarity of Board members'/management's roles relative to leading practices for:

- Organizational strategy, oversight, and decision making
- Enterprise risk management (ERM)

BAKER TILLY

Candor. Insight. Results.

Board Roles and Responsibilities



Independent Director Role

BAKER TILLY

Candor. Insight. Results.

Highest level of accountability and authority for organizational decisions

Exercising leadership as an independent director with:

- Duty of care
- Duty of loyalty
- Duty of obedience (good faith)

May delegate many decisions to others, such as senior management

May rely on the advice and counsel of qualified advisors

Not an employee with a job; rather, a fiduciary who performs a role

Management runs the organization; Board oversees, guides, and challenges as needed

Director Role – Accountability and Oversight

BAKER TILLY

Candor. Insight. Results.

Accountability:

The director is accountable to the organization as a whole, for which he or she is a fiduciary. This means that the director must also represent the collective interests of the organization's stakeholders.

Oversight:

Key oversight areas include:

- Organization's ethical culture
- Organization's strategy
- Performance and financial reporting
- Risk management (including cyber risk)
- Regulatory compliance
- Executive talent management, including CEO performance, compensation, and succession
- The Board also oversees its own performance and education

Fiduciary Responsibilities

BAKER TILLY

Candor. Insight. Results.

- Organizational mission statement
- Board composition, structure, and leadership
- Selecting, evaluating, and compensating the CEO; monitoring, evaluating, compensating, and replacing organization officers when necessary
- Co-developing, reviewing, and approving management's strategic and business plans
- Reviewing and approving financial objectives, plans, and actions, including significant capital allocations and expenditures
- Monitoring performance against the strategic and business plans
- Ensuring the existence of an adequate organizational compliance and ethics information and reporting system for employees

Board Division of Responsibilities

BAKER TILLY

Candor. Insight. Results.

Essential Functions of the Full Board

- Amendment of governing documents
- Approval of a plan of merger or consolidation
- Sale, lease, or exchange of all of the company's assets
- Dissolution of the organization

Committees

BAKER TILLY

Candor. Insight. Results.

Enterprise Risk Management

Enterprise Risk Management
Purpose

BAKER TILLY

Candor. Insight. Results.

To identify both risks and opportunities presented by the uncertainties faced and to proactively determine what level of uncertainty is acceptable and what steps should be taken to mitigate circumstances that are beyond that level

Enterprise Risk Management is:

BAKER TILLY

Candor. Insight. Results.

A process, ongoing and flowing through an entity

Effected by people at every level of an organization

Applied in strategy setting

Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk

Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite

Able to provide reasonable assurance to an entity's management and board of directors

Geared to achievement of objectives in one or more separate but overlapping categories

ERM Programs: COSO Framework

BAKER TILLY

Candor. Insight. Results.

Levels of Risk

- Strategic
- Operating
- Financial
- Compliance

Bonus Info: Proposed Updated COSO ERM Framework

BAKER TILLY

Candor. Insight. Results.

Risk Governance and Culture

1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Model
3. Defines Desired Organizational Behaviors
4. Demonstrates Commitment to Integrity and Ethics
5. Enforces Accountability
6. Attracts, Develops, and Retains Talented Individuals

Risk, Strategy, and Objective-Setting

7. Considers Risk and Business Context
8. Defines Risk Appetite
9. Evaluates Alternative Strategies
10. Considers Risk while Establishing Business Objectives
11. Defines Acceptable Variation in Performance

Risk in Execution

12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritizes Risks
15. Identifies and Selects Risk Responses
16. Assesses Risk Execution
17. Develops Portfolio View

Risk Information, Communication, and Reporting

18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance

Monitoring Enterprise Risk Management Performance

22. Monitors Substantial Change
23. Monitors Enterprise Risk Management

BAKER TILLY

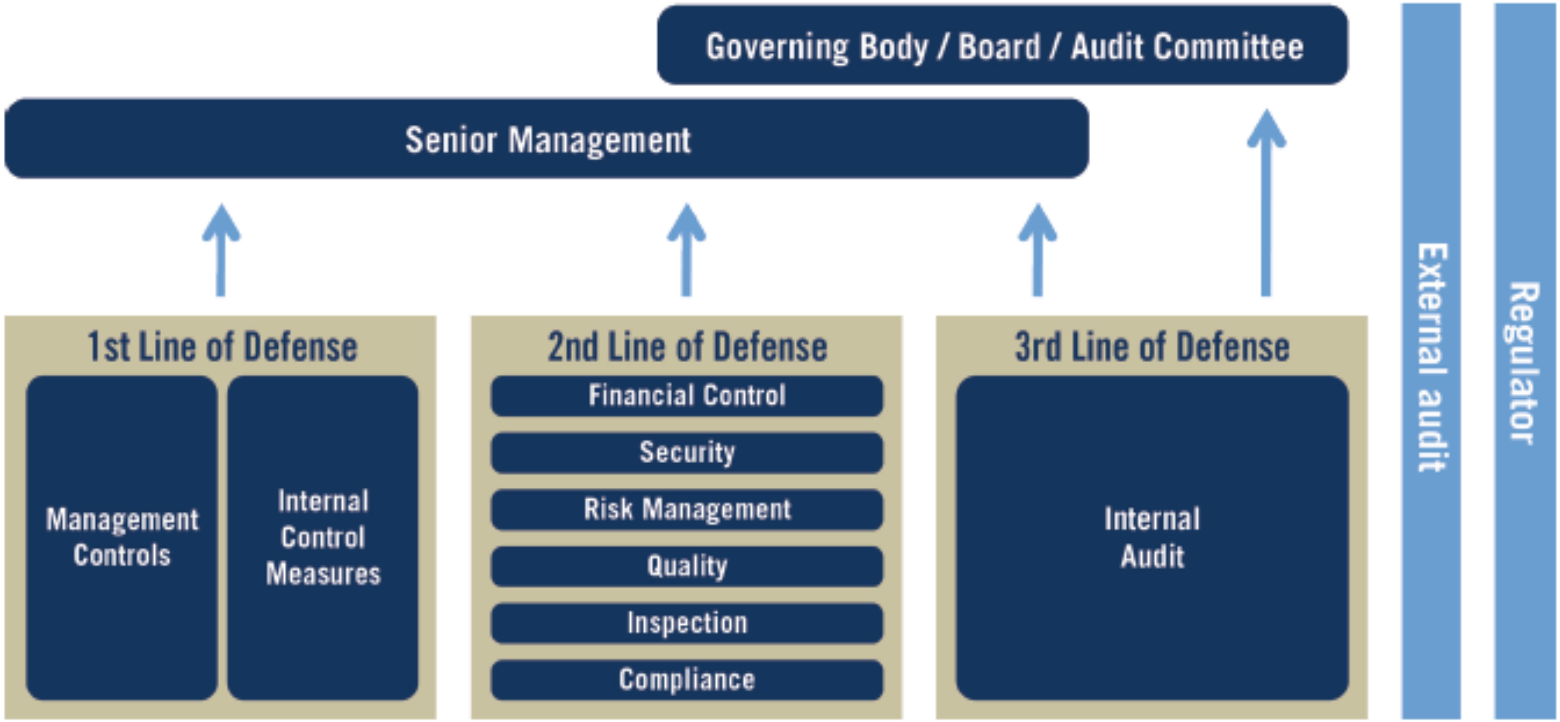
Candor. Insight. Results.

ERM Roles & Process Considerations

Roles – Management, ERM, Compliance, Internal Audit

BAKER TILLY

Candor. Insight. Results.



Institute of Internal Auditors' Three Lines of Defense in Effective Risk Management and Control

Senior Leadership

BAKER TILLY

Candor. Insight. Results.

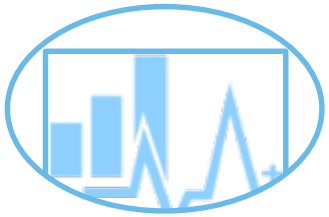
Approve the risk management process	Own the risk	Prepare a strategic risk heat map
Oversee and approve the mitigation strategies	Present to Committee of full Board	Consider operating, financial and compliance risks

The Board

BAKER TILLY

Candor. Insight. Results.

Risks



Receives the strategic risks annually

Oversight

Oversees management process to mitigate strategic risks

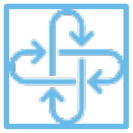
Board Oversight Committee

BAKER TILLY

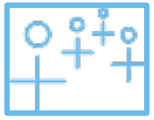
Candor. Insight. Results.

Charter – best practice

Risk management process



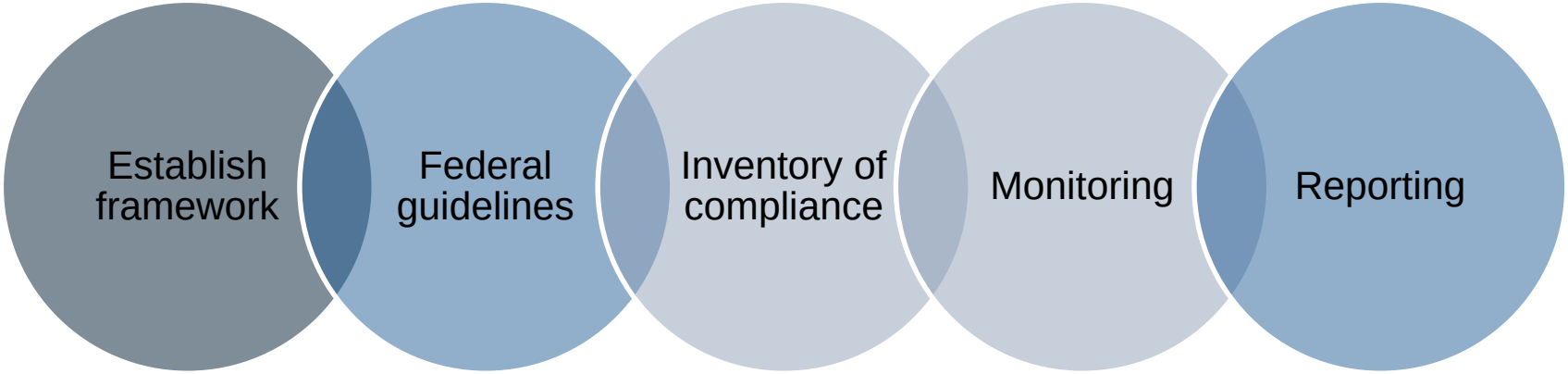
Communicate to the full board



Compliance Risks and Program

BAKER TILLY

Candor. Insight. Results.



ERM: An Alternate Governance View

BAKER TILLY

Candor. Insight. Results.

Enterprise Risk Governance & Policy

Executive Risk Committee	ERM Working Group	Board Committee	Business Units	Internal Audit / Internal Controls
Oversight / ensure consistency, Approve risk rating / response, monitor critical risks	Identify, Measure, Aggregate, Monitor & Report	Set risk appetite, Oversee process, understand critical risks	Take & Manage risks at a department level	Facilitate, Review Process, Leverage, Recommend Improvements and Controls

Various activities to be undertaken within each area of risk governance

BAKER TILLY

Candor. Insight. Results.

ERM Programs – Observations for Evolving and Sustaining

ERM Lessons Learned

BAKER TILLY

Candor. Insight. Results.

Common challenges and lessons learned

- ERM is a journey – keep the process fresh
- Senior leaders own strategic risks
- Don’t overemphasize operating risks
- Consider compliance risks
- Bubble charts, COSO cubes, and influence diagrams aren’t for everyone
- Priorities change over time due to internal and external factors

Approaches for Strengthening and Improving ERM

BAKER TILLY

Candor. Insight. Results.

ERM process assessment

Board strategic risk discussions

Board process oversight

Approaches

Board committees mitigation strategies discussion

Mitigation plans scorecard/dashboard

Sustaining ERM – Evaluation of the ERM Program

BAKER TILLY

Candor. Insight. Results.

Ultimately the responsibility for risk management lies with management and the board

Risk management should be periodically evaluated as to its adequacy to protect enterprise assets, reputation, and ongoing operations

An assessment can examine, evaluate, report, and recommend improvements on the adequacy and effectiveness of management's ERM program

BAKER TILLY

Candor. Insight. Results.

Discussion

BAKER TILLY

Candor. Insight. Results.

Questions?

Contact Information

BAKER TILLY

Candor. Insight. Results.

Raina Rose Tagle

Partner, CPA, CISA

National Consulting Leader, Higher Education

Baker Tilly

raina.rosetagle@bakertilly.com

703 923 8251