UT Dallas 12th Annual Fraud Summit

March 31, 2017

Disclaimer: PwC will not independently validate the feedback received from third-party sources for consideration in the continued development of the Framework
With you today

David Fox
Director, Houston
Risk Management & Compliance Solutions

Amanda Herron
Partner, North Texas
Internal Audit, Risk Management, and Compliance Solutions
COSO
Enterprise Risk Management –
Aligning Risk With Strategy and Performance
Why Update the ERM Framework Now

Since 2004 however, the market has continued to evolve and the COSO Framework is evolving with it.

- ERM concepts and **practices have evolved** and the bar is rising
- There is a need to **incorporate lessons learned** from recent events
- Business **environments are increasingly complex**, technologically driven, and global in scale
- Stakeholders are seeking **greater transparency** and accountability
- Risk **discussions are increasingly prominent** at the board level
A New Title

The updated title illustrates how the Framework...

- Integrates decision making
- Supports strategy
- Focuses on performance
- Delineates between internal control
Depicting Enterprise Risk Management

The updated Framework includes a new graphic to illustrate the alignment of risk, strategy, and performance.

2004 COSO ERM Graphic

Updated COSO ERM Graphic
Clarifying Enterprise Risk Management

Similar to recent COSO Frameworks and guidance, the updated Framework sets out a series of principles:

- Depict the essential aspects of enterprise risk management
- Apply to organizations of all legal structures, size, and purpose
- Are not specific rules that replace management judgment
Clarifying Enterprise Risk Management (continued)

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
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
12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritizes Risks
15. Identifies and Selects Risk Responses
16. Assesses Risk in Execution
17. Develops Portfolio View
18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance
22. Monitors Substantial Change
23. Monitors Enterprise Risk Management Performance
What’s Changed

In addition to a new title, the more substantive changes related to:

1. **Strategy**
   - Elevates discussion of strategy

2. **Performance**
   - Enhances alignment between performance and enterprise risk management

3. **Culture**
   - Examines the role of culture

4. **Controls**
   - Delineates between enterprise risk management and internal controls
Elevates Discussion of Risk and Strategy

- Research suggests that organizations are looking to strengthen the integration between strategy and enterprise risk management
- The updated Framework enhances the conversation of risk and strategy introduced in 2004
Enhances Alignments Between Risk and Performance

The Framework considers how risk relates to performance

For instance, it explores the questions:

- Does the entity understand the risk it is taking when setting performance targets?
- Has the entity performed as expected and achieved its target?
- What risks are occurring that may be affecting performance?
- Did the entity take enough risk to attain its target?
Examines Roles of Risk Culture

- The Framework sets out a “culture spectrum” which aligns with the conversation on risk appetite
- Measuring and reporting on culture remain a key challenge and will likely evolve significantly in the coming years

Risk culture is linked to the conversation of management’s attitude towards risk taking

- Risk Averse
- Risk Neutral
- Risk Aggressive
Delineates Relationship between ERM and Internal Controls

- Internal control remains an integral part of ERM, although users are looking for a more focused ERM document.

- Aspects of internal control that are common to both this publication and *Internal Control—Integrated Framework* are not repeated in the updated Framework.

- Where necessary, aspects of internal control are further developed in the updated Framework.

- The two COSO Frameworks are distinct and provide a different focus — neither supersedes the other.
Emphasizes Relationship between Risk and Value

What the framework did:

2004

“every entity...exists to provide value for its stakeholders; further the value of an entity is largely determined by the decisions that management makes—from overall strategy decisions through to day-to-day decisions.”

2017

- Research suggests the relationship between risk and value could be more prominent
- The updated Framework enhances the focus on how entities create, preserve and realize value

Results

Value is:
- Prominent in the core definition of ERM
- Discussed extensively in principles
- Linked directly to risk appetite and the ability to manage risk to acceptable levels
Issued by COSO, this guide (intended to support Principle 8 of the 2013 Internal Control – Integrated Framework) lays out a framework for organizations to build fraud risk management programs, including:

- Establishing fraud risk governance policies
- Performing a fraud risk framework
- Designing and deploying fraud preventive and detective controls
- Conducting investigations
- Monitoring and evaluating the total fraud risk management program
Ongoing, comprehensive fraud risk management process

1. Establish a fraud risk management policy as part of organizational governance
2. Perform a comprehensive fraud risk assessment
3. Select, develop and deploy preventive and detective fraud control activities
4. Establish a fraud reporting process and coordinated approach to investigation and corrective action
5. Monitor the fraud risk management process, report results, and improve the process
Alignment to COSO 2013 Framework

1. The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.

2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.
Which path are you on?

Principle 8 COSO 2013 Internal Control – Integrated Framework:
The organization considers the potential for fraud in assessing risks to the achievement of objectives.

**Compliance Approach**
Assess fraud on a stand-alone basis

**Programmatic Approach**
Assess fraud risk as part of a broader Fraud Risk Management Program

**Fraud Risk Management Principle #2**
The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

**Fraud Risk Management Principles #1-#5**
In addition to fraud risk assessment, this approach also encompasses fraud risk governance, designing and implementing fraud control activities, fraud investigation and corrective action, and fraud risk management evaluation and monitoring.
**Principle 2: Fraud Risk Assessment**

1. **Establish the fraud risk assessment team considering**
   - Appropriate management levels
   - All organizational components

2. **Identify all fraud risk schemes and fraud risks, including**
   - Internal and external factors
   - Various types of frauds
   - Risk of management override

3. **Determine all personnel and departments potentially involved, considering the fraud triangle**

4. **Identify existing controls and assess their effectiveness**

5. **Assess and respond to residual risks that need to be mitigated**
   - Strengthen existing control activities
   - Add control activities
   - Consider data analytics

6. **Reassess risk periodically considering changes**
   - External to the organization
   - Operational
   - Leadership

7. **Document the risk assessment**

8. **Estimate likelihood and significance of each fraud scheme and risk**

**Process considers all relevant points of focus and opportunities, incentives/pressures and attitudes/rationalizations**
**Principle 2: Fraud Risk Assessment**
Assesses likelihood & significance and how to respond

### COSO endorsed framework

<table>
<thead>
<tr>
<th>Fraud risk</th>
<th>L</th>
<th>S</th>
<th>People or Dept.</th>
<th>Internal control</th>
<th>Assessment of internal control</th>
<th>Residual risk</th>
<th>Fraud risk response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Revenue</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backdating contracts</td>
<td>RP</td>
<td>M</td>
<td>Sales, contract admin</td>
<td>Standard Contracts, &amp; Cut-off</td>
<td>Weak controls in certain divisions</td>
<td>Yes, backdated contracts</td>
<td>Reps from sales dept., Look back analyses</td>
</tr>
<tr>
<td>Manual JE’s</td>
<td>P</td>
<td>M</td>
<td>Accounting, Finance</td>
<td>Systematic ID control, Levels of approval</td>
<td>Good, but Subject to management override</td>
<td>Yes, fraudulent revenue entries</td>
<td>Data mining JEs by IA</td>
</tr>
</tbody>
</table>

L = Likelihood, S = Significance
**Principle 2: Fraud Risk Assessment**

Analysis of internal and external factors

**Internal factors**
- Consider output from the Enterprise Risk Management Process
- Impacts of incentive compensation plans
- Consider control deficiencies from audits
- Review whistleblower log
- Consider changes in personnel in key control positions or positions of authority
- Consider changes in Business and IT processes and controls

**External factors**
- Review relevant SEC Accounting & Auditing Enforcement Actions, and Cease & Desist Orders.
- Review risk factors included in the 10K and those of competitors
- History of litigation against the company and history of frauds common to the industry
- Consideration of prior years’ SEC Comment letters.
Principle 3: Fraud Control Activities

Preventive Controls

- Business process controls
  - How to structure and manage operations
  - Delegation of authority and responsibilities
  - Centralization/decentralization of processes
  - In-house/out-sourcing or sub-contracting
- Physical access controls
- Logical access controls
- Transaction control activities
- Technological control activities

Detective Controls

- Occur in the ordinary course of business
- Draw on external information to corroborate internally generated information
- Routinely and automatically communicate identified deficiencies and exceptions to appropriate leadership
- Use results to enhance and modify other controls
**Principle 4: Fraud Investigation & Corrective Action**

**Point of Focus: Establish Fraud Investigation and Response Protocols**

- Initially evaluating the allegations to determine if an investigation is warranted and the appropriate degree of urgency.
- Notifying employees regarding document presentation and securing data systems.
- If necessary, engaging independent counsel and forensic accounting support.
- Conducting the investigation while controlling and safeguarding evidence.
- Assessing root causes and initiating mitigating processes and controls.
- Reporting the results in the appropriate format (oral summary of key points or comprehensive written report).
- Following policies regarding retention of reports, documents, work papers, and other information.
**Principle 5: Fraud Risk Management Monitoring Activities**

- Number of frauds identified versus complaints, grievances, etc.
- Extent of the loss
- Length of time to detection of fraudulent activity
- Number of interactions with employees and stakeholders, e.g. messages supporting ethical behavior by executives or surveys concerning integrity or culture
- Comparison of the number of frauds discovered versus the number of fraud investigations performed
- Number of vendors and customers who have or have not signed the organization’s ethical behavior requirements
- Number of employees who have or have not signed the corporate ethics statement or completed ethics training
- Number of fraud allegations via the organization’s hotline or other means
- Number of background checks performed and the number of problems identified in those background checks
Thank You

“PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.

Not for further distribution without the permission of PwC.

Disclaimer: PwC will not independently validate the feedback received from third-party sources for consideration in the continued development of the Framework