What is ERM according to COSO?

2004 COSO ERM Definition
"ERM is a process, affected 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."

2017 COSO ERM Definition
"The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value."

2017 COSO ERM Framework – Integrating with Strategy and Performance
This new framework highlights the importance of ERM in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

Five risk management components

COSO's ERM framework focuses on just five key components for building an effective ERM program, and introduces 20 key principles within each of the components.

COSO ERM Framework – why the change and what’s different?

Key differences from COSO’s 2004 ERM Framework:

1. Provides greater insight into the role of ERM when setting and executing strategy
2. Enhances alignment between performance and ERM
3. Expands reporting for greater stakeholder transparency
4. Accommodates evolving technologies and growing data analytics use

Why the change?

The complexity of risks has changed, new risks have emerged, and boards have enhanced their awareness and oversight of ERM while asking for improved risk reporting.

Value of aligning strategy and risk

ERM helps an organization better understand:

- How mission, vision, and core values shape what types and amount of risk are acceptable when setting strategy
- The types and amount of risk the organization potentially exposes itself to by choosing a particular strategy
- The possibility that strategy and business objectives may not align with the mission, vision, and core values
- The types and amount of risk in carrying out the strategy and its ultimate value
Perspectives on the new COSO Framework

Strategic value of ERM

- Increases the range of opportunities
- Increases positive outcomes while reducing negative surprises
- Identifies and manages entity-wide risks
- Reduces performance variability
- Improves resource deployment
- Enhances enterprise resilience

Lessons learned and key takeaways

1. Leverage the new COSO framework to integrate ERM with business practices for improved decision making
2. Understand your company’s risk culture and how it can be measured and monitored to improve risk awareness across the organization
3. Align strategy with mission, vision, values and business objectives
4. Proactively identify, analyze and understand the implications of risks to executing the strategy
5. Spot, assess, and manage emerging challenges and risks to the enterprise’s current business model and strategy
6. “Stress test” the assumptions underlying new strategies or initiatives in order to determine how these choices could be threatened in unexpected ways

Sample Tools
Example ERM dashboard

<table>
<thead>
<tr>
<th>Category Risk</th>
<th>Metric</th>
<th>Current Estimate</th>
<th>Trend</th>
<th>Mitigation Actions</th>
<th>Residual Risk</th>
<th>Executive Sponsor/Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Quarterly Risk Reporting Dashboard

This risk dashboard quickly shows the progress and effectiveness of the mitigation strategies on the key risks.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Owner</th>
<th>Key Risk Indicators</th>
<th>Risk Progress/Update</th>
<th>Risk Owner</th>
<th>On/Off Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Assessment: Case Study

Lynn S. McGivern
Chief Compliance Officer

HCCA Chicago Regional Conference
October 28, 2018
Company Overview

About ATI
- Outpatient Therapy
- 8,000+ workforce
- 5,000+ licensed/credentialed
- 25 States
- 850+ Locations
- 11 A/B MACS
- Home Health (Chicago)
- DME (Hand Therapy)
- Other Programs

Compliance
- Structure
- Scaling
- Employees v. Technology

Compliance IS AN ENTERPRISE WIDE SOLUTION

Compliance Team/Structure

Scaling Risk – Case Study

Mistakes will not end your business. If you are nimble and willing to listen to constructive criticism you can excel by learning and evolving.

© 2018 ATI Holdings LLC All Rights Reserved

Meridith Valiando Rojas
The risk of a wrong decision is preferable to the terror of indecision. Maimonides

Scaling a Risk Assessment

- Operations
- Patient safety
- Strategy
- Legal & regulatory
- Human capital
- Tech
- Disaster recovery
- Finance

KEEP CALM AND THINK BEYOND THE OIG WORK PLAN

- DOJ – Complaints & Settlements
- OIG – Reports Under the Work Plan
- Corporate Integrity Agreements
- Specific State Issues
Scaling - Technology

- How broad is the scope of risk?
- EMR
- Leveraging Technology
- Safeguards

Risk Resources
Discussion Questions

- What have been the key barriers your organization has faced in implementing/maintaining the ERM program?
- What have been the key lessons learned/critical success factors in implementing/maintaining the ERM program?
- How do you articulate the value of the ERM program to others within your organization?
- Please describe your organization's approach to risk assessment?
- How does your organization approach "risk mitigation" (e.g., not just through internal audit or compliance but through management action plans)?
- What monitoring or reporting do you provide related to ERM? To Whom? How frequently?
Speaker Information

Julie Hamilton, CHC, FACHE
Managing Director
Deloitte & Touche
julhamilton@Deloitte.com
Office: 312.486.0303
Mobile: 727.215.3002

Lynn McGivern, LLM, JD
Chief Compliance Officer
ATI Physical Therapy
Lynn.Mcgivern@atipt.com
630.296.2222 x 7193