Enterprise Risk Assessment
Best Practices
Julie Hamilton, CHC, FACHE
Managing Director, Deloitte & Touche
Lynn McGivern, LLM, JD
Chief Compliance Officer, ATI Physical Therapy

What is ERM according to COSO?

2004 COSO ERM Definition
"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, 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's new framework focuses on integration, emphasizes value, links to strategy and performance, recognizes the importance of culture, and focuses on risk-based decision-making.
COSO ERM Framework – why the change and what’s different?

Key differences from COSO’s 2004 ERM Framework:

- Provides greater insight into the role of ERM when setting and executing strategy
- Enhances alignment between performance and ERM
- Expands reporting for greater stakeholder transparency
- 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 possibility that strategy and business objectives may not align with the mission, vision, and core values
- The types and amount of risk the organization potentially exposes itself to by choosing a particular strategy
- The types and amount of risk in carrying out the strategy and its ultimate value
### 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

- **Leverage the new COSO framework to integrate ERM with business practices for improved decision making**
- **Understand your company’s risk culture and how it can be measured and monitored to improve risk awareness across the organization**
- **Align strategy with mission, vision, values and business objectives**
- **Proactively identify, analyze and understand the implications of risks to executing the strategy**
  - Spot, assess, and manage emerging challenges and risks to the enterprise’s current business model and strategy
  - “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>Key risk indicators</th>
<th>Trend</th>
<th>Mitigation actions</th>
<th>Residual risk</th>
<th>Exec sponsor/ Board committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Implementation</td>
<td>Metric: Budget vs. actual (project expenditures)</td>
<td></td>
<td>• Strong controls related to design/deployment of systems</td>
<td></td>
<td>CIO/Board</td>
</tr>
<tr>
<td></td>
<td>Current measure: Under budget</td>
<td></td>
<td>• Strong governance and project planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>project timeline: String milestone met</td>
<td>N/A</td>
<td>• Outside expertise engaged to assist/audit the project.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business case: To be measured in FY11</td>
<td>N/A</td>
<td>• Proactive communications with appropriate stakeholders.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physician Arrangements</td>
<td>Contract database completeness; missing contracts</td>
<td>8/50</td>
<td>• Standardized forms (e.g., contract checklist, contract approval matrix) to be developed.</td>
<td></td>
<td>General Counsel/Legal</td>
</tr>
<tr>
<td></td>
<td>Fair market value calculations</td>
<td>81%</td>
<td>• Corporate policy around physician agreements to be updated and distributed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Guidance related to fair market value to be developed and distributed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA Security</td>
<td>User access controls: Deficiencies found/ controls tested</td>
<td>7/53</td>
<td>• Data encryption on key/required areas</td>
<td></td>
<td>Director of Compliance/C Compliance Committee</td>
</tr>
<tr>
<td></td>
<td>Data protection/ encryption compliance</td>
<td>98%</td>
<td>• Enhance terminated user procedures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Increase security training and awareness; develop annual training module.</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>Rating</th>
<th>Key Risk Indicators</th>
<th>Risk Response / Mitigation Update</th>
<th>Risk Owner</th>
<th>On/Off schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk A</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk B</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk C</td>
<td>○</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- ✗ High (not in acceptable range)
- ○ Medium (near acceptable range)
- ✓ Low (acceptable range)

Illustrative

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

© 2018 ATI Holdings LLC All Rights Reserved
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.

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

Select your state from the below map

[Map Image]

- Compliance
- Technology
- Statewide Efforts
- EMR: QA
- EMR: OSH
- EMR: QI
- EMR: Improvement Project
- Facility Maintenance Log
- Incident Report Form
Lynn S McGivern, LLM, JD
Lynn.McGivern@atipt.com
(630) 296-2222, ext. 7193
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@aitpt.com
630.296.2222 x 7193