

Enterprise Risk Assessment Best Practices

Julie Hamilton, CHC, FACHE
Managing Director, Deloitte & Touche

Lynn McGivern, LLM, JD
Chief Compliance Officer, ATI Physical Therapy

1

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."

2

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.

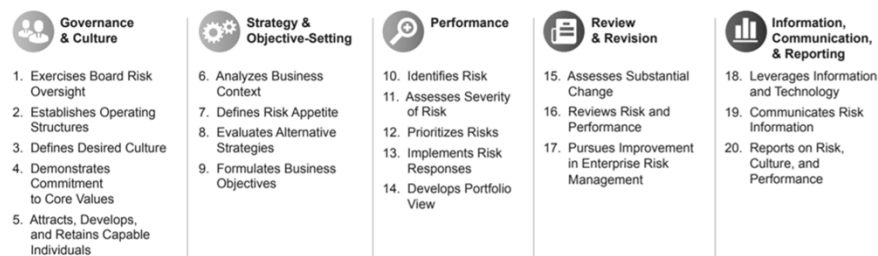


COSO published the ERM framework in September 2017. You can download an executive summary and the full presentation at www.coso.org.

3

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

4

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.

Source: Enterprise Risk Management Integrating with Strategy and Performance September 2017

Perspectives on the new COSO Framework 5

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

6

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

Copyright © 2017 Deloitte Development LLC. All rights reserved.

Perspectives on the new COSO Framework 7

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

Perspectives on the new COSO Framework 8

Sample Tools

Example ERM dashboard

Illustrative

Category/ Risk	Key risk indicators			Mitigation actions	Residual risk	Exec sponsor/ Board committee
	Metric	Current measure	Trend			
IT Implementation	Budget vs. actual (project expenditures)	Under budget	N/A	<ul style="list-style-type: none"> Strong controls related to design/deployment of Strong governance and project planning Outside expertise engaged to assist/audit the project. Proactive communications with appropriate stakeholders. 		CIO/Board
	Project timeline	String milestone met	N/A			
	Business case	To be measured in FY11	N/A			
Physician Arrangements	Contract database completeness; missing contracts	8/50	↓	<ul style="list-style-type: none"> Standardized forms (e.g., contract checklist, contract approval matrix) to be developed. Corporate policy around physician agreements to be updated and distributed. Guidance related to fair market value to be developed and distributed. 		General Counsel/Legal
	Fair market value calculations	81%	↓			
HIPAA Security	User access controls: Deficiencies found/controls tested	7/53	↑	<ul style="list-style-type: none"> Data encryption on key/required areas Enhance terminated user procedures. Increase security training and awareness; develop annual training module. 		Director of Compliance/C ompliance Committee
	Data protection/encryption compliance	98%	↑			

10

Quarterly Risk Reporting Dashboard

Illustrative

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

Risk	Rating	Key Risk Indicators	Risk Response / Mitigation Update	Risk Owner	On/ Off schedule
Risk A	x	.	.	.	
Risk B	✓	.	.	.	
Risk C	O	.	.	.	

x High (no tin acceptable range)
O Medium (near acceptable range)
✓ Low (acceptable range)

11

Risk Assessment: Case Study

Lynn S. McGivern
Chief Compliance Officer

HCCA Chicago Regional Conference
October 28, 2018

the  **ATI** way

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

© 2018 ATI Holdings LLC All Rights Reserved

Compliance

- Structure
- Scaling
- Employees v. Technology

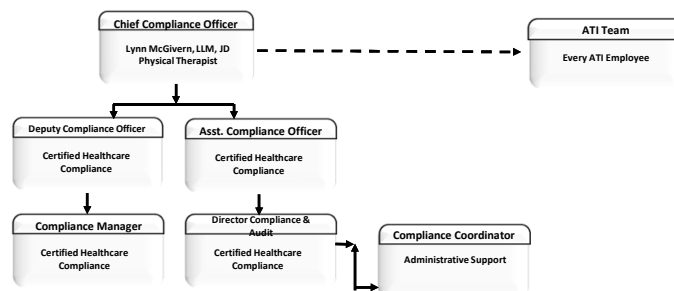


**COMPLIANCE IS AN
ENTERPRISE WIDE
SOLUTION**



the  **ATI** way

Compliance Team/Structure



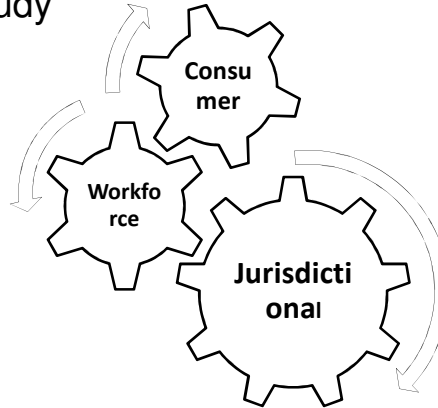
© 2018 ATI Holdings LLC All Rights Reserved

the  **ATI** way

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




© 2018 ATI Holdings LLC All Rights Reserved

the  **ATI** way

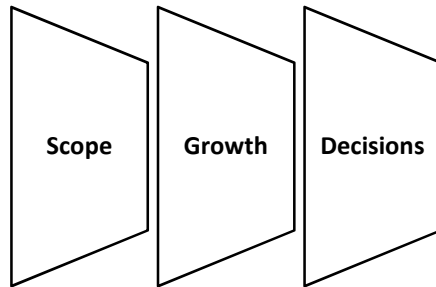
**The risk of a wrong decision
is preferable to the terror of
indecision.**

Maimonides

 BrainyQuote

the  **ATI** way

Scaling a Risk Assessment



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

© 2018 ATI Holdings LLC All Rights Reserved



- 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

the  **ATI** way

Risk Resources

Select your state from the below map



the  **ATI** way

SharePoint

ATl PHYSICAL THERAPY Compliance Hotline
Clinical Operations > Compliance

To *exceed* customer expectations by providing the *highest* quality of care -- friendly -- encouraging environment

Departments Clinical Operations Business Development Human Resources Education Research Locations Corporate

Updated Pages
Compliance
Training, Current
Training
Training Page
Compliance Hub
Map, DMIL_Hover
Mapped States 1050px

Compliance Hub
Upcoming Project
Dates

MSDS - Material Safety
Data Sheets
MSDSOnline

Policies & Procedures
Policy Management
Business Development
Clinical Operations
Compliance
Credentialing
Red Envelope
Risk Management
Risk Mgmt. Reporting

HIPAA Policy Manual
Compliance Program
Guide
Bibazard References
Compliance Team Site
Recent
URAC QI Email

Compliance Hotline

As part of its Compliance Program, ATl Physical Therapy provides several communication channels through which employees may report potential violations of the law or potential violations of ATl's compliance policies. The Compliance Reporting System is designed to provide an easy-to-use, confidential way to report conduct that the employee believes to be illegal, inappropriate or a violation of ATl's Compliance Program. All ATl employees are encouraged to report potential violations to their supervisor or directly to the Compliance Officer in person, by phone, email or by use of interoffice mail.

ATl also provides a hotline for you to anonymously report suspected violations of ATl compliance policies or procedures or the code of conduct as outlined in the Employee Handbook. The hotline number is administered by an external vendor on behalf of ATl. Each caller will be connected to a live person who will answer the call "ATl Physical Therapy". Any information provided during the hotline call is translated into an email and forwarded to the Chief Compliance Officer. Calls to the Hotline will not be traced or recorded. If callers choose to identify themselves, their identity will be kept confidential to the fullest extent possible or as permitted by law. The Chief Compliance Officer will work with all necessary departments and personnel to address any issue brought forward. The Compliance Hotline number is 1-800-428-1678.


ATl has a non-retaliation policy. This means no action of retaliation or reprisal will be taken against anyone for calling the Hotline to make a report, complaint or inquiry. However, calls to the Hotline do not protect callers from appropriate disciplinary action regarding their own performance or conduct.

[Report Your Concern via Email](#)

[Compliance Hotline
800-428-1678](#)

For general compliance questions, please submit your questions through the Compliance Questions form below:

[Submit your Compliance Questions!](#)

the  **ATl** way

Lynn S McGivern, LLM, JD

Lynn.McGivern@atipt.com

(630) 296-2222, ext. 7193

© ALL RIGHTS RESERVED
This presentation, nor any part, may be reproduced or utilized in any form or by any means, electronic or mechanical, including recording, or by any information storage and retrieval system, without permission in writing from ATl Physical Therapy Compliance.

the  **ATl** way

Discussion Questions

23

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?

24

Speaker Information

25

Speaker Contact 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

26