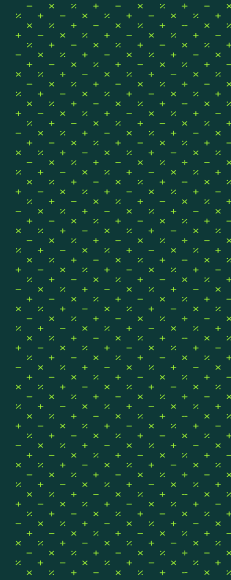




Risk Assessments and Enterprise Risk Management

Lori Laubach, CHC, Partner
May 17, 2019



1

Objectives

- Understand risk assessment strategies to identify the highest risks to achieving organization objectives
- Identify ways to mitigate risk in key areas through internal audits or reviews
- Utilize effective processes to monitor and assess internal control performance over time



2

What is risk assessment?

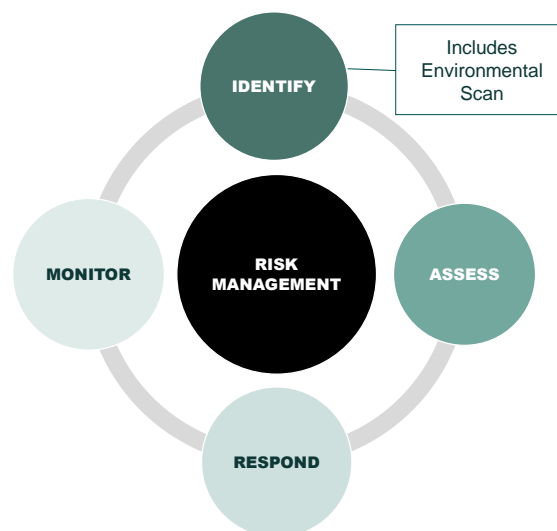
Risk: Anything that will hinder or prevent your organization from achieving its goals or purpose.

Risk Assessment: Evaluating, measuring, and prioritizing likely relevant events or risks that may materially hinder or prevent your organization from achieving its goals or purpose.

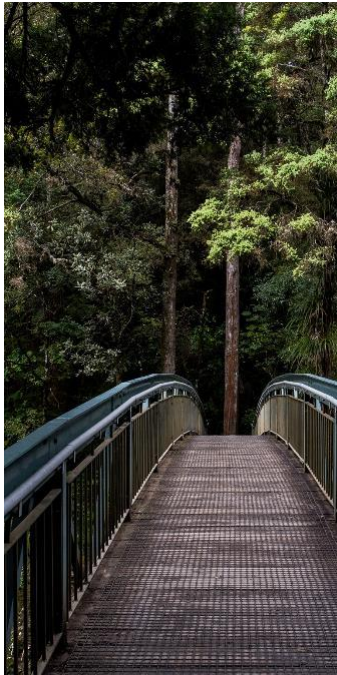


3

Managing risk is a continuous process



4



Why should you care?

- Office of Inspector General (OIG)
- US Sentencing Guidelines (2004)
- Office for Human Research Protections (OHRP)/Food and Drug Administration (FDA)/Office of Research Integrity (ORI)
- Centers for Medicare and Medicaid Services
- Health Insurance Portability and Accountability Act (HIPAA)
- Stark/Anti-Kickback
- Organization/Board Responsibilities



5

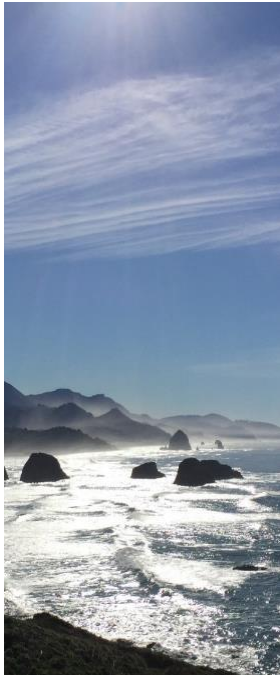


In Guidance

- American Health Lawyers Association and OIG compliance guidance for Boards
 - Does the compliance program address the significant risks of the organization?
 - How were those risks determined, and how are new compliance risks identified and incorporated into the program?
 - How is the Board kept apprised of significant regulatory and industry developments affecting the organization's risk?
 - How is the compliance program structured to address such risks?



6



Why conduct a risk assessment?

- Proactive versus reactive
- Supports enterprise risk management
- Cultural integration
- Raises awareness of program value
- Mitigation of penalties
- Continuous program improvement
- Basis for annual work plan
- Identifies needed resources
- OIG requires for organizations under a CIA



7



Risks-Compliance versus Internal Audit

Compliance

Threat from violations of laws, regulations, code of conduct or standards of practice

Internal Audit

Same but also consider financial statement risks and other operational risks



8



Enterprise Risk Management-Framework-2017

- Governance & Culture
- Strategy & Objective-Setting
- Performance
- Review & Revision
- Information, Communication & Reporting



- <https://www.ciso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>



9



What is ERM?

- Is not a function or department
- Is more than a risk listing
- Addresses more than internal control
- Is not a checklist
- Can be used by organizations of any size



10











American Society for Healthcare Risk Management (ASHRM) ERM Framework

- Enterprise risk management in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connections to total value



11

American Society for Healthcare Risk Management (ASHRM) - ERM Domains

Domain	Description/Example
Operational	 The business of healthcare is the delivery of care that is safe, timely, effective, efficient, and patient centered within diverse populations. Operational risks relate to those risks resulting from inadequate or failed internal processes, people, or systems that affect business operations.
Clinical/ Patient Safety	 Risks associated with the delivery of care to residents, patients and other healthcare customers. Clinical risks include: failure to follow evidence based practice, medication errors, hospital acquired conditions (HAC), serious safety events (SSE), and others.
Strategic	 Risks associated with the focus and direction of the organization. Because the rapid pace of change can create unpredictability, risks included within the strategic domain are associated with brand, reputation, competition, failure to adapt to changing times, health reform or customer priorities.
Financial	 Decisions that affect the financial sustainability of the organization, access to capital or external financial ratings through business relationships or the timing and recognition of revenue and expenses make up this domain. Risks might include: costs associated with malpractice, litigation, and insurance, capital structure, credit and interest rate fluctuations, growth in programs and facilities, capital equipment.
Human Capital	 This domain refers to the organization's workforce. This is an important issue in today's tight labor and economic markets. Included are risks associated with employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity and compensation. Human capital associated risks may cover recruitment, retention, and termination of members of the medical and allied health staff.
Legal/ Regulatory	 Risk within this domain incorporates the failure to identify, manage and monitor legal, regulatory, and statutory mandates on a local, state and federal level. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, Centers for Medicare and Medicaid Services (CMS) Conditions of Participation (CoPs) and Conditions for Coverage (CfC), as well as issues related to intellectual property.
Technology	 This domain covers machines, hardware, equipment, devices and tools, but can also include techniques, systems and methods of organization. Healthcare has seen an explosion in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Risk Management Information Systems (RMIS), Electronic Health Records (EHR) and Meaningful Use, social networking and cyber liability.
Hazard	 This ERM domain covers assets and their value. Traditionally, insurable hazard risk has related to natural exposure and business interruption. Specific risks can also include risk related to: facility management, plant age, parking (lighting, location, and security), valuables, construction/ renovation, earthquakes, windstorms, tornadoes, floods, fires.

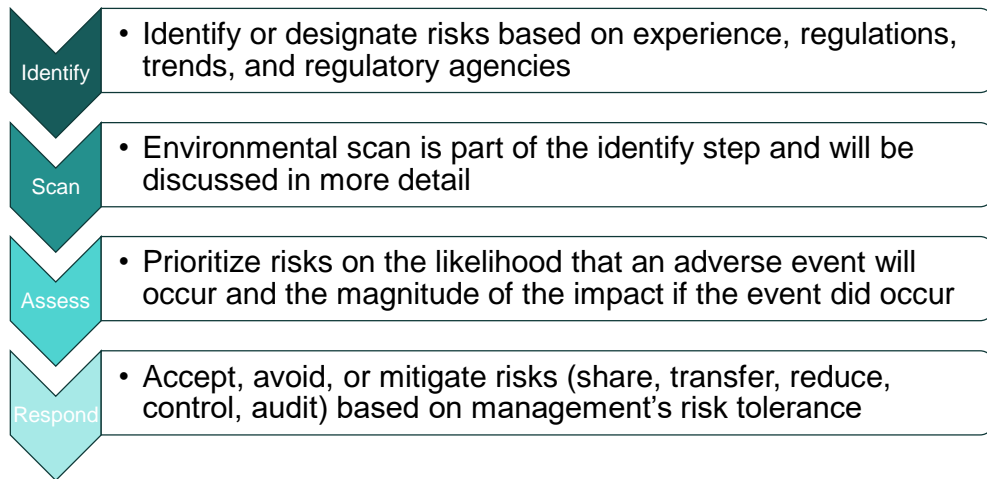


12

- <http://www.ashrm.org/resources/ERM-Resources.dhtml#Resources>

12

Risk management key components



13



What is a risk?



- Exposures now and in the next 3-5 years
- Key process or functions which lack mitigation or could have impact on operations
- Complex studies, processes, or functions with multiple stakeholders, hand-offs, control, and authority
- Key strategic initiatives, mergers, etc



14

How to identify compliance risks

Identify

- Start with your organization's strategies and key initiatives
- Consider regulations – what has changed
- Updated or deleted policies, and procedures
- Innovation
- Evaluate the OIG work plan, audits, and enforcement activity
- Consult requirements of other federal and state agencies OCR, OHRP, FDA, OSHA, OSHPD



15

How to identify compliance risks (cont.)

Identify

- Review auditing and monitoring results, prior risk assessments, and reports
- Evaluate how data mining, predictive analytics, and cross-jurisdictional intelligence might impact you
- Survey employees, key stakeholders, vendors
- Conduct individual interviews
- Convene focus groups and brainstorming sessions
- Convene content groups



16



Other Sources of Risks

Identify

- The OIG Work Plan is just a starting point – search for your specialty in other federal reports and keep current in your reading
<http://oig.hhs.gov/newsroom/whats-new/>
- Search your Contractor website and newsletters for updates and changes in your contractor policy



17

Environmental scanning-What?

Scan



- Systematic process of collecting and analyzing information about an organization's internal and external environments for planning, forecasting, or choosing a preferred future
- Being integrated into leading edge risk management programs



18

Environmental scanning: Objectives

Scan



- Detecting important economic, social, cultural, environmental, technological, and political trends, situations, and events
- Identifying potential opportunities and threats implied by trends, situations, and events
- Gaining an accurate understanding of the strengths and limitations of your organization
- Identifying and assessing risks as part of your risk management program



19

Environmental scanning: Stakeholders

Scan



- Internal
 - Involve cross-functional stakeholders and subject matter experts across the organization
- External
 - Vendors, community physicians, legal and risk management advisers, external financial auditors



20

Environmental scanning: Techniques


 Scan

- Review the literature broadly
- Consult your colleagues
- Benchmark with peers
- Survey employees, key stakeholders, vendors
- Conduct individual interviews
- Convene focus groups and brainstorming sessions
- Use delphi-type conferences and polling techniques



21

Sample evolving risks


 Scan

- Ability to control genetics of humans, animals, and plants
- Bionic people
- Connectivity across the continuum of care
- Convergence of 3D digital design, medical imaging, and 3D printing
- Convergence of nanotechnology, biotechnology, information technology, and cognitive science
- Open health care information versus privacy
- Patient choice, patient power
- Rise in telemedicine
- Wearable devices



22

Assess and prioritize identified compliance risks



- Evaluate risks on the likelihood that an adverse event will occur
- Evaluate on the impact (or consequence) event would have on entity
- Rank risks – based on likelihood and impact

ILLUSTRATIVE LIKELIHOOD SCALE		
Rating	Descriptor	Definition
3	Frequent	▪ > 50% chance of occurrence
2	Possible	▪ > 10% up to 50% chance of occurrence
1	Unlikely	▪ < 10% chance of occurrence



23

Example of Likelihood and Impact



Likelihood				
Rare E	Unlikely D	Moderate C	Likely B	Almost Certain A
Highly Unlikely to occur	Given current practices and procedures, this risk unlikely to occur	Risk has occurred in past	Risk likely to occur	Risk is very likely to occur, possibly several times
OR				
5% chance of occurring	20% chance of occurring	50% chance of occurring	80% chance of occurring	95% chance of occurring
Impact (Consequence)				
Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Impact could be handled through normal activity	Adverse event which could be handled / resolved with some management effort	Serious event which requires significant management effort and involvement to resolve	Critical event which requires extraordinary management effort	Disaster with potential to lead to collapse



24

Example

Assess

Risk	Reputation	Financial	Legal	Risk Impact	Likelihood	Detectability	Vulnerability	Controls	Risk Prioritization Score (RPS)	Comments
				0			0		0	
				0			0		0	
				0			0		0	
				0			0		0	
				0			0		0	

Risk Area Identified	Likelihood of Adverse Event	Magnitude of Adverse Event	Inherent Risk Score	Internal Controls Mitigation	Residual Risk	Comments



25

Example Matrix

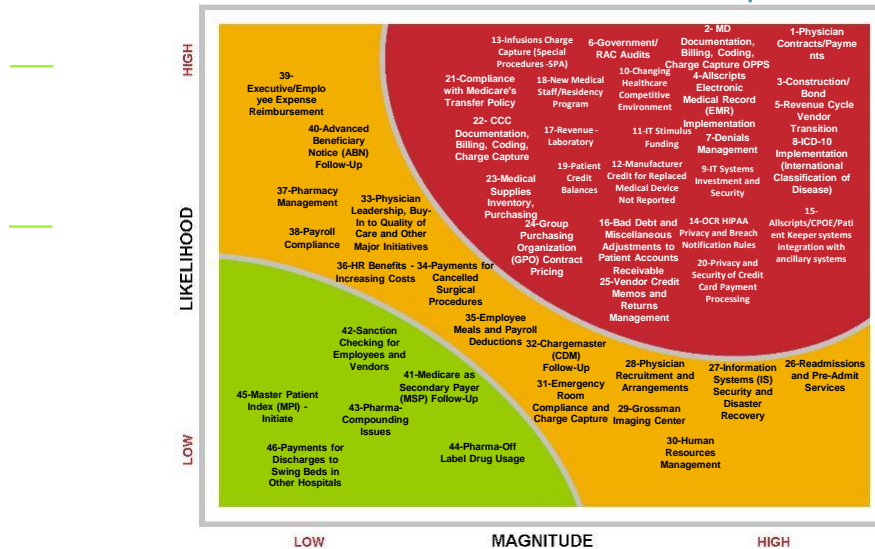
Assess

			Impact (Consequence)				
			Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood of Occurrence	A	Almost Certain	High	High	Extreme	Extreme	Extreme
	B	Likely	Moderate	High	High	Extreme	Extreme
	C	Moderate	Low	Moderate	High	Extreme	Extreme
	D	Unlikely	Low	Low	Moderate	High	Extreme
	E	Rare	Low	Low	Moderate	High	High



26

Risk Assessment Heat Map



29

Risk Response Work Plan



- Once risks have been identified and prioritized it is important to take action and address risks
 - Transfer
 - Avoid
 - Reduce
 - Accept
 - Monitor
 - Audit
- Identifying and prioritizing risks can create risk if nothing is done with the information



30

What about the audit plan?

Establish a plan on what to

- Audit,
- Monitor,
- Data Mine
- Strategize



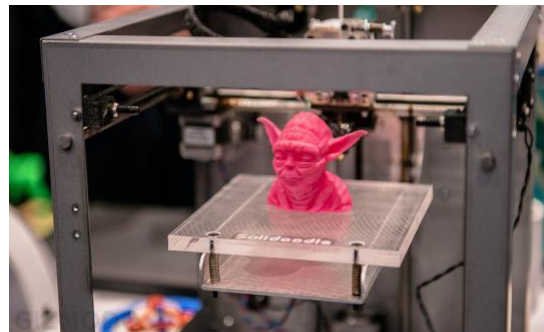
31

31

Part 3 – Reducing risk profile

Case #1 – Convergence of 3D digital design, medical imaging, and 3D printing

- What compliance risks are introduced?
- What mitigation strategies should compliance be using?
- Can you suggest any best practices?



32

Part 3 – Reducing risk profile

Case #2 – Rise in Telemedicine

- What compliance risks are introduced?
- What mitigation strategies should compliance be using?
- Can you suggest any best practices?



33



Wrap up

- We went through the key steps in a robust risk management process
- Discussed ERM and how it applies to Health Care
- We defined and explained how environmental scanning can improve how you identify and address risks
- And together we shared our knowledge and experiences regarding a few emerging or evolving risk area



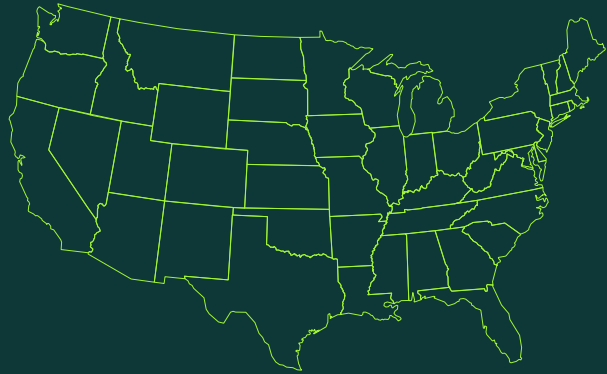
34

QUESTIONS?

Lori Laubach, CHC
Partner

Lori.Laubach@mossadams.com

(253) 284-5256



35

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.

THANK YOU



36 [to edit Footer; go "Insert" (tab) > "Header & Footer"]

36