1

"A reputation once broken may possibly be repaired, but the world will always keep their eyes on the spot where the crack was."

- Joseph Hall (1574-1656)

2

2

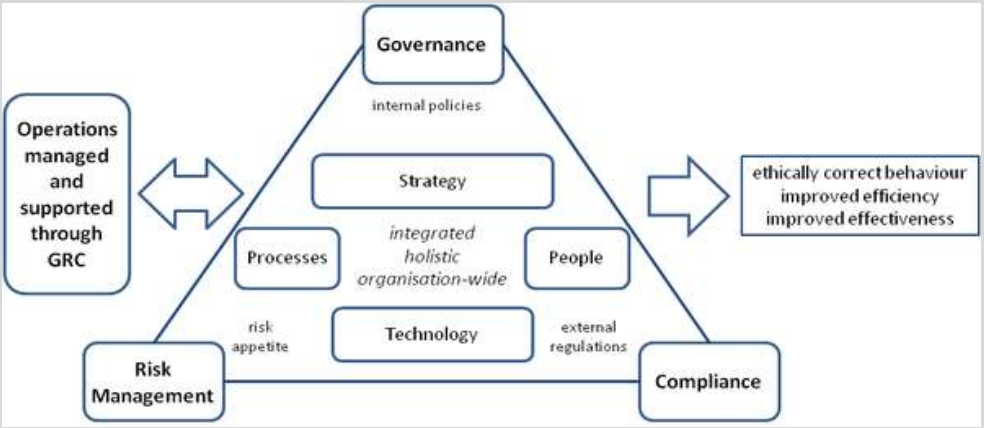
- Integrating core concepts across risk domains, compliance processes, and engaging RM into the audit/ investigation workflow.
- The hazards of not preparing for potential issues can have significant, long-term effects. Neglecting to have a comprehensive risk management plan in place can compromise patient care, increase liability risks, and result in financial losses.
- Case study - following through the investigation of internal controls in evolving organization, review of potential mitigation steps and associated outcomes.

3

What is GRC?

4

GRC Framework



Creative Commons

- Chart created by CreativeCommons.org

5

What is Risk & Where it Resides?

6

Nature of Risks

Risk is…

R – Relative as perception of downside and upside risk is individual; risk applies to people and organizations

I – Intuitive because we learn with experience and time

S – Significant because everything we do has positive and negative consequences

K – Kinetic because it changes relative to situations, events, time, and space

- Risk is universal
- Risk is not properly identified and managed by most organizations, including governments
- Need a common risk vocabulary
- Need improved risk management methodologies
- Risks are diverse & inherent to the business operations
- If non-clinical risks are not managed they are just as hazardous as clinical risks

7

7

Risk Tolerance

- Risk tolerance question is difficult.
- Risk is not always clear.
- Does organization puts greater onus on criminal rather than civil risk?
- Does organization consider 'enforcement' probability?
- How does organization factor in reputation exposure?
- Risk to different parties may be unequal.
- Does organization fully understand the risks it is facing before accepting the risk?

8

8

Risk Domain

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, managemer 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.

https://www.ashrm.org/system/files/media/file/2020/12/ERM-Implementing-ERM-for-Sucecess-White-Paper_FINAL.pdf

9

Common Healthcare Internal Risks

- Policies & Procedures
  - Documentation of internal control structure
- Contracting
  - Vendor relationships
  - Physician relationships
- Financial Reporting
- Financial statements
  - Tax returns
  - Cost reports
  - 990 Reports
  - Credit risk
  - Liquidity Risk
- Crisis management program
  - Business continuity plan
- Human resource management
  - Hiring & terminations
  - Employee relations
- Governance
  - CEO succession planning
  - Director succession planning
- Clinical practices
  - Quality
  - Core measures
  - Evidence based
- Information technology
  - Security
  - Disruptions
- Document management

10

10

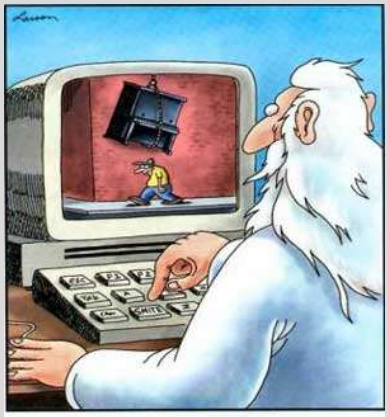
Common Healthcare External Risks

- HHS Officer of the Inspector General
- CMS
- State Health Department
- Licensing agencies
- OSHA
- EPA
- Investors
- Litigators
- Past Employees
- HIPAA/HITECH
- IRS
- Auditors
- Competition
- Integrity Program Contractors

11

11

Unknown Risks



God at His computer

12

12

Controls

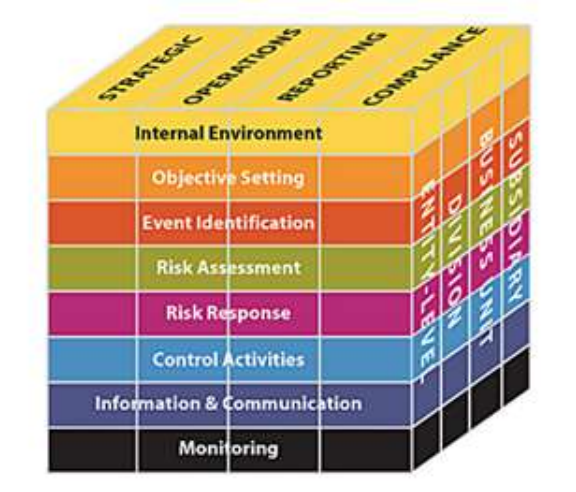
13

Internal Controls

- COSO - The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of the five private sector organizations dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.
- Enterprise risk management 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.
- Internal controls is a process, effected by an entity's board of directors, management, and other personnel, designated to provide reasonable assurance regarding the achievement of objectives in the following categories
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations

14

14



15

15

Control Elements

Control environment – the tone of a company and its audit committee, which influences the control consciousness of its personnel

Risk assessment – from a financial reporting perspective, a company's assessment of its identification, analysis, and management or risks relevant to the preparation of financial statements

Control activities – the policies and procedures to ensure that the company's directives are carried out

Information and communication – the company's information systems, which includes the accounting systems

Monitoring – a process to assess whether controls are operating as intended and whether they are modified as appropriate for changes in conditions

16

16

Types of Control

- Preventive Controls
  - Designated to prevent errors or irregularities before they have occurred
  - E.g.:
    - Regular balancing and reconciliation are completed by an individual independent of the transactions process through the accounts
    - Passwords and physician safeguards are established to restrict access to appropriate personnel
    - Authorization and limits are set to ensure the appropriate oversight of significant transaction
- Detective Controls
  - Designed to detect errors or irregularities after they have occurred
  - E.g.:
    - Exception reports are reviewed and cleared by persons with appropriate authority
    - Systems maintenance reports are reviewed to ensure changes are completed properly and authorized
    - Documentation reviews are completed to ensure files are complete

17

17

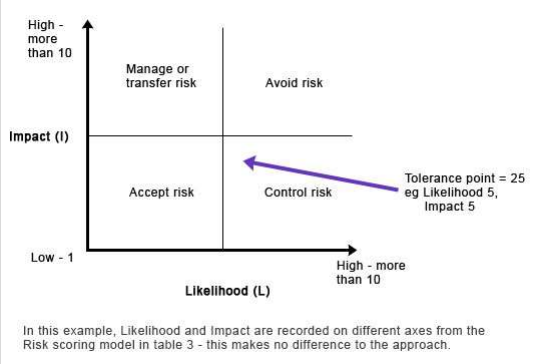
Types of Control

- Business controls
  - Can be preventive or detective
  - Executed by people
  - E.G – Review and approve expense report
- Application Controls
  - Input: Developed logic to prevent key errors in a system
  - Process: controls that ensure that the operation methods are correct
  - Output: controls that detect errors in processing of data

18

18

Risk Continuum & Internal Controls



In this example, Likelihood and Impact are recorded on different axes from the Risk scoring model in table 3 - this makes no difference to the approach.

19

19

Risk Assessments

- Process of identifying, analyzing and managing risks relevant to objectives
- Consideration of the risk's significance, likelihood of occurrence, and how they should be managed
- Management may initiate plans, programs, or actions to address risks or accept the risk due to cost or other considerations
- Elements to consider:
  - Changes in operating environment
  - New personnel
  - New or revamped information systems
  - Rapid growth
  - New technology
  - New lines, products, or activities
  - Corporate restructuring
  - Accounting pronouncements

20

20

Risk Rating Matirx

Impact	Likelihood				
	Rare	Unlikely	Possible	Likely	Almost certain
Catastrophic	moderate	moderate	high	critical	critical
Major	low	moderate	moderate	high	critical
Moderate	low	moderate	moderate	moderate	high
Minor	very low	low	moderate	moderate	moderate
Insignificant	very low	very low	low	low	moderate

21

21

Controls: Internal Audit vs. Compliance

- Internal Audit Work Plan Elements
  - Operational
  - Financial
  - Human Capital
  - Strategic
  - Legal/ regulatory
  - Information technology
- Compliance Work Plan Elements
  - Education
  - Monitoring
  - Investigative/ hotline reports
  - Policies & procedures
  - Response

22

22

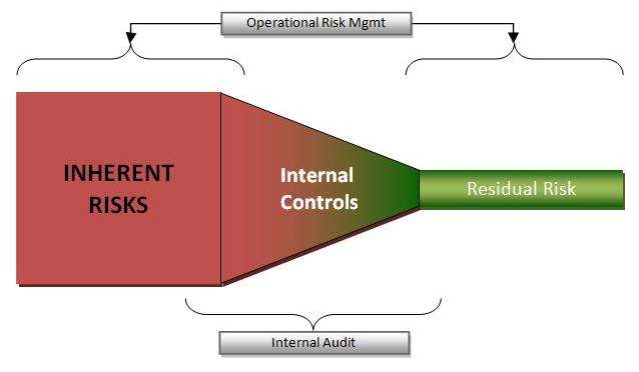
Managing risk is a continuous process…

23

Risk Transfer & Residual Risk

24

Risks Mitigation



25

25

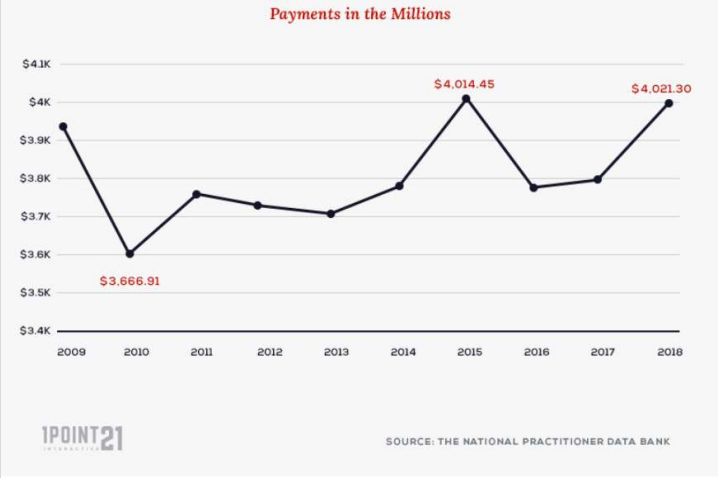
Historical perspective

- Medical responsibility first outlined in 2030 BC in Code of Hammurabi
  - "If the doctor has treated a gentlemen with a lancet of bronze and has caused the gentleman to die, or has opened an abscess of the eye for a gentleman with a bronze lancet, and has caused the loss of the gentleman's eye, one shall cut off his hands"
- Under Roman law, medical malpractice was a recognized wrong
- Richard Caeur De Lion developed English common law of early 12th century and established well documented precedents related to "unwholesome medicine"
- In 1532, during the reign of Charles V, the law required the
  - Opinion of medical men in cases of violent death, and
  - Expert testimony in cases of medical negligence
  - Establishing the "standard of care"
- In US, early cases date back to early 1800

26

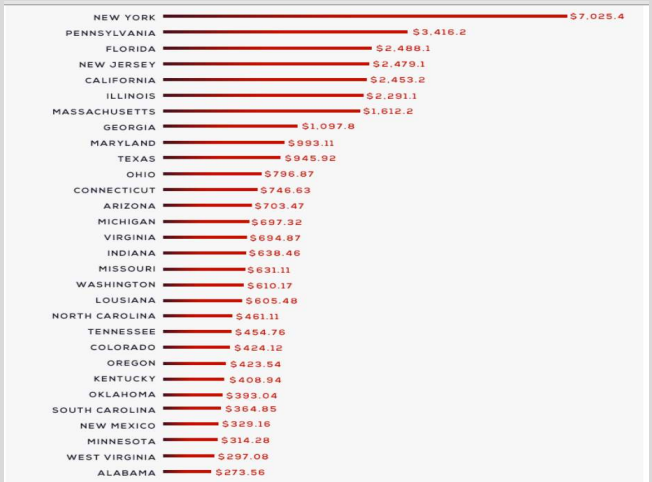
26

US Medical Malpractice Payment by Year



27

Total Medical Malpractice Payments by State, 2009-2018

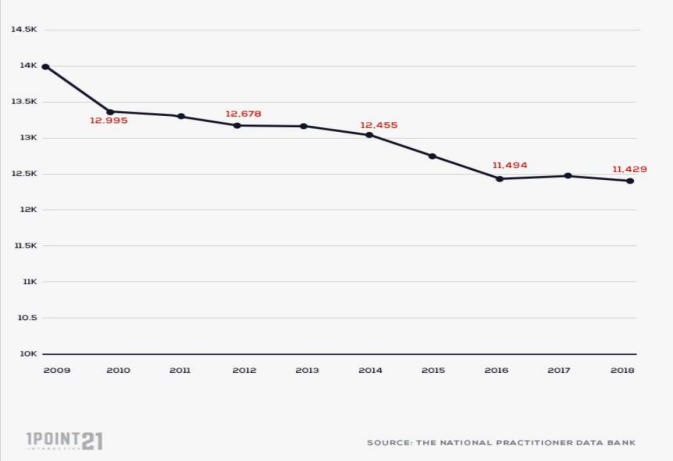


*In Millions

* Source - NPDB

28

US Medical Malpractice Reports by Year, 2009-2018



29

Estimates of National Costs of Medical Liability System

Component	Estimated cost (billions of 2008 dollars)	Quality of evidence supporting cost estimate
Indemnity payments	$5.72	Good as to the total; moderate as to the precision of the split among the components
Economic damages	$3.15	
Noneconomic damages	$2.40	
Punitive damages	$0.17	
Administrative expenses	$4.13[a]	Moderate
Plaintiff legal expenses	$2.00[a]	Good
Defendant legal expenses	$1.09	Moderate
Other overhead expenses	$3.04	Good
Defensive medicine costs	$45.59	Low
Hospital services	$38.79	
Physician/clinical services	$6.80	
Other costs		
Lost clinician work time	$0.20	Moderate
Price effects	–[b]	Low
Reputational/emotional harm	–[b]	No evidence
Total	$55.64	

SOURCE Authors' analysis. [a]Although plaintiff legal expenses are separately itemized, they are not included in the overall administrative costs total because, in the contingent fee system, they are already represented in the indemnity costs. [b]These costs are not estimable with the available data.

"National Costs of the Medical Liability System," Health Affairs 29, no 9 (2010): 1569-1577

30

30

ERM & Ensuring Continuity

31

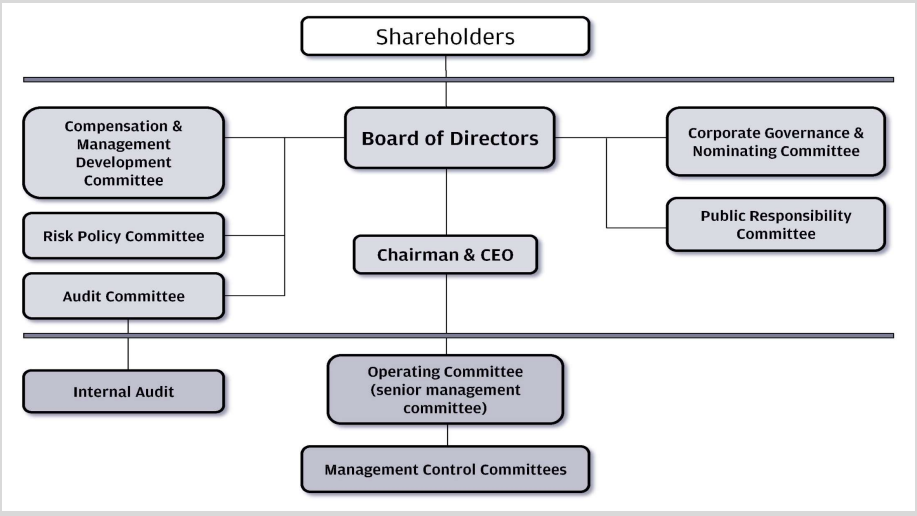
ERM Framework

32

ERM On the ground….

33

Corporate Governance Structure



34

34

Board Committees

- To perform these tasks, the most commonly created board committees are, according to the most recent survey by the American Hospital Association's Center for Healthcare Governance:
  - Finance (83%)
  - Quality (75%)
  - Executive (68%)
  - Governance and nominating (60%)
  - Audit and compliance (51%)
  - Strategic planning (44%)
  - Executive compensation (36%)
  - Physician relations (35%)
  - Fund-raising/Development (18%)
  - Community benefit/Mission (14%)
  - Government relations (4%)

35

Stakeholders & Communications

Clear and **continuous** lines of communication between stakeholders is critical to *effective* and *efficient* risk management.

36

Ideally...

37

37

A few afterthoughts

- GRC should not strangle the life out of an organization or undermine its strategic goals
- Risk assessment and internal controls are tools to support organizational mission, vision, and values
- Internal controls should be balanced to the risk addressed
- Internal controls are often better at keeping honest people honest then they are at preventing criminals
- No organization can controls all the risks

38

38

Case Study

- Dr. Campanella has been part of Ophthalmology Faculty for a few years coming after a brief tenure at another AMC. He has a significant volume of Cataract & Glaucoma surgeries and relied heavily on the residents and fellows, who absolutely adore him as he often uses some as 'assisting' during surgeries. During standing small sample compliance audits, his documentation compliance rate is within the faculty profile of about 95%.
- The RevCycle manager responsible for faculty billing brings to your attention that on his clinic days, Dr. Campanella has been increasingly seeing between 80 and 120 patients which is almost twice higher then other glaucoma specialists, but the Department has been overlooking the trend since he was brining the 'dough.'
- **Where would you start your investigation? What compliance and operational controls should you test? What governance functions are implicated?**
- ***Investigation Post Mortem:***
- *The Harvard Time study showed that Dr. Campanella could not have personally performed or overseen performance of all clinic services. EMR audit trail consistently showed entries under Dr. Campanella's name off hours and very few entries by assigned residents, which indicate violation of password policy, PATH issues, potential conflict with GME requirements for teaching institutions, and puts in doubt that all services were, in fact, billable.*
- *Interviews with residents and support stuff identify that completion of medical record has been done by staff, who would code , and submit encounters under physician's log ins. The requested audit by CISO, identify multiple concurrent EMR log-ins during Dr. Campanella's clinic. Upon request from CCO, CISO implements ongoing monitoring across the practice.*
- *Interviews with the Faculty and review of peer reviews, show wide knowledge of the non-compliance, which is consciously overlooked. Peer review was completed pro-formally.*
- *Faculty ends up self-reporting the issue to State Medicaid IG and OIG as part of self-disclosure and substantial refund. Dr. Campanella is allowed to resign, as the termination would be reported through NPDB.*
- *A few years later Faculty CCO receives a call from FBI – Dr. Campanella was implicated in similar behavior in another AMC.*

39