Risk Assessments & Internal Controls

Mark P. Ruppert, CPA, CIA, CISA, CHFP
Director, Internal Audit
Cedars-Sinai Medical Center, Los Angeles
Do we know what it is that we seek to assess and control?

WHAT IS RISK?
Dictionary.COM:

• Exposure to the chance of injury or loss;

• A hazard or dangerous chance: as in “It's not worth the risk.”
• But there is also upside risk.

• Definition: “a hazard or dangerous chance”

• There’s an upside risk, that is a “chance,” a chance that you’ll take a “risk” and it’ll turn out good.
So, then
What is Risk?
• Well, it’s not a thing, not...
  –a feeling,
  –a do or a don’t,
  –a will or a won’t,
  –a have or have not...
  –But then, it is
• It’s all those things. Isn’t it?!
• RISK just IS.
RISK
Relative
Intuitive
Significant
Kinetic
• **R** = Relative – Risk is relative because perception of downside and upside risk is individual, and that applies to people and organizations.

• **I** = Intuitive – Risk is intuitive because we learn with experience and time.

• **S** = Significant – It is significant because everything we do has positive and negative consequences.

• **K** = Kinetic – It is kinetic because it changes relative to situations, events, time, space.
RISK IS LIFE!

We can’t live without taking risk.

If we don’t take risks, we can not live!
Goals of This Session

• Create a Balanced View of Risk & Control
• Identify Concepts Audit Committees Need to Understand About Risk and Controls
• Address Questions You as audit Committee Members Should be Asking
A Balanced View of Risk & Control
• The founders of the organizations we serve…. knew this concept of risk and life.

They risked it all for the benefit of many.

• You likely know it well for the organizations you lead.

• And, our patients too understand this level of risk, not that they don't fear the risk of the procedure, but it's the very chance they choose instead!
We must remember that…

– We need leaders who understand risk and life.

– We need leaders who can stay focused on the vision without becoming caught up in the maze leading to that vision.

– If we lose the vision, then navigating the maze is pointless.

– Our organizations need to remain in a Risk Life mode to grow and evolve and prosper…to continue as a going concern and to “matter.”
So how does this impact risk discussions with the audit committee?

- We should **not** use the concepts of risk and control and governance to strangle the life out of the organization.

- Risk assessment and internal controls are tools:
  - We must use them wisely… in a manner to that supports the mission and vision of the organization.
  - Like the organizations served, these tools are as unique as they are similar.
Risk & Control Concepts
Familiarize Yourself with key Risk and Control Terms

• Enterprise Risk Management / Risk Management
• Risk Assessment
• Significance
• Probability
• High, Medium, Low
• Risk Appetite / Risk Boundaries
• Preventive and Detective Controls
• Custody, Authorization, Recordation, Evaluation, Duty Segregation
• Cost Benefit
Understand Your Entity’s Mission and Vision & Risks that Support and Challenge

• Key regulations like HIPAA
• What’s insured and what’s not
• Planned systems implementation
• New Buildings
• New businesses
• Key physician hires
• Key management changes
• Deviations from Mission & Vision
• Significant internal control breakdowns
Internal Control
COSO Definition

Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed 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 & regulations
Internal Control
COSO - Key Concepts

• Internal control is a **process**. It is a means to an end, not an end in itself.

• Internal control is **effected by people**. It’s not merely policy manuals and forms, but people at every level of an organization.

• Internal control can be expected to **provide only reasonable assurance**, not absolute assurance, to an entity’s management and board.

• Internal control is **geared to the achievement of objectives** in one or more separate but overlapping categories.
Internal Control
Other Considerations

• Internal Controls Should be Balanced to the Risk They Address

• Internal Controls are often better at keeping honest people honest than they are at preventing criminals from committing crimes.

• Don’t expect to control all risk and don’t risk it all on static control systems.
Questions to Ask

Audit Committee
Six Senses
First,

- A controlled and compliant but stagnant and lifeless organization is not a strong organization.
- Most risk assessments do not factor in things like management morale.

Audit Committees Should Consider:

- Is our executive management excited and passionate about their work?
- Do they believe in and fulfill their responsibilities in a manner that embraces mission and vision?
- For high risk initiatives, like a major system install, do we have someone with passion for leading the project and are they in the right position to be leading that project?
Second,

- Risk management and risk assessment are not an exact science: there is no one-size-fits-all approach.
  - They are unique to your organization. While common elements are shared in the industry, the processes are variable as the organization.
  - They are only one component of audit plan development.
  - They include many variables.
  - Scoring of individual risk factors and risk by several people will likely result in disagreement.
  - However, the results should feel right, especially in terms of how risk is viewed overall and what rises as significant versus not so significant.

- Audit Committee members shouldn’t get caught up in the details, they should consider…
• Does the risk management and assessment approach make sense for our organization?
• Are we satisfied with the results? Do we collectively believe that the things that seem to matter (up and downside risk) float to the top?
• Can we support management’s decisions on this new venture even understanding the downside risks? Does it support the mission and vision of the organization?
• What other factors are used in developing the annual audit plan and compliance work plan?
• How are the risk not included in those plans being addressed?
Third,

- The risk spectrum is broad. Are audit committees responsible for all risk?
- No. But the full compliment of the Board should collectively know the organization risk picture.
- The Audit Committee is not responsible for ERM.

Audit Committees Should Consider:
- Do we understand our organizations governance structure and process? Do we believe it to be effective?
- What are our responsibilities and how do we know that the Board is picking up the gaps?
- Do we know and understand our Charter?
- What risks does each Board Committee address?
Forth,
- Risk strategy, risk management and controls are a management imperative. Internal Audit and Corporate Compliance do not own risk and control.

Audit Committees should consider:
- Is management talking to the Committee about risk and controls, or is it only a topic understood by Internal Audit?
- What does management present to the Committee? And, what gets presented to the Board?
Fifth,

- For specific risk types like HIPAA, Audit Committees don’t have ample meeting time to walk through the detail of all 43 standards during limited meeting time.

Audit Committees Should Ask:

- Who is responsible for ensuring compliance?
- How do we know they are meeting the responsibility?
- What major gaps do we currently have to fill and what are our plans to do so?
- How concerned should we be about the gaps (in the short run / in the long run)?
Sixth,

- Auditors, Compliance Professionals, Management and Others Present various information to Audit Committees.

Audit Committees Should:

- Be involved in determining what should and shouldn’t be presented. What do we want/should we see and discuss?
- Understand the context of what is presented, preferably in advance of the meeting. How does this relate to the risks we need to understand and address?
- Focus on solution implementation. How and when will an issue be solved?
Questions

and Discussion