Enterprise Risk Assessment and Management

April 21, 2017

Presenters

- **Aimee Bertrand**, MBA, CHC, RHIA
  - Vice President of Compliance
  - Schumacher Clinic Partners

- **Eden Ezell**, JD, MBA, CHC
  - Vice President and Chief Compliance Officer
  - Ochsner Health System
  - eezell@ochsner.org

- **Joyce Hall**, JD
  - Watkins & Eager
What is Enterprise Risk Management?

- Enterprise Risk Management ("ERM") is an interdisciplinary process through which an organization identifies, analyzes, prioritizes, and addresses the risks and opportunities that can affect the achievement of its strategic objectives, whether in positive or negative ways.


**Focus Areas**

- Enterprise Risk Management and healthcare compliance – where do they intersect?

- Understanding the Compliance department’s existing role in enterprise Risk Assessment

- Uncovering your organization’s attitude towards enterprise risk

**Traditional**

- Risk = negative outcome
- Risk driven
- Silo approach

**Enterprise**

- Risk = any issue affecting the organization’s ability to meet its objectives
- Value driven
- Holistic approach
ERM vs. Compliance

- **Compliance** Risk = 1,000 foot view
  - Limited look at compliance risks
    - Typically fraud, waste, abuse, HIPAA, etc.

- **Enterprise** Risk = 50,000 foot view
  - Global look at risks across organization
    - What keeps you up at night?

- Not every risk area is a problem for your organization

ERM: The Compliance Connection

- **Sarbanes-Oxley Act**
  - Internal Control Implementation framework
    - Regular Risk Assessments

- **Collaborative Effort**
  - Compliance, Internal Audit, and Risk Management
Compliance Program Elements vs. COSO ERM framework

**Fundamental Elements of an Effective Compliance Program**

1. Written standards and policies
2. Compliance program oversight
3. Effective training and education
4. Communication
5. Enforcing standards through corrective action guidelines
6. Auditing and Monitoring
7. Response and Prevention
8. Non-Intimidation and Non-Retaliation

**COSO ERM Framework**

- **Internal Environment**
  - Objective Setting
  - Event Identification
- **Risk Assessment**
- **Risk Response**
- **Control Activities**
- **Information & Communication**
- **Monitors**

Risk Assessments: Compliance, ERM and IA

<table>
<thead>
<tr>
<th>Objective</th>
<th>ERM</th>
<th>Internal audit</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, prioritize, and assign accountability for managing strategic, operational, financial, and reputational risks</td>
<td></td>
<td>Determine and prioritize risks to aid in developing the internal audit plan, helping to provide the board and the executive team with assurances related to risk management efforts and other compliance activities</td>
<td>Identify, prioritize, and assign accountability for managing existing or potential threats related to legal or policy noncompliance—or ethical misconduct—that could lead to fines or penalties, reputational damage, or the inability to operate in key markets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope</th>
<th>ERM</th>
<th>Internal audit</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any risk significantly impacting the organization’s ability to achieve its strategic objectives</td>
<td></td>
<td>Financial statement and internal control risks, as well as some operational and compliance risks that are likely to materially impact the performance of the enterprise or financial statements</td>
<td>Laws and regulations with which the organization is required to comply in all jurisdictions where it conducts business, as well as critical organizational policies—whether or not those policies are based on legal requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typical owner</th>
<th>ERM</th>
<th>Internal audit</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Risk Officer/Chief Financial Officer</td>
<td></td>
<td>Chief Audit Executive</td>
<td>Chief Compliance Officer</td>
</tr>
</tbody>
</table>
### Risk Assessment

**Purpose of Risk Assessment**
- Identify Risks
- Assess Risks
- Manage & Monitor Risks

**Assess and Measure the Nature of Risks**
- Measure impact to organization
- Determine likelihood of occurrence
- Acknowledge existing mitigation efforts
- Identify gaps

---

### Key Risk Indicators

**Mapping risks to KRI. Defining Key Risk Indicators.**

- Enhance board and management risk awareness
- Improve the execution of an organization’s strategy
- Increase the effectiveness of the ERM process
### KRI Examples

<table>
<thead>
<tr>
<th>Business Risk Area</th>
<th>KRI Name</th>
<th>KRI Description</th>
<th>Source</th>
<th>Reporting Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Lack of Employee Standards of Conduct training</td>
<td>% completion of code of conduct training</td>
<td>OLN report</td>
<td>Annual</td>
</tr>
<tr>
<td>Compliance</td>
<td>Outdated hospital's standards, policies, and procedures</td>
<td>% completion of review of compliance policies</td>
<td>Policy Review Report</td>
<td>Bi-Annually</td>
</tr>
<tr>
<td>Compliance</td>
<td>Failure to establish and maintain procedures for the receipt, retention and treatment of complaints received by the hospital regarding compliance-related matters</td>
<td>Number of hotline calls per month</td>
<td>Issue tracking log</td>
<td>Monthly</td>
</tr>
</tbody>
</table>

### Internal and External Risk Domains

- Operational – quality, safety, outcomes, productivity
- Strategic – competition, resources, labor management
- Technological – infrastructure, security
- Financial – reporting, accounting, internal controls
- Regulatory – licensing, accreditation, investigations
- Reputational – public relations, community involvement
- Compliance/Ethical – fraud, waste, abuse
Scoring Risks

Impact
- Estimate of the severity of adverse effects
- Magnitude of a loss
- Potential opportunity cost should a risk be realized
- Risk that exists before you address it

Likelihood
- Adverse effects, loss or potential area may occur
- Likelihood that the risk will occur before you address it

Inherent Risk vs. Residual Risk

- Inherent risk is the level of risk with the absence of any controls in place to mitigate it.
- Residual risk is the modified risk after controls and their effectiveness have been applied for consideration.
Risk Heat Map

Impact

<table>
<thead>
<tr>
<th>Impact</th>
<th>1 Insignificant</th>
<th>2 Minor</th>
<th>3 Moderate</th>
<th>4 Major</th>
<th>5 Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>Med Low</td>
<td>Medium</td>
<td>Med Hi</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Likely</td>
<td>Low</td>
<td>Med Low</td>
<td>Medium</td>
<td>Med Hi</td>
<td>High</td>
</tr>
<tr>
<td>Moderate</td>
<td>Low</td>
<td>Med Low</td>
<td>Med Low</td>
<td>Medium</td>
<td>Med Hi</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Med Low</td>
<td>Med Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Med Low</td>
</tr>
</tbody>
</table>

Risk Exposure

Sample ERM Work Plan

<table>
<thead>
<tr>
<th>COSO ERM Elements</th>
<th>Related Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Internal Environment / Objectives Setting</td>
<td>Implement System ERM Committee &amp; Meeting Rhythm</td>
</tr>
<tr>
<td>2. Event Identification/Risk Assessment</td>
<td>Activate Hospital ERM framework at remaining facilities</td>
</tr>
<tr>
<td>3. Risk Response/Control Activities</td>
<td>Survey current ERM activities and communicate results to CEO &amp; Compliance Dyad at each facility as well as the Board</td>
</tr>
<tr>
<td>4. Information &amp; Communication</td>
<td>Develop ERM specific education and include ERM article summaries in the monthly Compliance Officer communication</td>
</tr>
<tr>
<td>5. Monitoring</td>
<td>Complete implementation of GRC monitoring tool for selected risks and controls at process, facility and system level</td>
</tr>
</tbody>
</table>
### Top Issues Confronting Hospitals in 2016

<table>
<thead>
<tr>
<th>Issue</th>
<th>2016</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial challenges</td>
<td>2.7</td>
<td>3.2</td>
<td>2.5</td>
</tr>
<tr>
<td>Governmental mandates</td>
<td>4.2</td>
<td>4.5</td>
<td>4.6</td>
</tr>
<tr>
<td>Patient safety and quality</td>
<td>4.6</td>
<td>4.2</td>
<td>4.7</td>
</tr>
<tr>
<td>Personnel shortages</td>
<td>4.8</td>
<td>5.1</td>
<td>7.4</td>
</tr>
<tr>
<td>Patient satisfaction</td>
<td>5.5</td>
<td>5.3</td>
<td>5.9</td>
</tr>
<tr>
<td>Access to care</td>
<td>5.8</td>
<td>6.2</td>
<td>---</td>
</tr>
<tr>
<td>Physician-hospital relations</td>
<td>5.9</td>
<td>5.7</td>
<td>5.9</td>
</tr>
<tr>
<td>Population health management</td>
<td>6.6</td>
<td>6.3</td>
<td>6.8</td>
</tr>
<tr>
<td>Technology</td>
<td>7.2</td>
<td>7.1</td>
<td>7.3</td>
</tr>
<tr>
<td>Reorganization (e.g., mergers, acquisitions, restructuring, partnerships)</td>
<td>7.8</td>
<td>7.4</td>
<td>---</td>
</tr>
</tbody>
</table>


### ERM Roles and Responsibilities (Illustrative)

[Diagram showing ERM roles and responsibilities]

Source: HCFAA, Enterprise Risk Assessment and Management Panel
E achieving the lines of defense begins to align.

- ERM is integrated with business planning and key processes.
  - Basic and evolving level capabilities are applied on a consistent basis.
  - Technology is leveraged to coordinated ERM activities and share risk information across the lines of defense.
  - Risk data is used to support decision making to improve performance.
  - Risk information is integrated into key business processes.
  - Metrics are defined, linked to risk appetite, and used to monitor risks.
  - Risks are monitored across the three lines of defense.
  - A governance structure and process is established.

**QUESTIONS??**