Enterprise Risk Management

Jonathan Brouk
AVP Strategic Planning
Children’s Hospital New Orleans

Eden Ezell
VP & Chief Compliance Officer
Ochsner Health System

C. Joyce Hall
Member
Watkins & Eager PLLC

Objectives

- Discuss the motivation for moving toward an ERM solution
- Outline the structure and composition of an ERM committee
- Provide an overview of Key Risk Indicator Development
Siloed Roles

Evolution of Healthcare Compliance Function

- **External Focus**
  - Regulatory Driven
  - Meet Regulatory Obligations

- **Internal Alignment**
  - Intrinsic Motivation
  - Values, Tone, and Risk Appetite
True Value of an Effective Compliance Program

The “true value” of an effective compliance program does not derive solely from program implementation and the program’s ability to protect from those risks identified by the organization; instead, “true value” is derived from the organization’s implementation of best practices, which attribute to improved organizational performance and patient care.

-Huron Consulting Group

Enterprise Risk Management

By collaborating to address overlapping issues and functions, leaders are more efficient in addressing shared interests and better able to focus on their distinct functions.
What is Enterprise Risk Management?

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.


**Traditional Risk Management**

Risk = negative outcome imposed by an external or third-party force

**Enterprise Risk Management**

Risk = any issue affecting the organization’s ability to meet its objectives

Enterprise Risk Management (ERM)
Enterprise Risk Management (ERM)

- Utilizes a process or framework for assessing, evaluating, and measuring all of an organization’s risks
- Any event that can adversely affect the objective/organization
  - Asset preservation
  - Failure to grow
  - Failure to execute on opportunities
- Consider designation of Chief Risk Officer
Areas of Risk

<table>
<thead>
<tr>
<th>Medicare Compliance</th>
<th>Internal Financial Controls</th>
<th>HIPAA Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>General Liability / Property &amp; Casualty</td>
<td>Human Resources</td>
</tr>
<tr>
<td>Safety &amp; Security</td>
<td>Regulatory</td>
<td>Healthcare Fraud &amp; Abuse</td>
</tr>
</tbody>
</table>

Leading Trends for Effective ERM

- Increased focus on risk “intelligence” and risk assessment
- Analytics and other predictive tools for early detection of – and response to – emerging risks
- More frequent and dynamic assessment of top risks
- Management-level and Board-level accountability for the ERM process and for each key risk
- Integration of risk management and strategy / major initiatives
- Improved discipline and better documentation
- Key Risk Indicators vs. Key Performance Measures
Poll Question:
Do you have an enterprise risk function?

1. Yes
2. No

ERM Committee

Responsibilities

- Provide education/in-services regarding changes in rules and regulations of relevant agencies
- Provide clarification and guidance on current regulations
- Assess processes to determine if facilities are in compliance with current regulations
- Standardize processes across organization, as appropriate
- Share methods, technology, and best practice
- Create toolkits for continued readiness
- Develop and monitor Key Risk Indicators
Agencies/Areas Monitored

<table>
<thead>
<tr>
<th>The Joint Commission (TJC)</th>
<th>Centers for Medicare and Medicaid Services (CMS) Conditions of Participation</th>
<th>Medicare Compliance (Billing/Coding)</th>
<th>Office of Inspector General (OIG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Health and Hospitals (DHH)</td>
<td>HIPAA / Privacy</td>
<td>Department of Insurance</td>
<td>Office of the National Coordinator (ONC) IT Security</td>
</tr>
</tbody>
</table>

ERM Committee

**Functions**

- Define the scope of the program
- Approve key policies & procedures
- Require periodic, substantive reporting by management
- Ask questions
- Oversight of external auditor, internal audit function, & compliance program
- Monitoring effectiveness of internal controls processes
- Approve and monitor Key Risk Indicators
ERM Committee

01 Compliance 02 Quality 03 Legal 04 Finance
05 Patient Safety 06 Human Resources 07 IT/Privacy 08 EVS

Key Performance Indicators (KPIs)

Key performance indicators (KPIs) are metrics used to measure key business processes that reflect strategic performance:

**Inpatient flow**
- Inpatient raw mortality rate
- Patient vs Staff Ratios
- Harm events per 1,000 patient days
- Readmission rate
- Occupancy rate
- Average length of stay
- Average cost per discharge

**Revenue cycle**
- Total operating margin
- A/R days due to coding
- Total A/R days outstanding
- Average cost per discharge
- Cash receipt to bad debt
- Claims denial rate
- Days of cash on hand
Key Risk Indicators (KRIs)

**Key Risk Indicators** (KRIs) are critical predictors of unfavorable events that can adversely impact organizations. They monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises, and mitigate them in time.

Relationship between KPIs and KRIs

- **KPIs**: Measure Historical Performance
- **KRIs**: Predict Future Risk
Developing Key Risk Indicators

Identify relevant metrics linked to organization’s objectives

Source: COSO Report: Developing Key Risk Indicators to Strengthen Enterprise Risk Management

Developing Key Risk Indicators

Analyze a risk event that has affected the organization in the past (or present) and then work backwards to pinpoint intermediate and root cause events

Source: COSO Report: Developing Key Risk Indicators to Strengthen Enterprise Risk Management
Core Elements of Well-Designed KRIs

- Allow for measurable comparisons across time and business units
- Consume resources efficiently
- Developed consistently across the organization
- Provide opportunities to assess the performance of risk owners on a timely basis
- Provide an unambiguous and intuitive view of the highlight risk
- Based on established practices or benchmarks

Key Risk Indicator Assignment

- Identify 2-3 Key Risk Indicators for your area:
  - Must be a predictor of risk
  - Can be simple
  - Must be measurable and reportable monthly
  - Data must be available (not a labor intensive process)
  - May be something that you are already monitoring
- Determine low, moderate, and high risk scores
- Identify responsible person
ERM Committee KRI

**Compliance**
- One Day Stays
- Medical Necessity
- Meaningful Use

**Quality**
- Surgical Site Infections
- CLABSI/CAUTI

**Legal**
- Dollar Amounts of Settlements
- Number of New Lawsuits
- Accrued Reserve Dollars for Settlements

**Finance**
- Internal Controls
- Executive Expenses
- Payroll Testing

**Patient Safety**
- Barcode Scanning Rates
- Hand Hygiene
- Universal Protocol
- Opioid Prescription Reduction

**Environmental**
- Generator Checks
- Emergency Preparedness

**Human Resources**
- Drug Diversion
- Employee Incidents
- Turnover % in Key Position

**IT/Privacy**
- Virus Email Received
- Inactive Users Disabled
- Firewall Penetration Attempts

---

**KRI Examples**

<table>
<thead>
<tr>
<th>Business Risk Area</th>
<th>KRI Name</th>
<th>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 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 organization regarding compliance-related matters</td>
<td>Number of hotline calls per month</td>
<td>Issue tracking Log</td>
<td>Monthly</td>
</tr>
</tbody>
</table>
Reporting Key Risk Indicators

**Key Risk Indicators Dashboard**

<table>
<thead>
<tr>
<th>Category</th>
<th>1 Day Stays</th>
<th>Patient Status</th>
<th>Transfer Request Accepted</th>
<th>Transfer Requests Declined</th>
<th>Transfer Requests Out</th>
<th>Transfer Requests Refused</th>
<th>BID Rule Compliance</th>
<th>4/11/2018</th>
<th>2/11/2018</th>
<th>2/11/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Compliance</td>
<td>12.5%</td>
<td>77.0%</td>
<td>173</td>
<td>201</td>
<td>369</td>
<td>28</td>
<td>99.1%</td>
<td>8/160</td>
<td>7/44</td>
<td>0.31</td>
</tr>
<tr>
<td>EMR/LA</td>
<td>102</td>
<td>109</td>
<td>71</td>
<td>172</td>
<td>205</td>
<td>17</td>
<td>99.1%</td>
<td>8/160</td>
<td>7/44</td>
<td>0.31</td>
</tr>
<tr>
<td>Device Utilization</td>
<td>64</td>
<td>37</td>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>41</td>
<td>24</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td>Virus Emails Received</td>
<td>2,386</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Users Disabled</td>
<td>177</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forward/Permutation Attempts</td>
<td>30,703,672</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of Website Blocked</td>
<td>2,582,718</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incoming Emails Blocked</td>
<td>289,460</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Risk Tolerance Key**

<table>
<thead>
<tr>
<th>Metric</th>
<th>1 Day Stays</th>
<th>Patient Status</th>
<th>Transfer Request Accepted</th>
<th>Transfer Requests Declined</th>
<th>Transfer Requests Out</th>
<th>Transfer Requests Refused</th>
<th>BID Rule Compliance</th>
<th>4/11/2018</th>
<th>2/11/2018</th>
<th>2/11/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure Compliance</td>
<td>Low: &lt;9%</td>
<td>Moderate: 6-15%</td>
<td>High: &gt;15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Status</td>
<td>Low: &lt;8%</td>
<td>Moderate: 8-15%</td>
<td>High: &gt;15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BID Rule Compliance</td>
<td>Low: &lt;8%</td>
<td>Moderate: 8-15%</td>
<td>High: &gt;15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Operational Managers**

All KRI s within their scope need real-time reporting.

**Senior Management**

KRI s for risks and opportunities with significant potential impact to the organization, less frequent (e.g. monthly).

**Board of Directors**

Only most significant KRI data to be confident that risk management is functioning as designed and approved, aggregated data for strategic evaluation.
Thank you!