Effectively Managing Risk: The Intersection of Compliance, Enterprise Risk Management and Internal Audit

Donald A. Sinko
Chief Integrity Officer

Vicki R. Bokar
Sr. Director Corporate Compliance
Cleveland Clinic

April 9, 2019

Three Different Risk Assessments

• Enterprise Risk Management (ERM) process
• Compliance Program risk assessment
• Internal Audit plan risk assessment
Internal Audit and Compliance

- The risk assessments for Internal Audit and Corporate Compliance are:
  - Narrower in scope
  - Specific to their charters
  - Focused on policies, procedures, regulations and internal controls
  - Are we doing the right thing

Enterprise Risk Management

- A “big picture,” holistic approach to organizational risk
- A framework for making risk management decisions
- Driven by the Board & Senior Management
- A continuous process that ties risks to the organization’s strategy, mission and values
Levels & Depth of Risk Assessment

• Enterprise risks are identified, prioritized and linked to strategic plan initiatives
• Summarize risk/control profile by individual risk, business function, risk category; utilize risk information for decision making
• Execute risk assessment / risk mandate & identify emerging risks and monitor controls

ERM Governance at Cleveland Clinic
So Where Does Compliance & Internal Audit Fit?

Risk ID & Assessment → Risk Analysis

Risk Analysis → Mitigation & Response

Mitigation & Response → Response to Detected Deficiencies

Response to Detected Deficiencies → Monitoring & Auditing

Risk ID & Assessment

Top ERM Risks

Updated April 2018
Methodology and Ratings

Mitigation Ratings

<table>
<thead>
<tr>
<th>Thresholds: Risk Response</th>
<th>Mitigation Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective</td>
<td>⚫</td>
</tr>
<tr>
<td>Requires minor/moderate improvements</td>
<td>○</td>
</tr>
<tr>
<td>Requires major/critical improvements</td>
<td>⚫</td>
</tr>
</tbody>
</table>

Risk Ratings

<table>
<thead>
<tr>
<th>Thresholds: Overall Score</th>
<th>Risk Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-4</td>
<td>⚫</td>
</tr>
<tr>
<td>5-12</td>
<td>○</td>
</tr>
<tr>
<td>&gt;13</td>
<td>⚫</td>
</tr>
</tbody>
</table>

Risk Assessment

<table>
<thead>
<tr>
<th>Sub-Risk Components</th>
<th>Response Effectiveness</th>
<th>Current Risk Response Mitigation Activities</th>
<th>Components Mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Executive Sponsor - Risk Owner - Strategic Initiatives:

Potential Impacts - Risk Indicators:
So Where Does Compliance & Internal Audit Fit?

ERM, Compliance & Internal Audit

• Allows for validation of identified risks and potential gaps
  - Compare identified risks against previous audit findings, detected deficiencies, compliance work plans
• Compliance and audit work plans can inform the ERM process
  - Focus of limited resources
  - More effective mitigation of identified risks
### High-Priority Risk:

<table>
<thead>
<tr>
<th>Sub-Risk Area</th>
<th>Current Risk Rating</th>
<th>Previous Risk Rating</th>
<th>Mitigating Activities</th>
<th>Current Mitigation Rating</th>
<th>Previous Mitigation Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td></td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>●</td>
<td></td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>●</td>
<td></td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>●</td>
<td>●</td>
<td></td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

### Monitoring & Auditing

- Mitigation already being done, but is it really?
- Trust is not an internal control!
- Compliance & Audit adds value to ERM by ensuring that risk management activities are really happening and are truly effective
- Provides comfort to the Board and Management