Why Risk Assessment?

Assure that you are appropriately using/assigning compliance program resources

Assure that you are focused on and addressing the right risk areas

Help your leadership team define/understand the strategy for your compliance program

Does This Represent Risks You Manage?
What Risks Does Your Program Manage?
What would your leadership team say?

What are the characteristics of risks they want you to help them avoid?

Do you really have compliance program resources to manage every conceivable regulatory requirement?

What Risks Do You Manage?

- Stark & AKS
- Privacy & Security
- Revenue Cycle; Billing & Coding

Why Risk Assessment?

“(c) In implementing a compliance program, the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each [compliance program element] to reduce the risk of criminal conduct identified through this process.”

USSG §8B2.1.(c)
Why Risk Assessment?

“. . . the OIG strongly encourages [providers] to identify and focus their compliance efforts on those areas of potential concern or risk that are most relevant to their individual organizations.”


Why Risk Assessment? New CIA Requirements

“Within 120 days after the Effective Date, [Organization] shall develop and implement a centralized annual risk assessment and internal review process to identify and address risks associated with the submission of claims for items and services furnished to Medicare and Medicaid program beneficiaries. The risk assessment and internal review process shall include:

(1) a process for identifying and prioritizing potential risks;
(2) developing an assessment plan to evaluate and respond to potential risks, including internal auditing and monitoring of the potential risk areas;
(3) developing action plans to remediate potential risks; and
(4) tracking results to assess the effectiveness of the risk assessment and internal review process, including any remediation efforts that [Organization] pursues.”

New risk assessment requirement from recent (2016) corporate integrity agreement.

How Does Compliance Risk Assessment Fit In?

<table>
<thead>
<tr>
<th>ERM</th>
<th>Internal Audit</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective &amp; Focus</td>
<td>Strategic Risks</td>
<td>Financial Statement Integrity &amp; Internal Controls</td>
</tr>
<tr>
<td>Typical Owner</td>
<td>Chief Risk Officer/Chief Financial Officer</td>
<td>Chief Audit Executive</td>
</tr>
</tbody>
</table>
Typical Risk Assessment Process

• Identification of compliance risks
• Evaluation of identified risks
  • Risk Impact: (Financial, Reputational, Legal)
  • Vulnerability: (Likelihood, Detectability)
• Prioritization of risks
• Plan/develop mitigation strategies
• Re-evaluate: Do it again!

Typical Risk Assessment Process

• Identification of compliance risks
  • OIG Workplan
  • Recent Settlements
  • Organization’s Recent Experience
  • Interviews/Surveys of Leadership
  • Other
Typical Risk Assessment Process

- **Impact Score**
  (Financial + Reputational + Legal)
- **Vulnerability Score**
  (Impact Score x likelihood x detectability)
- **Risk Prioritization**
  - No controls – Vulnerability Score x 100%
  - Limited controls – Vulnerability Score x 75%
  - Some formal controls – Vulnerability Score x 50%
  - Adequate controls – Vulnerability Score x 25%
  - Complete controls – Vulnerability Score x 0%
Culture & Conduct Risk

"Conduct Risk" is an amalgamation of

• Organizational Culture
  ("tone at the top," "mood in the middle" and "buzz at the bottom)

• Conflicts of Interest
  (created by business models and strategies)

• "People Risk"
  (created by behavioral incentives or disincentives, including compensation and disciplinary practices)

• Periodic culture surveys may be the best way to measure

Culture & Conduct Risk

• Organizational Culture
  • Are control functions valued?
  • Are policy & control breaches tolerated?
  • Are organization’s compliance processes proactively identifying risk and non-compliance events?
  • Are immediate managers effective role models of firm culture?
  • Are sub-cultures that do not conform to the desired culture identified and addressed?

• Conflicts of Interest
  • "People Risk"
    (created by behavioral incentives or disincentives, including compensation and disciplinary practices)

Culture & Conduct Risk

• Conflicts of Interest
  • Systematically identifying & inventorying conflicts
  • Resolving or reporting (where necessary) conflicts
  • Periodically testing conflicts management systems

• "People Risk"
  • Training
  • How people are compensated
  • Consistent discipline