Achieving a Risk-Based Approach to Compliance Management

Featuring: Holland & Knight | Kiewit
Achieving a Risk-Based Approach to Compliance Management

Moderator:
Joe LeBas
Chief Strategy Officer
Convercent

Kwamina Williford
Partner
Holland & Knight

Chris Caron
Compliance Director
Kiewit
Foundation for a Risk-Based Compliance Program

To be deemed an effective compliance program, an organization must engage in periodic risk assessments when designing, implementing, and modifying its compliance and ethics program.

U.S. Sentencing Guidelines 8B2.1, cmt 7

Concept accepted by federal enforcement agencies:

- Department of Justice
- Securities and Exchange Commission
- Department of Health & Human Services, Office of Inspector General
The Basics: How Can it Work?

1. Understand Your “Risk Profile”
2. Analyze Risk
3. Prioritize Risk
4. Manage Risk in Approach to Compliance
Step 1: Understanding Your “Risk Profile”

Risk profile: An organization’s overall exposure to some specific risk or group of risks.

Considerations include:

- Strict Regulatory Scrutiny
- Industry Enforcement Climate
- Recent Complaints / Litigation / Audit Results
- Managerial Buy in on Compliance - “Tone from the Top”
- Organization’s Compliance History
- Existence of Internal Controls
Step 2: Analyze Risk

Risk is any issue that impacts an organization’s ability to meet its objectives.

*When analyzing risk, look at measuring:*

- Likelihood of Occurrence
- Likelihood of Impact

*Create common language to analyze risks*
### Step 2: Analyze Risk

**What is the Likelihood of Impact?**

*Sample metrics for analysis*

<table>
<thead>
<tr>
<th>Scale</th>
<th>Legal liability</th>
<th>Health and Safety</th>
<th>Operations (class/research)</th>
<th>Financial Loss</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>-1- Insignificant</strong></td>
<td>Violation with little or no fine/action probable</td>
<td>No injuries or no medical treatment required</td>
<td>Very minor, no operational loss</td>
<td>&lt; $1 M or &lt;1% of Operating Budget</td>
<td>Minor impact to reputation, mention in local news paper</td>
</tr>
<tr>
<td><strong>-2- Minor</strong></td>
<td>Civil fines and/or penalties up to $50,000; little risk of exclusion</td>
<td>First Aid Treatment</td>
<td>Impacts 1 department; possible closure 1-2 days</td>
<td>$1M -$10M or 1% of Operating Budget</td>
<td>Adverse local public attention or complaints</td>
</tr>
<tr>
<td><strong>-3- Serious</strong></td>
<td>Serious breach of regulation with investigation or report to authority possible; fines up to $100,000</td>
<td>Medical Treatment / Hospitalization</td>
<td>Impact beyond 1 department; closes operations for 1 week</td>
<td>$10-20M or 2% of Operating Budget</td>
<td>Probably short terms bad press &amp; highlighted concern from community; some constituent fall out</td>
</tr>
<tr>
<td><strong>-4- Disastrous</strong></td>
<td>Criminal investigation probably, loss of business unit accreditation possible, major litigation, fines up to $1M</td>
<td>Death or extensive injuries</td>
<td>Entire school or business unit and ability to operate for up to 2 weeks</td>
<td>$20-50 M or 6% of Operating Budget</td>
<td>Substantial adverse national media / public attention; constituent fall out</td>
</tr>
<tr>
<td><strong>-5- Catastrophic</strong></td>
<td>Significant prosecution and litigation; criminal conviction and/or exclusion; fines and penalties in excess of $1M</td>
<td>Multiple deaths or severe permanent disabilities</td>
<td>Entire University is unable to operate for a month or longer</td>
<td>&gt;$50 M or &lt;6% of Operating Budget</td>
<td>Prolonged negative press; serious media outcry; sponsors/board questions management; substantial constituent fallout</td>
</tr>
</tbody>
</table>
### Step 2: Analyze Risk

**What is the Likelihood of Occurrence?**

*Sample metrics for analysis*

<table>
<thead>
<tr>
<th>Scale</th>
<th>Likely Occurrence</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1- Rare</td>
<td>Aware of something like this happening elsewhere; expected to occur once every 10 years; <strong>very effective policies, mandatory training, activities monitored and audited.</strong></td>
<td></td>
</tr>
<tr>
<td>-2- Unlikely</td>
<td>Event does occur somewhere from time to time; expected once every 4 to 10 years; responsible persons ensure compliance with policies, regular training, internal monitoring and auditing of activities.</td>
<td></td>
</tr>
<tr>
<td>-3- Possible</td>
<td>Event has occurred at least once during your career; expected once every 3 years; policies are followed and updated, training provided when needed; some informal monitoring.</td>
<td></td>
</tr>
<tr>
<td>-4- Likely</td>
<td>Event has occurred several times or more during your career; expected once a year; policies and procedures in place; compliance not enforced or mandated; some on the job training and no monitoring.</td>
<td></td>
</tr>
<tr>
<td>-5- Almost Certain</td>
<td>Event has occurred in the last six month; expected more than once a year; No controls in place.</td>
<td></td>
</tr>
</tbody>
</table>
Step 3: Prioritize Risk

Likely Impact x Likely Occurrence = Risk Level

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Score Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extreme</td>
<td>17-25</td>
</tr>
<tr>
<td>High</td>
<td>14-16</td>
</tr>
<tr>
<td>Substantial</td>
<td>10-13</td>
</tr>
<tr>
<td>Medium</td>
<td>5-9</td>
</tr>
<tr>
<td>Low</td>
<td>1-4</td>
</tr>
</tbody>
</table>

Highest Likelihood
Highest Impact

Lowest Likelihood
Lowest Impact
Step 4: Managing Risk in Approach to Compliance

Prioritize highest risk areas that impact compliance obligations first:

- Ensure management has buy in on importance of addressing risks to compliance
- Prioritize resources based on risk levels
- Ensure internal controls exist

Note: Lower risk areas should not be ignored, and should be addressed with the requisite priority.
Step 4: Managing Risk in Approach to Compliance

Develop and prioritize internal controls to help manage the risk and promote compliance

- Policies and procedures
- Clear Reporting mechanisms
- Training and Education
- Auditing and monitoring
- Corrective Actions
The Five Monkeys Experiment

In 1967 ....
This will be easy, right?

<table>
<thead>
<tr>
<th>“But we’ve always done it that way!”</th>
<th>“What’s this going to cost us?”</th>
<th>“How long will it take until everything is compliant?”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make sure your efforts don’t conflict with the company goals</td>
<td>Make sure your budget reflects the entire picture</td>
<td>Make sure you set realistic expectations</td>
</tr>
<tr>
<td>Understand what “that way” really means</td>
<td>Understand how budgets drive your company</td>
<td>Understand where Compliance fits in schedule-wise</td>
</tr>
<tr>
<td>Explain that some changes result from regulation changes</td>
<td>Explain that cost avoidance is your goal</td>
<td>Explain that Compliance efforts will be ongoing</td>
</tr>
</tbody>
</table>
Risk? What Risk?

**Enterprise Risk Assessment**
- Focus on Compliance topics
- Categorize each risk by policy or regulatory topic
- Do the ERA on a set schedule

**Identify Past Compliance Issues**
- Internal audits
- External audits / fines
- Industry issues
Managing the Risk You Know

Each Compliance risk must have an associated procedure
- Policy statements
- Procedures manuals
- Expectations

Determine which Compliance risks impact each business unit
- Let them choose from the list
- Let them rate the likelihood of occurrence
- Let them rate the risk impact

Mitigate each compliance risk appropriately
- Procedures / Training / Monitoring
- Assessments
- Measurement
Easy and Hard Learned Lessons

- If management doesn’t support the program, it won’t happen
- If you rely on training alone, you’ll be training forever
- If you’re only a cop, you’ll be the last to know about issues
- If you make Compliance easy or rewarding, people will get it done
- If you don’t update your program regularly, you’re creating hard to change habits
Thank you. Questions?

You’ll receive a recording of this webinar along with a copy of the presentation slides shortly. Thank you for attending!