Some Realism about Risk Assessments

Scott Killingsworth
SCCE Regional Compliance & Ethics Conference
Nashville, Tennessee
June 21, 2019

The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify [its compliance efforts] to reduce the risk of criminal conduct identified through this process.

• To meet [these] requirements, an organization shall
  – Prioritize periodically…to focus on preventing and detecting the criminal conduct identified…as most serious, and most likely, to occur.
  – Modify, as appropriate, the actions taken to reduce the risk of criminal conduct identified…as most serious, and most likely, to occur.

Federal Sentencing Guidelines

The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify [its compliance efforts] to reduce the risk of criminal conduct identified through this process.

• To meet [these] requirements, an organization shall
  – Prioritize periodically…to focus on preventing and detecting the criminal conduct identified…as most serious, and most likely, to occur.
  – Modify, as appropriate, the actions taken to reduce the risk of criminal conduct identified…as most serious, and most likely, to occur.
DOJ Leniency Evaluation Criteria

DOJ “Evaluation of Corporate Compliance Programs,” revised April 2019:

- Policy used for leniency credit in DOJ charging decisions and decisions on monetary penalties and settlement terms
- Sets the criteria for evaluating compliance program design, good-faith implementation, and effectiveness
- Risk Assessments are Part I.A. (!) Looks at:
  - Methodology for identification, analysis and ranking of compliance risks
  - Prioritization and ongoing tailoring of program activities, resources, and mitigation efforts based on risk assessment

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction in a low-risk area.”

Process Fundamentals

- **Identify** the relevant universe of compliance risks
- Assess inherent **likelihood** of each risk in the context of the company's business activities
- Assess the **impact** of compliance failure for each risk
- Likelihood x Impact = Inherent Risk Score
- Evaluate and consider the effect of existing **controls** on the inherent risk
- Arrive at **residual risk** score taking controls into account
- What else could you do to mitigate this risk?
- Based on residual risk and susceptibility to additional controls, prioritize and design improvements to compliance program.

**Toolkit: Risk Universe and Key Data**

<table>
<thead>
<tr>
<th>Compliance Mandate</th>
<th>Doral Priority</th>
<th>History of Problems?</th>
<th>Are They Written?</th>
<th>Who has Manual/Procedures?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fair Credit Reporting Act</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money Laundering</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copyright/Software License</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance/Privacy Policy</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contributions, Gifts, Lobbying</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclosure</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conflicts of Interest - Vendor Relations</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Relations - Gifts, Contracts, Rules, Commercial Bribery</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual Property Protection (Company Trademarks, Copyrights, Patents, Trade Secrets)</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community Involvement</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Charitable Contributions</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Privacy and Security</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of Corporate Resources (e.g., Email, Internet policies)</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information and Records Management and Retention</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic Espionage</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foreign Corrupt Practices Act</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export Controls</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic Embargoes</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.S. Antidumping Law</td>
<td>(Y/N)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Toolkit: Questionnaires

[COMPANY]
ANTI-CORRUPTION RISK ASSESSMENT QUESTIONNAIRE

Contents
A. Country Risk........................................................................................................1
B. Sectoral Risk........................................................................................................2
C. Methods of Seeking Business or Regulatory Treatment.................................2
D. Internal Organization, Procedures and Controls.................................................2

A. Country Risk
1. Please list each country in which each Company operation is present or does or seeks to do business (including sales or purchases to or from that country). For each country, please indicate:
   1.1. What is the country’s reputation for corruption?
   1.1.1. See, for example, Transparency International’s Corruption Perception Index:
   or other sources of information.
   1.1.2. Do local business conditions and customs encourage bribery or kickbacks?
   1.1.3. What requirements does the operation itself have with corruption in the country?
1.2. What requirements of the government of the country affect Company’s business? For example:
   1.2.1. Customs and import requirements
   1.2.2. Export requirements
   1.2.3. Biodiversity qualifications and related information requirements
   1.2.4. Local partner participation requirements
   1.2.5. Local agent requirements

Toolkit: Heat Map

Risk Heat Map

Impact

Likelihood
**Toolkit: Heat Map (Backstage)**

- Identify the relevant universe of compliance risks
- Assess inherent **likelihood** of each risk in the context of the company’s business activities
- Assess the **impact** of compliance failure for each risk
- Likelihood x Impact = Inherent Risk Score
- Evaluate and consider the effect of existing **controls** on the inherent risk
- Arrive at **residual risk** score taking controls into account
- What else could you do to mitigate this risk?
- Based on residual risk and susceptibility to additional controls, **prioritize and design improvements** to compliance program.
More Good Advice

- Buy low, sell high
- Marry your true soul mate
- If bitten by a rattlesnake, remain calm

If You’ve Seen One, You’ve Seen One

<table>
<thead>
<tr>
<th>Business Factors</th>
<th>Compliance Program Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company size</td>
<td>Maturity of existing compliance program</td>
</tr>
<tr>
<td>Industries and industry-specific regulations</td>
<td>- Is this your first checkup?</td>
</tr>
<tr>
<td>Geography</td>
<td>- Familiarity with operations</td>
</tr>
<tr>
<td>Organizational structure</td>
<td>Budget</td>
</tr>
<tr>
<td>Products/Services</td>
<td>In-house skills and resources</td>
</tr>
<tr>
<td>History – M&amp;A or organic growth?</td>
<td>Whose sponsorship/ cooperation can you get?</td>
</tr>
<tr>
<td>Revenue per employee (shape of pyramid)</td>
<td></td>
</tr>
</tbody>
</table>

11

12
Resource constraints tradeoffs

• Compliance staff time vs. other important compliance tasks
  – Including risk mitigation and remediation
• Maximizing use of borrowed resources vs. control over timing and responsiveness and rigor
• Outsourcing: benefits of rented resources vs. cost
• Diminishing returns (and maybe adverse side effects) of more data than you can act on – trail of futility
• Regulator perspective
• Adjust the size with your eyes on the prize!

TINSTAAFL *
*There is no such thing as a free lunch.

Scope and Methodology

• Selecting the risk universe to assess
• Whose opinions do you ask for?
• How do you ask them?
### Scope and Methodology: Risk Universe

**Why not assess all compliance domains?**
- Data quality/respondent fatigue
- Personnel time/cost
- More data than you can act on
- Low end of risk spectrum = large quantity of low-value data

**Who decides what goes on the list for substantive review?**
- Input from compliance and subject-matter experts, e.g. law department, compliance, internal audit, controller, HR, EHS, IT
- Work forward from compliance mandates or backward from business activities?

---

**Scope and Methodology: Risk Universe**

**What areas that are potentially important can be omitted?**
- "Stand-alone" compliance areas with their own risk assessment processes?
- Areas to be assessed later using a different process (e.g. organizational culture)

**What to include regardless:**
- Areas in regulatory flux or intensifying enforcement climate
- Risks related to areas of rapid revenue growth or changes in lines of business, products, services
- Risks associated with geographic expansion
- Acquired businesses
Scope and Methodology: Whose Opinions and How?

- Compliance subject-matter experts
- Senior executives – corporate and business unit
- Designated compliance risk owners if not included above
- Data quality does not necessarily improve when more opinions are solicited; may decline
- Surveys vs. focus groups vs. one-on-one interviews
  - Consider adapting questions and topics to the audience

Building on the Foundation: Follow-on and Specialized Assessments

- Organizational culture
  - Different methodology than domain-based risk assessment
- New acquisitions/new lines of business
- Divestitures and downsizing
  - Lost control functions/subject-matter expertise/compliance ownership
- Third party risks
  - Not just anti-corruption
- Regulatory or enforcement changes
- Deep dives – geographic, line of business, regulatory domain
Some Realism about Uncertainty

- Risk = “effect of uncertainty on achievement of objectives”
- Rummy’s ruminations and the paradox of pursuing precise uncertainty
- The slide rule rule: the output of a calculation can’t be more precise than the least precise input.
- In other words, objects in spreadsheets are fuzzier than they appear

Some Realism about Uncertainty

- Two top risk assessment challenges reported by a large audience of compliance professionals:
  - No consistent means of measuring compliance risks across the organization
  - Can’t get sufficient time, engagement, input from business leaders
- Can you really fix this with even more questions, highly refined criteria for ranking, or a 10-point scale?
  - Or does MEGO effect lead to GIGO effect?
- How about by asking more people?
  - Seriously?
  - Let’s look at what we’re asking people to quantify
Thinking about Impact: How Accurate is the Impact Number?

Prominence of connecting lines indicates relative contribution to overall risk.

Thinking about Impact: How Accurate is the Impact Number?
Working with Uncertainty:  
Do the Math

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5 6</td>
<td>2 3 4 5 6 7 8</td>
</tr>
</tbody>
</table>

Risk Score = \textbf{10} (5x2) but if accuracy of each score realistically is + or – 1, the correct value might be 4 (1x4), or 18 (3x6).

Don’t fight these limitations, you probably can’t win. Accept them and move on. \textit{Any reasoned ranking by knowledgeable people that leads to action is a step forward!}

---

Pitfalls to Avoid

- Falling in love with the process – all prep and documentation, and no action
- Too much data, too little information
  - A mile wide and an inch deep
  - Asking the wrong kind of questions
  - Asking the wrong people
- Biting off more than you can chew
- Letting the perfect be the enemy of the good
- Spurious precision and the illusion of certainty
- Failure to follow up, mitigate risks, and document it
Questions

Scott Killingsworth
Attorney
1364 Rainier Falls Dr. NE
Atlanta, GA 30329-4102
404.272.2203
vskillingsworth@gmail.com