LOOKING FOR TROUBLE:
RISK ASSESSMENTS UNDER THE
REVISED SENTENCING GUIDELINES

Dennis Muse
CEO, Global Compliance

Steven Lauer
Corporate Counsel, Global Compliance

WHAT IS THE GOAL OF A RISK ASSESSMENT?

“A well-managed organization makes a holistic assessment of the risks it faces now and in the future, taking into account the needs of a broad range of external and internal stakeholders. It then designs appropriate risk management and control mechanisms to handle these.”

HOW TO CONDUCT AN ETHICS AND COMPLIANCE RISK ASSESSMENT

- Survey business activities to identify problematic areas and to assess existing compliance efforts
- Survey compliance within industry
- Poll for problematic areas and developing issues
- Synthesize data
- Establish the structure of the ethics and compliance program

US SENTENCING GUIDELINES:
Required elements of an “effective” compliance and ethics program

- Risk-based standards, policies and procedures
- High-level person(s) with direct oversight, authority, and adequate resources
- Care in delegating substantial discretionary authority
- Effective training and communication of standards, policies and procedures
- Detection systems
  - Auditing and Monitoring (“periodic evaluation”) to ensure program is being followed
  - Internal anonymous reporting systems, non-retaliation (Helpline)
  - Means by which employees can seek guidance

Source: [http://www.uscc.gov](http://www.uscc.gov); USSG §8B2.1, Nov. 2004
US SENTENCING GUIDELINES:
Required elements of an “effective” compliance and ethics program

• Appropriate, consistent discipline, including incentives
• Appropriate response mechanisms
  • Program modification to prevent, detect, and correct
  • Voluntary disclosure
• Additions in 2004:
  • Promote culture of ethics and commitment to compliance
  • Ongoing risk assessment as part of program

Source: http://www.ussc.gov; USSG §8B2.1, Nov. 2004

OBJECTIVES OF RISK ASSESSMENT

• Enhance an organization’s compliance and ethics program to meet internal and external requirements and “best practices”
  • Identify risks/gaps and monitor/review performance against requirements
  • Meet US Sentencing Guidelines “risk assessment” and other requirements
• Coordinate methodology and scheduling, as appropriate, with existing enterprise risk assessment processes
• Identify and prioritize significant legal and ethical (reputational) risks to the business
OBJECTIVES OF RISK ASSESSMENT

- Collect and address data and risk indicators from various channels (formal and informal)
- Mitigate the most significant risks through implementation of compliance plans
- Make an organization’s effort less “reactive” and more “proactive”
- Adopt continual improvement approach to risk management
- Synchronize with the organization’s business planning/budget cycle

WHO SHOULD DO THE ASSESSMENT?

- A multidisciplinary team of departments with the following functionality:
  - Legal
  - Human resources
  - Operations
  - Environment and safety
  - Compliance
  - Finance
  - Audit
  - Outside counsel and other experts
WHAT SHOULD THE TEAM REVIEW?

“Each organization will need to scrutinize its operating circumstances, legal surroundings, and industry history to gain a practical understanding of the types of unlawful practices that may arise in future organizational activities”


SOME PRACTICAL CONSIDERATIONS

- Identify legal and ethical (reputational) risks to the business
  - Use a systematic list of questions, working with subject matter experts
  - Include knowledgeable business people in identifying risks
  - Work across “silos” (“you don’t know what you don’t know...”)

- Incorporate and address risk-related information from many channels
  - Helpline and other investigations
  - Audits
  - Employee surveys and certifications
  - Strategy, merger and acquisition
  - External sources (industry, regulatory agencies, etc.)
SOME PRACTICAL CONSIDERATIONS

- Prioritize potential risks by significance—consider fines, business interruption, reputational damage, other costs
- Prioritize - most significant risks first - establish a compliance plan for each
  - Is there a policy (even if only in the Code of Conduct)?
  - Procedures, controls, documentation to implement policy
  - Training and other communications
  - Monitoring and measurement
  - Corrective/preventive mitigating activities
- Continual improvement, year-over-year, will allow you to address additional risk areas and to assess continuing effectiveness of program

REVIEW COMPLIANCE HISTORY

- Criminal matters
- Administrative/regulatory matters
- Civil exposure
- Disciplinary history
EXISTING COMPLIANCE EFFORTS

- Do existing compliance programs cover all appropriate or needed areas?
- Review the workforce (don’t forget agents as appropriate) to develop training and other tools
  - Foundational policies (e.g., anti-harassment)
  - More-specific issues (e.g., antitrust, FCPA)

RISK IDENTIFICATION

- Define “ethics and compliance risk” for the organization
- Try to anticipate future risks (trends)
- Risks in competing organizations
- Who manages each risk area?
- Categorize and match to functional areas
- Identify “events” (an act or occurrence that can affect achievement of program and entity objectives, ethical and legal)
- What events or situations might lead to reputational harm?
### SAMPLE RISK AREAS

- Anti-bribery/Anti-Corruption
- Antitrust/Competition
- Conflicts of Interest
- Corporate Communications
- Data Privacy
- Employment
- Environmental
- Financial Integrity
- Gifts and Entertainment
- Information Security
- Intellectual Property
- Occupational Health and Safety
- Records Management
- Trade Controls – Export and Import
- Use and protection (from misuse) of Company Assets

### SAMPLE COMPANY RISK INVENTORY

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>RISK DESCRIPTION</th>
<th>PROBABILITY</th>
<th>IMPACT</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Corruption</td>
<td>No process for agent screening</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Control of e-mail and Instant Messaging</td>
<td>No controls in place</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Routine Purge of Non-Records</td>
<td>No automated purge is in place</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Relations with competitors</td>
<td>No procedures or training exist</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Records Management Audit</td>
<td>Insufficient audit against compliance goals, metrics</td>
<td>2</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Gifts</td>
<td>No policy with regard to receiving gifts</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>
RISK PRIORITIZATION

- Likelihood – what are the odds that the risk will occur?
- Magnitude (severity) – if it happens, how great will its impact be?
- Frequency – how often might it occur?

PREPARE A RISK MATRIX (“HEAT” MAP)

- Vertical axis – severity
- Horizontal axis – frequency
- Divide entire chart into at least four quadrants
SAMPLE RISK MATRIX OR “HEAT MAP”

ANALYSIS

- What are the costs and benefits of eliminating each identified risk? - low/medium/high threat

- Link the risks and mitigating actions to company’s strategic objectives
IMPLEMENTATION

- Determine whether and how to reduce or eliminate each risk (how much risk will organization tolerate?)
- Determine mitigation actions
- Use “heat map” to organize mitigation efforts and to focus on higher priority (magnitude and probability)
- Report
- Monitor
- Periodically reassess

ISSUES TO KEEP IN MIND

- Internal performance pressures (incentives, evaluation-linked performance criteria, etc.) – how do they impact organizational behavior?
- Culture (risk averse vs. entrepreneurial)
- Well-informed workforce?
- Third-party-related risks (insurance industry rules regarding sales practices of agents)
QUESTIONS?

Dennis Muse
dennis.muse@globalcompliance.com

Steven Lauer
steven.lauer@globalcompliance.com