LOOKING FOR TROUBLE: RISK ASSESSMENTS UNDER THE REVISED SENTENCING GUIDELINES

Dennis Muse
CEO, Global Compliance

Steven Lauer
Corporate Counsel, Global Compliance

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."

Source: PricewaterhouseCoopers, "Protecting the brand: The evolving role of the compliance function and the challenges for the next decade, posted at http://www.pwc.com/extweb/pwcpublications.nsf/docid/466A7F52C643A65F8525702F004A818A/$File/compliancestudydef.pdf

Global Compliance.

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

3

Global Compliance.

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.ussc.gov; USSG §8B2.1, Nov. 2004

4

Global Compliance.

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

5

Global Compliance.

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

6

Global Compliance.

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

7

Global Compliance.

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

8

Global Compliance.

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"

Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines (October 7, 2003), p. 91

9

Global Compliance.

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.)

10

Global Compliance.

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

11

Global Compliance.

REVIEW COMPLIANCE HISTORY

- Criminal matters
- Administrative/regulatory matters
- Civil exposure
- Disciplinary history

12

Global Compliance.

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)

13

Global Compliance.

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?

14

Global Compliance.

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

15

Global Compliance.

SAMPLE COMPANY RISK INVENTORY

TOPIC	RISK DESCRIPTION	PROBABILITY 1. High 2. Medium 3. Low	IMPACT 1. High 2. Medium 3. Low	RISK 1. Very High 2. Very Low
Anti-Corruption	No process for agent screening	**1**	**1**	**1**
Control of e-mail and Instant Messaging	No controls in place	**2**	**1**	**2**
Routine Purge of Non-Records	No automated purge is in place	**1**	**3**	**3**
Relations with competitors	No procedures or training exist	**2**	**2**	**4**
Records Management Audit	Insufficient audit against compliance goals, metrics	**2**	**3**	**6**
Gifts	No policy with regard to receiving gifts	**3**	**3**	**9**

16

Global Compliance.

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?

17

Global Compliance.

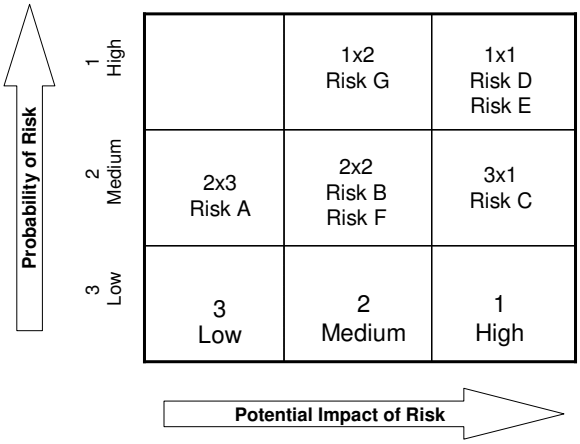
PREPARE A RISK MATRIX ("HEAT" MAP)

- Vertical axis – severity
- Horizontal axis – frequency
- Divide entire chart into at least four quadrants

18

Global Compliance.

SAMPLE RISK MATRIX OR "HEAT MAP"



19

Global Compliance.

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

20

Global Compliance.

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

21

Global Compliance.

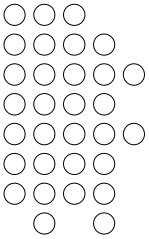
ISSUES TO KEEP IN MIND

- 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)

22

Global Compliance.

QUESTIONS?



Dennis Muse
dennis.muse@globalcompliance.com

Steven Lauer
steven.lauer@globalcompliance.com

Global Compliance