Some Realism about Risk Assessments

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

1

1

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

2

2

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

3

3

DOJ Leniency Evaluation Criteria

"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."

4

Source: U.S. DOJ, "Evaluation of Corporate Compliance Programs," April 2019, p. 3

4

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.

5

5

Toolkit: Risk Universe and Key Data

	A	B	C	D	E	F	G	H	I
1	**Compliance Mandate**	Overall Priority	History of Problems ?	Primary Contacts (Internal: Name, Title, Phone Number; for Outside Counsel or Advisors, give name of Firm as well as Lead Attorney/Consultant). Include outside advisors only if they have or had a major role in formulating or implementing policy.				Are There Written Manuals/ Policies/ Procedures (other than Code)?	Who has Manuals/ Procedures?
2		(H,M,L, 0)	(Y/N)	In-house Legal	Corporate Staff/Operations	Outside Legal	Other Outside Advisors	(Y/N)	
52	Fair Credit Reporting Act								
53	Money Laundering								
54	Copyright/Software License Compliance/ Piracy								
55	Political Activity – Contributions, Gifts, Lobbying Disclosure								
56	Conflicts of Interest -- Vendor Relations								
57	Customer Relations – Gifts, Contracting Rules, Commercial Bribery								
58	Intellectual Property Protection (Company Trademarks, Copyrights, Patents, Trade Secrets)								
59	Community Involvement/ Charitable Contributions								
60	Data Privacy and Security								
61	Use of Corporate Resources (e.g., Email, Internet policies)								
62	Information and Records Management and Retention								
63	Economic Espionage								
64	Foreign Corrupt Practices Act								
65	Export Controls								
66	Economic Embargoes								
67	U.S. Antiboycott Law								

6

6

Toolkit: Questionnaires

Attorney-Client Privileged and Confidential

[COMPANY]
ANTI-CORRUPTION RISK ASSESSMENT QUESTIONNAIRE

Contents

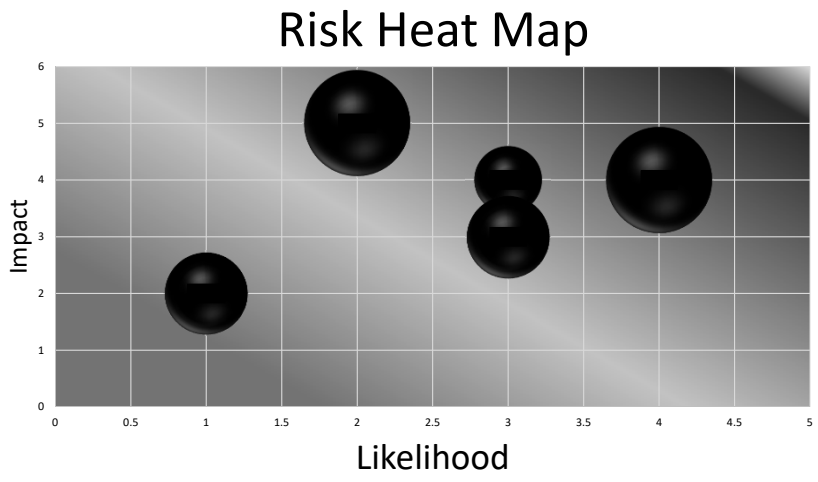
A. Country Risk

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 Perceptions Index: http://www.transparency.org/policy_research/surveys_indices/cpi/2010/results or other sources of information.
     - 1.1.2. Do local business conditions and customs encourage bribery or kickbacks?
     - 1.1.3. What experience 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. Bidder qualification and related information requirements
     - 1.2.4. Local partner participation requirements
     - 1.2.5. Local agent requirements

7

7

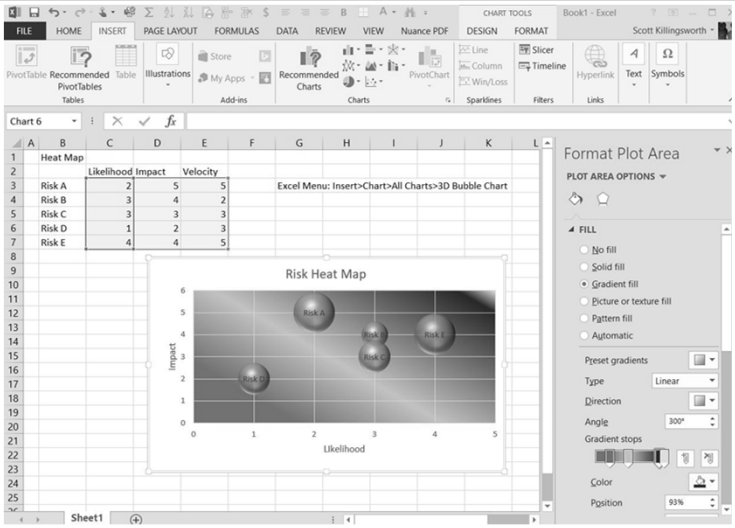
Toolkit: Heat Map



8

8

Toolkit: Heat Map (Backstage)



9

9

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.

10

10

More Good Advice

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

11

11

If You've Seen One, You've Seen One

Business Factors

- Company size
- Industries and industry-specific regulations
- Geography
- Organizational structure
- Products/Services
- History – M&A or organic growth?
- Revenue per employee (shape of pyramid)

Compliance Program Factors

- Maturity of existing compliance program
  - Is this your first checkup?
  - Familiarity with operations
- Budget
- In-house skills and resources
- Whose sponsorship/ cooperation can you get?

12

12

TINSTAAFL *

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

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!

13

13

Scope and Methodology

- Selecting the risk universe to assess
- Whose opinions do you ask for?
- How do you ask them?

14

14

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?

15

15

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

16

16

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

17

17

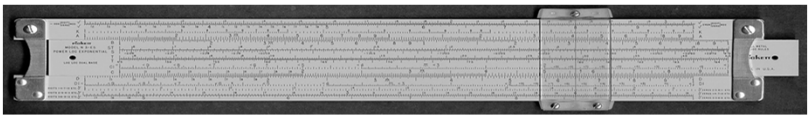
Building on the Foundation:
Follow-on and Specialized Assessments

- 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

18

18

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

19

19

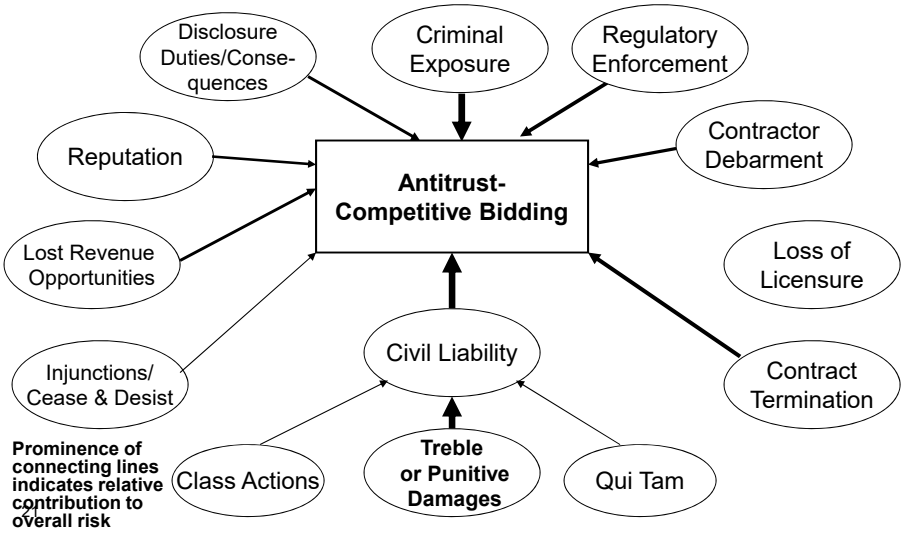
Some Realism about Uncertainty

- 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

20

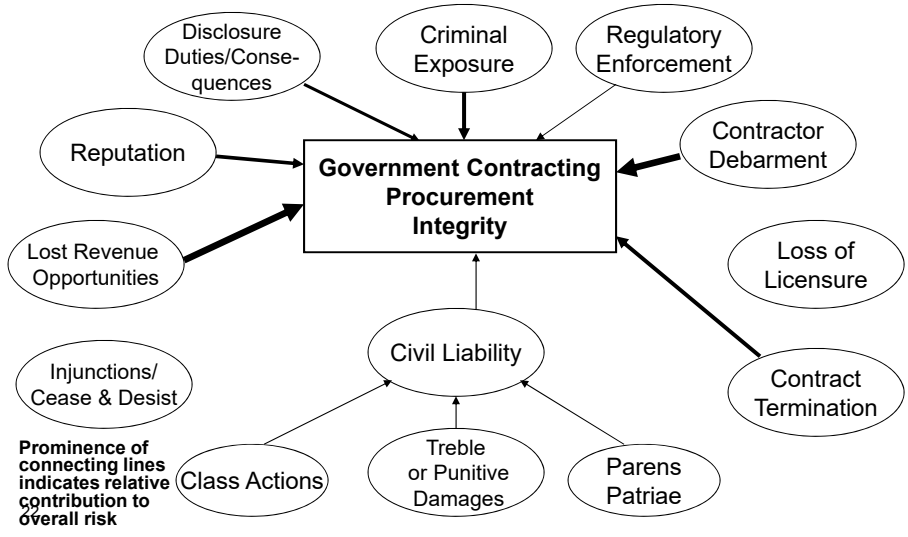
20

Thinking about Impact:
How Accurate is the Impact Number?



21

Thinking about Impact:
How Accurate is the Impact Number?



22

Working with Uncertainty:
Do the Math

Likelihood = 1 **2** 3 4 5 6

Impact = 2 3 4 **5** 6 7 8

Risk Score = **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. *Any reasoned ranking by knowledgeable people that leads to action is a step forward!*

23

23

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

24

24

Questions ?

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

vskillingsworth@gmail.com

25