

Compliance Risk Assessment and Management Workshop

Society of Corporate Compliance and Ethics and
Health Care Compliance Association



[1]

1

ASSESSING SEVERITY OF RISKS

Gwendolyn Lee Hassan, JD, CCEP

gwenhassan@yahoo.com

708-932-6437



[2]

2

Overview

- Defining risk and risk severity
- Looking at probability and impact of risk
 - Variables to consider in looking at both
- Different graphic depictions of risk
- Internal control effectiveness measures
- Advanced practice and methodology



{ 3 }

3

What do we mean by risk?

- Inherent Risk – The Effectiveness of Internal Controls = Residual Risk
 - **Actual** Residual Risk v. **Target** Residual Risk

If Actual > Target, then you need additional controls

Severity can be measured either on an inherent risk basis or after considering the effect of internal controls, but the preferred approach, and what we will do in this workshop, is to measure severity on an inherent risk basis.



{ 4 }

4

How do you measure severity of risk?

- The basic calculation:

$$\text{Probability of risk} \times \text{Impact of risk} = \text{Severity}$$

- Low probability x nominal impact = Low Risk
- High probability x catastrophic impact = High Risk



{ 5 }

5

Probability of risk

- How likely is it that this risk will occur?

$$\text{Probability of risk} \times \text{Impact of risk} = \text{Severity}$$

- First: What scale will you use?
 - Low-Medium-High
 - *Numeric scale of 1-3, 1-5, 1-10
 - Color scale (red, yellow, green)



{ 6 }

6

Probability Scale

- What does “low” likelihood mean?
- How do you define “medium” likelihood?
- And “high” likelihood?



[7]

7

Polling Question

- You have an in-ground pool in your backyard. It’s an awesome pool with a water slide and a diving board with a maximum depth of 10 feet. You allow your family and friends use the pool almost every weekend when the weather cooperates. How would you categorize the inherent risk of someone drowning in your pool?
 - A High
 - B Medium
 - C Low
 - D Nonexistent



[8]

8

Frequency

- Frequency as a component of likelihood
- Is this something that happens often? Rarely?
 - What do each of these terms mean in your organization?
- What about so-called “Black Swan” or “Perfect Storm” events?
- Is the frequency changing?



[9]

9

Probability Scale

- The importance of a clearly defined likelihood scale
 - Time bound for frequency measure
 - What time periods are we using to frame our assessment of probability? Year? Quarter? Month? Day?
- “Low likelihood means a risk our organization expects to encounter less than ____ in any given ____”



[10]

10

Other factors impacting likelihood

- Volume (repeatability) of activity
- Number of participants involved
- Complexity of processes, number of “steps” in a process
- Training, education and experience level of persons involved
- So-called “perverse” incentives and pressures



{ 11 }

11

Polling Question

- Consider the backyard pool example again, but this time, assume your pool is only used 2 weekends a year and only by you and your spouse who both swam on your college swim teams and are CPR certified. The pool has no diving board or slide and has a maximum depth of 5 feet. There is an 8-foot-tall electrified fence surrounding your pool to prevent unauthorized access. How would you categorize the inherent risk of someone drowning in your pool?
 - A High
 - B Medium
 - C Low
 - D Nonexistent



{ 12 }

12

Other probability factors

- Next: What factors should be considered to determine likelihood?
 - History of occurrence:
 - in the organization
 - in the industry
 - in a particular geography
 - Overall enforcement history for the subject matter



[13]

13

Impact of geographical scope

- Consider regional assessments
- Sub-regional assessments
- Country-based assessments
- Location-based assessment

- What level of granularity works best for your organization?



[14]

14

Carefully designed likelihood measures

- How sophisticated do you want to be?
- “Low likelihood means a risk our organization expects to encounter less than ____ in any given ____”
- “Low likelihood means a risk present in our industry in general but for which there have been no enforcement examples in the last calendar year in this particular geography and with which our organization has no direct history and for which our processes are simplified, and our training is extensive and is a low volume risk with no known pressures or incentives that we expect to encounter less than ____ in any given ____.”



15

15

Suggested approach

- Communicate these probability factors as part of instructions
- Suggest items to be taken into account by assessors
 - Vary factors by risk categories where possible
- Use simplified definitions



16

16

Suggested approach

- Anti-Bribery and Corruption Risk Assessment for North America:
 - “As you assess the *likelihood of risks* in this category, please consider the following important factors as part of your assessment:
 - Average CPI of countries in the region
 - History of enforcement actions in this region
 - Volume of business involving government officials in this region
 - Training previously provided in this region



17

17

Impact of the risk

Probability of risk x Impact of risk = Severity

- First: What scale will you use?
 - Low-Medium-High
 - *Numeric scale of 1-3, 1-5, 1-10
 - Color scale (red, yellow, green)



18

18

Impact scale

- Use of financial parameters as one measure of impact
 - Low risk: Potential financial impact of less than \$50,000
 - Medium risk: Potential financial impact of less than \$250,000
 - High risk: Potential financial impact of more than \$250,000



[19]

19

Other impact factors

- Legal/Compliance impact
 - Potential for a monitor
 - Disqualification from participation in preference programs
- Operational impact
 - Shut-down or interruption of operations, inefficiency in operations, diversion of resources
- Strategic impact
 - Inability to achieve one or more strategic goals



[20]

20

What time measure will you use for impact?

- Immediate impact?
 - Sudden drop in share price
 - Expenses for PR/Legal/Crisis Management
- Long-term impact?
 - Reserves for litigation and legal fees
 - Fines and penalties
 - Long-term drag on share value



[21]

21

Direct or indirect impact?

- Both!
- Closely related to immediate and long-term impacts



[22]

22

Reputational risk

- A note about reputational risk
- Is in “included” within a financial quantification of risk?
- Is it its own separate risk with its own potential financial impact?



[23]

23

Suggested approach

- Anti-Bribery and Corruption Risk Assessment for North America:
 - “As you assess the *impact of risks* in this category, please consider the following important factors as part of your assessment:
 - Financial and reputational impacts both immediate and long term, both direct and indirect
 - Operational risks including interruption or shut down of operations
 - Legal/compliance impacts including loss of qualification for government programs
 - Strategic risks including inability to meet strategic goals



[24]

24

Likelihood of the impact

- For more mature programs:
 - How likely is a particular impact?
 - How likely are certain ranges of costs to be incurred?



[25]

25

Effectiveness of controls

- How do you account for effective/ineffective controls on your risks?
- I suggest the following:
 - Probability of risk x Impact of Risk = **Inherent Risk**
 - Inherent Risk – Mitigating Measures = **Residual Risk**
- The difference between the two is the VALUE of your compliance program!



[26]

26

Types of potential controls

Mitigation Measures

- Policies
- Processes
- Audit programs
- Use of AI to detect aberrations
- Training
- Table-top exercises
- Crisis response plans
- System controls

Mitigation Measures

- Contractual clauses
- Recusal agreements
- Certifications
- Insurance coverage



[27]

27

Calculating the reduction in risk from effective controls

- Calculate Inherent Risk (f/k/a “gross risk”) first
- Avoid ignoring or “discounting” of risks due to mitigation
 - Can result in under-appreciation of compliance program
 - Loss of recognition of resources needed



[28]

28

Other approaches

- Individual assessment of each factor
 - Frequency: 3
 - Complexity: 2
 - Volume: 3
 - Incentives:3
- For example, bribery in a small sales office in the Middle East might have the scores above creating an average likelihood score of 2.75



[29]

29

Extra credit - mature program additions

- Additional measures to consider as your program matures:
 - Risk velocity
 - Risk trend analysis (year over year, quarter over quarter)
 - Emerging risks
 - Risk vulnerability analysis



[30]

30

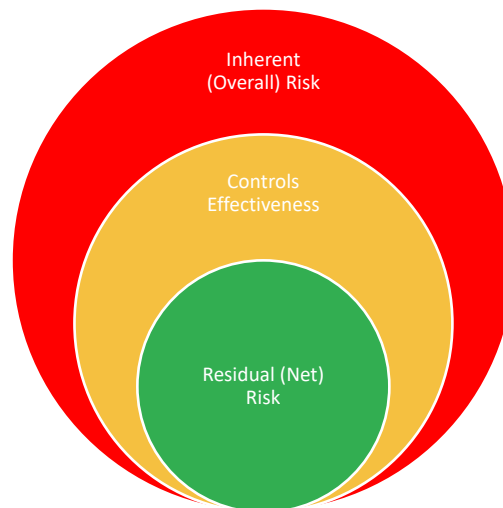
Graphic depictions of risk

There are many ways to graphically communicate risk levels.

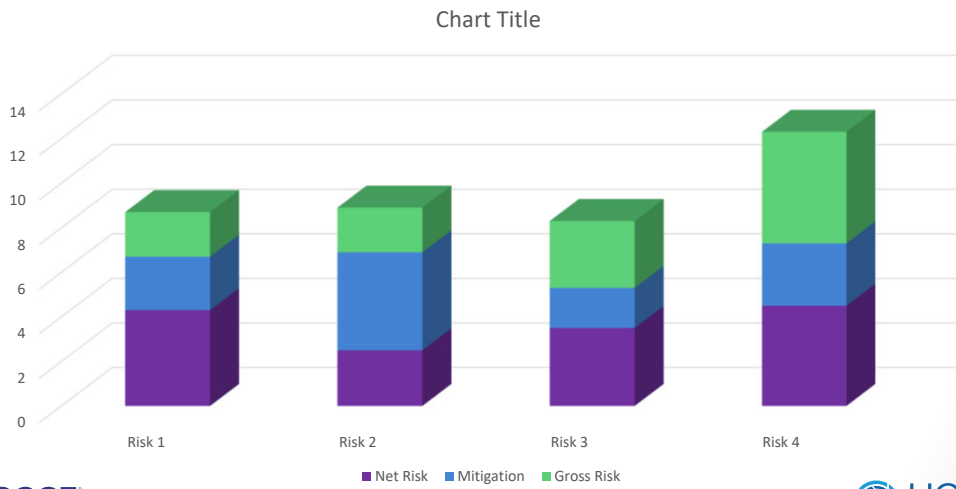
A simple “speedometer” graphic often works well.



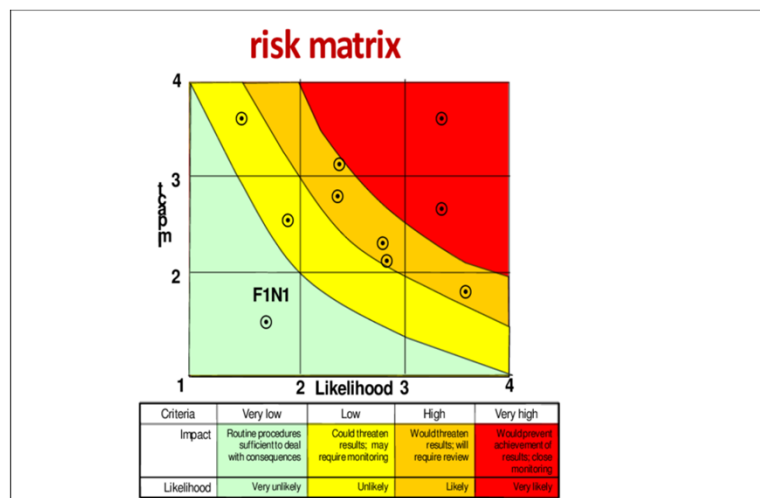
Depicting Residual Risk



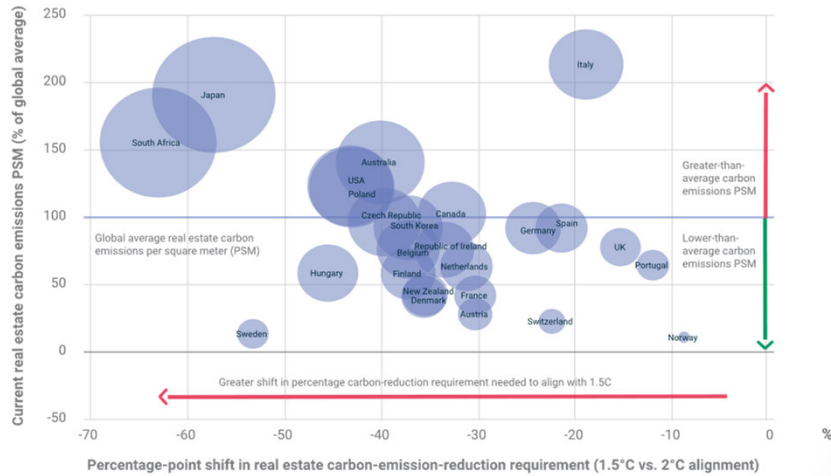
Depicting Residual Risk



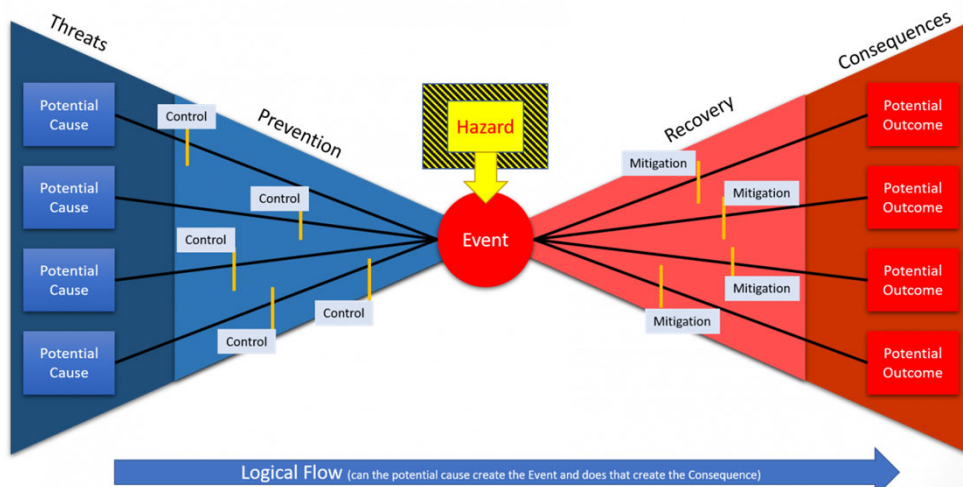
Graphic depictions of risk



Graphic depictions of risk

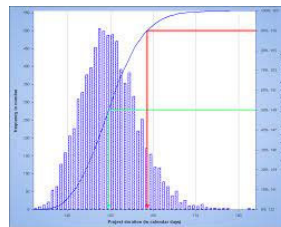


Advanced Techniques



Monte Carlo Analysis

- Wide range of potential outcomes based on probability
- Mathematical calculation
- “Go for broke” on one end of the spectrum
- Very conservative on the other end of the spectrum
- All the middle ground as well



37

37

Methodology

- The “how” of risk assessment
 - Who participates?
 - How do they participate?
 - Written survey or questionnaire
 - Interviews
 - Who develops the questions and gathers the data?
 - Who “crunches the numbers”?



38

38

Exercise

You are conducting an initial risk assessment for your organization. You are assessing, for the first time, the risk of a discrimination case in your operations in Latin America. Please take a few minutes to jot down your answers to the following questions:

1. What risk scale will you use?
2. What method will you use to assess risk?
3. Who will you select to participate in the assessment?
4. What questions will you ask participants to determine inherent risk and residual risk?
5. What additional information would it be helpful to have?



[39]

39

Question 1

- What risk scale did you use?
 - Simplified scale of Low-Medium-High?
 - More granular scale of 1 to 5
 - Detailed scale of 1 to 10



[40]

40

Question 2

- What method will you use to assess risk?
 - Written questionnaire only?
 - In-person (or virtual) interviews?
 - Phone?
 - Video?
 - Both?



[41]

41

Question 3

- Who will you select to participate in the assessment?
 - Local HR team?
 - Local management?
 - Local hourly staff?
 - U.S. HQ staff?
 - All of the above?



[42]

42

Question 4

- What questions will you ask participants to determine inherent risk and residual risk?
 - Questions about likelihood
 - Questions about impact
 - Questions about effectiveness of controls



[43]

43

Question 5

- What additional information would it be helpful to have?
 - Organization's risk appetite and tolerance
 - Target residual risk for discrimination
 - Enforcement history at this location
 - Helpline data for this location
 - Results of cultural survey for this location
 - Relative expertise of the human resources, compliance and management team at this location



[44]

44

Wrap-up

- Both probability and impact of risk can be impacted by multiple variables, make sure you're aware of them
 - The effectiveness of your controls will have the largest impact
- Choose the methodology and graphic depiction of risk that works best for your organization
- Pay attention to the demographics of those you invite to participate in your assessment

