Risk Management Insight

FAIR

(FACTOR ANALYSIS OF INFORMATION RISK)

Basic Risk Assessment Guide

NOTE: Before using this assessment guide…

Using this guide effectively requires a solid understanding of FAIR concepts

- As with any high-level analysis method, results can depend upon variables that may not be accounted for at this level of abstraction
- The loss magnitude scale described in this section is adjusted for a specific organizational size and risk capacity. Labels used in the scale (e.g., “Severe”, “Low”, etc.) may need to be adjusted when analyzing organizations of different sizes
- This process is a simplified, introductory version that may not be appropriate for some analyses

Basic FAIR analysis is comprised of ten steps in four stages:

Stage 1 – Identify scenario components

1. Identify the asset at risk
2. Identify the threat community under consideration

Stage 2 – Evaluate Loss Event Frequency (LEF)

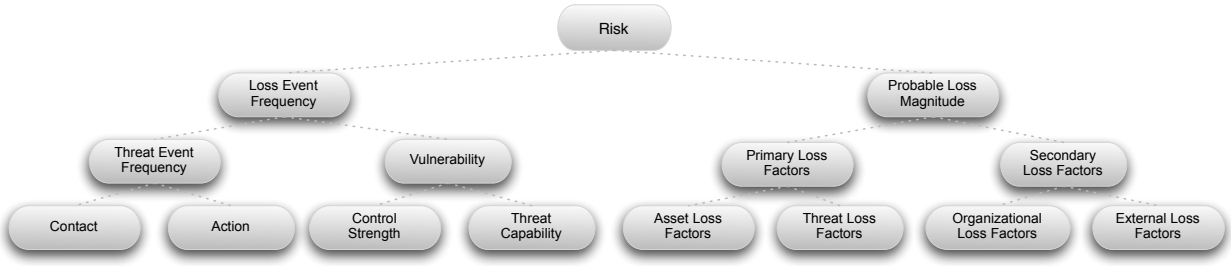
3. Estimate the probable Threat Event Frequency (TEF)
4. Estimate the Threat Capability (TCap)
5. Estimate Control strength (CS)
6. Derive Vulnerability (Vuln)
7. Derive Loss Event Frequency (LEF)

Stage 3 – Evaluate Probable Loss Magnitude (PLM)

8. Estimate worst-case loss
9. Estimate probable loss

Stage 4 – Derive and articulate Risk

10. Derive and articulate Risk



Stage 1 – Identify Scenario Components

Step 1 – Identify the Asset(s) at risk

In order to estimate the control and value characteristics within a risk analysis, the analyst must first identify the asset (object) under evaluation. If a multilevel analysis is being performed, the analyst will need to identify and evaluate the primary asset (object) at risk and all meta-objects that exist between the primary asset and the threat community. This guide is intended for use in simple, single level risk analysis, and does not describe the additional steps required for a multilevel analysis.

Asset(s) at risk: _____

Step 2 – Identify the Threat Community

In order to estimate Threat Event Frequency (TEF) and Threat Capability (TCap), a specific threat community must first be identified. At minimum, when evaluating the risk associated with malicious acts, the analyst has to decide whether the threat community is human or malware, and internal or external. In most circumstances, it's appropriate to define the threat community more specifically – e.g., network engineers, cleaning crew, etc., and characterize the expected nature of the community. This document does not include guidance in how to perform broad-spectrum (i.e., multi-threat community) analyses.

Threat community: _____

Characterization	

Stage 2 – Evaluate Loss Event Frequency

Step 3 – Threat Event Frequency (TEF)

The probable frequency, within a given timeframe, that a threat agent will act against an asset

Contributing factors: Contact Frequency, Probability of Action

Rating	✓	Description
Very High (VH)		> 100 times per year
High (H)		Between 10 and 100 times per year
Moderate (M)		Between 1 and 10 times per year
Low (L)		Between .1 and 1 times per year
Very Low (VL)		< .1 times per year (less than once every ten years)

Rationale	

Step 4 – Threat Capability (Tcap)

The probable level of force that a threat agent is capable of applying against an asset

Contributing factors: Skill, Resources

Rating	✓	Description
Very High (VH)		Top 2% when compared against the overall threat population
High (H)		Top 16% when compared against the overall threat population
Moderate (M)		Average skill and resources (between bottom 16% and top 16%)
Low (L)		Bottom 16% when compared against the overall threat population
Very Low (VL)		Bottom 2% when compared against the overall threat population

Rationale	

Step 5 – Control strength (CS)

The expected effectiveness of controls, over a given timeframe, as measured against a baseline level of force

Contributing factors: Strength, Assurance

Rating	✓	Description
Very High (VH)		Protects against all but the top 2% of an avg. threat population
High (H)		Protects against all but the top 16% of an avg. threat population
Moderate (M)		Protects against the average threat agent
Low (L)		Only protects against bottom 16% of an avg. threat population
Very Low (VL)		Only protects against bottom 2% of an avg. threat population

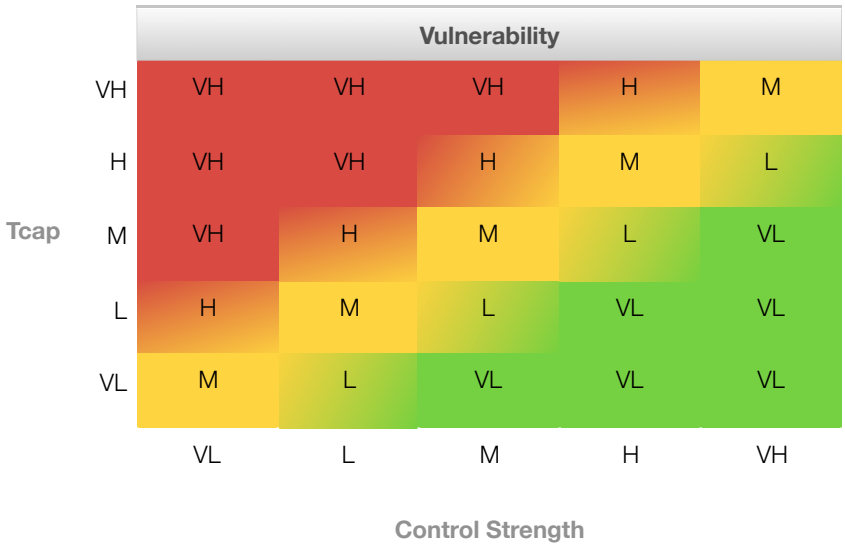
Rationale	

Step 6 – Vulnerability (Vuln)

The probability that an asset will be unable to resist the actions of a threat agent

Tcap (from step 4): _____

CS (from step 5): _____



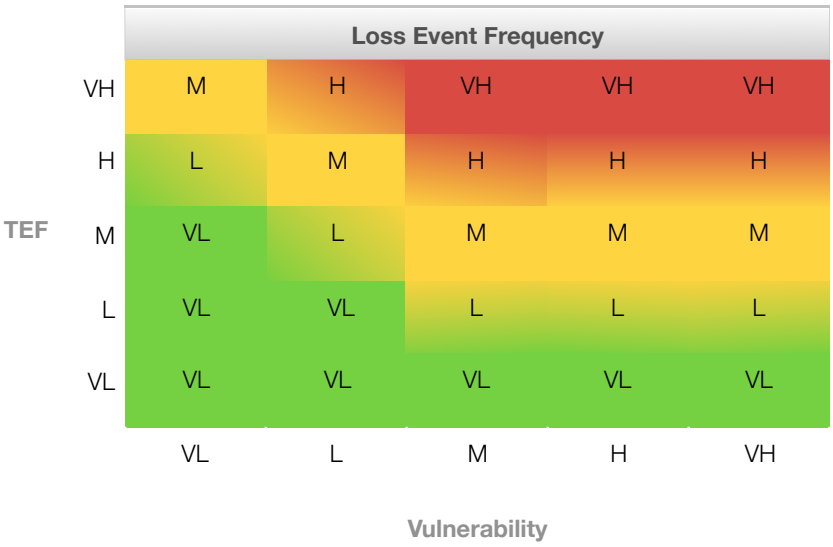
Vuln (from matrix above): _____

Step 7 – Loss Event Frequency (LEF)

The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset

TEF (from step 3): _____

Vuln (from step 6): _____



LEF (from matrix above): _____

Stage 3 – Evaluate Probable Loss Magnitude

Step 8 – Estimate worst-case loss

Estimate worst-case magnitude using the following three steps:

- Determine the threat action that would most likely result in a worst-case outcome
- Estimate the magnitude for each loss form associated with that threat action
- "Sum" the loss form magnitudes

	Loss Forms					
Threat Actions	Productivity	Response	Replacement	Fine/Judgments	Comp. Adv.	Reputation
Access						
Misuse						
Disclosure						
Modification						
Deny Access						

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	--
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

Step 9 – Estimate probable loss

Estimate probable loss magnitude using the following three steps:

- Identify the most likely threat community action(s)
- Evaluate the probable loss magnitude for each loss form
- "Sum" the magnitudes

	Loss Forms					
Threat Actions	Productivity	Response	Replacement	Fine/Judgments	Comp. Adv.	Reputation
Access						
Misuse						
Disclosure						
Modification						
Deny Access						

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	--
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

Stage 4 – Derive and Articulate Risk

Step 10 – Derive and Articulate Risk

The probable frequency and probable magnitude of future loss

Well-articulated risk analyses provide decision-makers with at least two key pieces of information:

- The estimated loss event frequency (LEF), and
- The estimated probable loss magnitude (PLM)

This information can be conveyed through text, charts, or both. In most circumstances, it's advisable to also provide the estimated high-end loss potential so that the decision-maker is aware of what the worst-case scenario might look like. Depending upon the scenario, additional specific information may be warranted if, for example:

- Significant due diligence exposure exists
- Significant reputation, legal, or regulatory considerations exist

		Risk				
	Severe	H	H	C	C	C
	High	M	H	H	C	C
PLM	Significant	M	M	H	H	C
	Moderate	L	M	M	H	H
	Low	L	L	M	M	M
	Very Low	L	L	M	M	M
		VL	L	M	H	VH
				LEF		

LEF (from step 7): _____

PLM (from step 9): _____

WCLM (from step 8): _____

Key	Risk Level
C	Critical
H	High
M	Medium
L	Low