THE FAIR MODEL

FAIR INSTITUTE
WWW.FAIRINSTITUTE.ORG

Factor Analysis of Information Risk (FAIR) is the only international standard quantitative model for information security and operational risk

DEFINITIONS:

RISK: The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY: The frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY: The frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY: The probability that a threat event will become a loss event

THREAT CAPABILITY: The level of force a threat agent is able to apply

RESISTANCE STRENGTH: A measure of how difficult it is for a threat actor to inflict harm (a.k.a. difficulty)

SECONDARY LOSS EVENT FREQUENCY: The percentage of time that secondary stakeholders are likely to react negatively to an event

FORMS OF LOSS:

PRODUCTIVITY LOSS: Loss that results from an operational inability to deliver products or services

RESPONSE COSTS: Loss associated with the costs of managing an event

REPLACEMENT COSTS: Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS: Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

FINES AND JUDGMENTS: Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE: Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

ANALYSIS SCOPING:

1. Clearly understand & describe the loss event
2. Identify the asset(s)
3. Identify relevant threat(s)
4. Define Effect: C-I-A

CALIBRATION:

- Start with the absurd
- Consider what you DO know
- Decompose the problem
- Identify / challenge your assumptions
- Consider where data may exist
- Seek out SMEs
- Focus on accuracy rather than high precision