The FAIR Model

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.