Revisiting Technology Risk Quantification

Atul Kumar
ISACA NL
15-02-2023

Technology risk management and its importance

- Alignment with business objectives
- Incorporate new solutions for better product/ services experience
- Data Sovereignty and protection standards
- Optimize existing technology stack
- Build and maintain stakeholder confidence in technology spend
- Improve cyber resilience
- Financial planning
- Enhance the GRC posture

What does it mean to us within corporate sector ?

Classical Risk Management (Qualitative) V/S Quantitative Risk Management techniques

• Easy to conduct • Simple to implement • Provides precise insights • Might not incorporate complex scenarios • Inaccurate insights	• Complex methodology • Requires high quality data sets • Requires expertise • Provides accurate insights • Cost benefit model • Supports Financial planning

Classical Risk Management (Qualitative) V/S Quantitative Risk Management techniques

Probability vs. Possibility

Quantitative risk analysis leads to:

1. identify most probable risks
2. risk transition scenario from potential to a real risk situation

The study of probability offers the opportunity to understand the level of certainty and impossibility for every given scenario. Unlike the binary nature of possibility, where a specific occurrence may or may not happen, probability intimates that an incident can happen, but it may also not, depending on the remedial and preventive actions that a company will exercise.

Precision vs. Accuracy

In measuring probabilities, the difference between precision and accuracy can, quite literally, translate to a life or death situation.

Accuracy refers to the closeness of the measurements to the factual value/s.

Precision is a measure of closeness of the range of measurements to each other and may be able to obtain exact data.

In the field of quantitative risk management accuracy is preferred

Quantitative risk management technique

Lets take an example:

- Storage system hardware value: US $100,000 (SLE HW)
- Virtualization software value: US $ 50,000 (SLE for SW)
- Statistical data informs that a system catastrophic failure (due to software or hardware) occurs once in 10 years (ARO = 1/10 = 0.1)
- ALE for HW = 100,000 * 0.1 = US $ 100,00
- ALE for SW = 50,000 * 0.1 = US $ 5000

Quantitative risk management technique cont.

Exposure factor (EF): potential % of loss to a specific asset if a specific threat is realized. It is a subjective value that the person assessing risk must define.

The exposure factor is represented in the impact of the risk over the asset, or percentage of asset lost.

Asset Value: total value of the asset

As an example, if the asset value is reduced two thirds, the exposure factor value is 0.66. If the asset is completely lost, the exposure factor is 1.0.

Single loss expectancy (SLE): Monetary value expected from the occurrence of a risk on an asset
SLE = EF * Asset Value

Annual rate of occurrence (ARO): The probability that a risk will occur in a particular year

Annualized loss expectancy (ALE): ALE provides an estimate of the yearly financial impact to the organization from a particular risk.

ALE = ARO *SLE

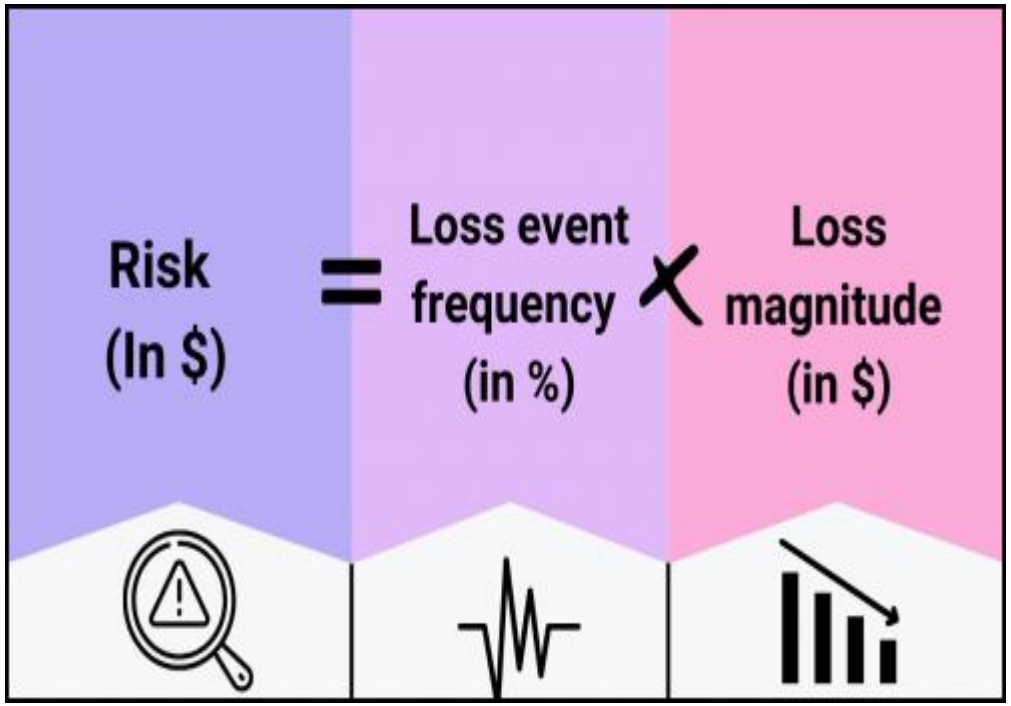
Quantitative risk model

Introduction to FAIR model

- FAIR™ (Factor Analysis of Information Risk)
- The open standard for quantifying and managing risk
- Emerged as the premier Value at Risk (VaR) model for cybersecurity and operational risk.
- Non-profit professional organization
- Dedicated to advancing the discipline of measuring and managing cyber and operational risk.

The FAIR Model (source: The FAIR Institute - https://www.fairinstitute.org/)

Introduction to FAIR model cont.



The FAIR Model (source: The FAIR Institute - https://www.fairinstitute.org/)

Implementation pre-requisites and areas to ponder

- Asset Management: the key to Risk Management
- Inadequacy of data
- Expertise is required in careful interpretation
- Stakeholders’ understanding and buy in
- External Audit preparation
- Time consumption
- Result credibility
- Ownership issues

Questions and Answers

Thank you!