Financial Risk

Aleksandr Lenin

Financial Risk

- Types of risk related to financing, including financial transactions, loans, etc.
- Often is understood to include only the potential or financial loss and uncertainty about its extent
- Portfolio Theory by Harry Markowitz (1952) – the science of managing market and financial risks
- Modern portfolio theory uses slightly different definitions of risk

Financial Risk

Main categories of financial risk are:

- Asset-backed risk – risks related to interest rate, term modification, prepayment
- Credit risk
- Foreign investment risk
- Liquidity risk – liquidity of assets and funding
- Market risk – equity risk, interest rate risk, currency risk, commodity risk
- Model risk
- Operational risk (including legal risk)

Financial Risk

Typically, financial risk is measured in terms of Annual Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$

Annual Loss Expectancy (ALE) – expected total yearly loss of all instances of a specific threat against a specific asset

Single Loss Expectancy (SLE) – impact associated with a single materialized risk against a specific asset.

Annual Rate of Occurrence (ARO) – expected frequency with which a specific threat or risk will occur within a single year.

Single Loss Expectancy

$$\text{SLE} = \text{Asset value} \times EF$$

EF (Exposure Factor) is percentage of loss in asset value in the result of threat occurrence

SLE is expressed as a monetary value

Imagine that you've got a system worth 100'000 EUR. In the event of a fire, the remains the system will be worth 8000 EUR. In the event of fire, the asset will lose 92% of its value – therefore EF is 0.92

$$\text{SLE} = 100'000 \times 0.92 = 92000 \text{ EUR}$$

Annualized Rate of Occurrence

ARO is the expected frequency with which a single risk will occur within a year.

ARO value 0.0 means that a risk will never occur within a single year.

ARO may range from 0.0 to very large numbers indicating frequent occurrence of risk

ARO calculation is known as frequency determination. It is calculated by multiplying the likelihood of a single occurrence by the number of threat agents who would initiate the treat

For example, ARO of an earthquake in a city may be 0.00001, however, an ARO of a workstation infection in an office may be 10′000′000.

Annual Loss Expectancy

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

If SLE of an asset is 90′000 EUR and the ARO of the considered threat (such as total power loss) is 0.5, then the ALE is 90′000 × 0.5 = 45′000 EUR.

If the ARO for a specific threat were 15 (e.g. a compromised user account), the ALE would be 1′350′000 EUR.

ALE Revisited

- Calculate ALE for the asset in the case when the security measure is deployed
  - This requires calculation of EF and ARO specific to the considered security measure
- Rationale baseline:
  - *the annual cost of security measure should not exceed the annual loss for the asset being protected by the security measure*

ALE Revisited

Value of the security measure to the company:

> ALE before security measure deployment−
>
> ALE after security measure deployment−
>
> annual cost of the security measure

- If the result is negative, it is not rational to invest into the considered security measure
- If the result is positive, that value is the *annual savings* and the organization can benefit from investing into such a security measure and deploying it – it is worth its costs.

The annual savings or loss from a security measure should not be the only factor considered when evaluating available security measures

Risk Components
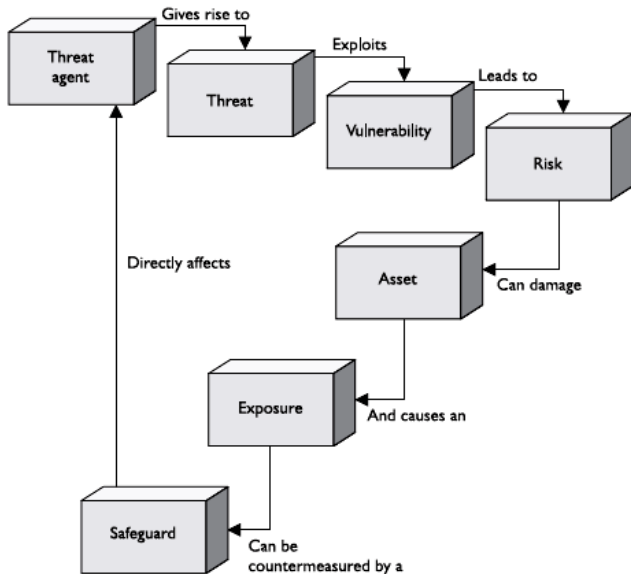
How do we measure risk?

- Use a structured methodology
- Predefine general values to avoid confusion
- Identify risks
- Straightforward way:
  - Define the expected damage for each threat
  - Calculate Risk = Probability $\times$ Damage Potential
  - Use some risk assessment framework – estimate the values of risk components, i.a. with a defined risk taxonomy

Qualitative Approaches:

- The Delphi technique
- Scenarios
- Frameworks, i.e. FAIR (Factor Analysis of Information Risk)

Quantitative approaches

- availability of statistical data
- relying on expert estimations - unreliable
- different models requiring varying parameters