Qualitative Risk Assessment

Aleksandr Lenin

Risk Assessment

According to ISO Guide 73:2009 Risk management – Vocabulary, risk assessment consists of the following three steps:

1. Risk Identification
2. Risk Analysis
3. Risk Evaluation

Risk Analysis:

- estimation of impact and likelihood of risk
- qualitative or quantitative

Qualitative Risk Analysis

Risk analysis is a technique concerned with discovering the *likelihood* and *impact* of risks.

Qualitative RA is more *scenario* based than calculation based.

Threats are ranked on an ordinal scale in terms of *categories* (low/medium/high) or *orders of magnitude* (dozens, hundreds, thousands).

Qualitative estimations are more subjective than quantitative ones.

Risk mitigation plans are more hard to justify to management.

Qualitative Risk Analysis

- Straightforward approach – direct estimation of likelihood and impact
- Estimation of risk components, with subsequent calculation of risk level

Qualitative Risk Analysis

Data input types:

1. Statistical data
2. Empirical evidence collection
3. Expert estimation
   - 3.1 Brainstorming
   - 3.2 Surveys
   - 3.3 Interviews
   - 3.4 Checklists
   - 3.5 Delphi technique
   - 3.6 ...
4. Calculation

Delphi technique

- A group decision and problem solving method
- A way to obtain expert opinions without experts being face-to-face
- Ensures that each member gives an honest opinion on any particular risk threat
- Relies on a panel of experts

Delphi technique

- The experts answer questionnaires in two or more rounds
- After each round the facilitator provides an anonymous summary of the experts' estimations and arguments from the previous round
- In the next round the experts are encouraged to revise their estimations considering the replies of the other members
- During such iterative process the group will converge towards an answer which is deemed correct
- The process is stopped after the pre-defined stop condition: number of rounds, achievement of consensus, stability of results, ...

Scenarios

- A basic process for all qualitative risk analysis mechanisms involves creation of scenarios
- A scenario is written description of a single major threat
- A description focuses on how a threat might occur and what effects it could have on
  - the organization
  - the IT infrastructure
  - specific assets
  - ...

Risk Matrices

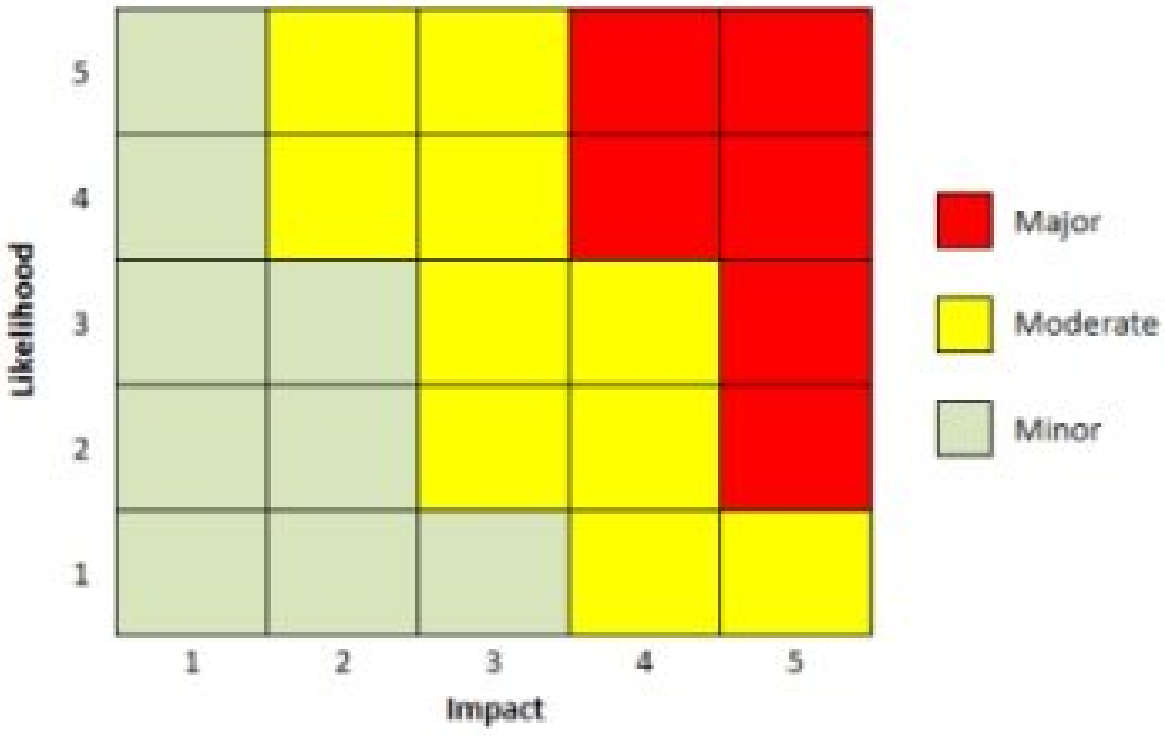
- Matrices depicting interrelations between various concepts contributing to risk
- in accordance with some risk taxonomy
  - US DoD, NASA, ISO, ...
  - Risk Taxonomy of The Open Group [1]
- Facilitate risk analysis – help estimate risk impact and likelihood
- Facilitate risk evaluation – help decide which risks require treatment, and which may be accepted

[1] `http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf`

Risk Matrices

For instance, the impact severity may be categorized as:

- Major
- Maoderate
- Minor



Impact could be also categorized into 4 categories.

For example: catastrophic, critical, marginal, negligible.

The Open Group Risk Taxonomy

http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

Factor Analysis of Information Risk

Risk = Loss Event Frequency $\times$ Probable Loss Magnitude

- LEF – a measure of likelihood, he occurrence, within a given timeframe, that a threat agent will inflict harm upon an asset.
- PLM – the likely outcome of a threat event, expected loss.

Factor Analysis of Information Risk

$$\text{LEF} = \text{Threat Event Frequency} \times \text{Vulnerability}$$

- TEF – the occurrence, within a given timeframe, that a threat agent will act against an asset.
- Vulnerability – the probability that an asset will be unable to resist the actions of a threat agent.

Factor Analysis of Information Risk

Vulnerability = Threat Capability / Control Strength

- Tcap – probable capability a threat agent is capable of applying against an asset, adversarial "strength".
- CS – the strength of a control as compared to a baseline measure of force.

Factor Analysis of Information Risk

Forms of loss:

- Productivity – the reduction in an organization's ability to generate its primary value.
- Response – expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, etc.).
- Replacement – the intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop, etc.).
- Fines and judgments (F/J) – legal or regulatory actions levied against an organization.

Factor Analysis of Information Risk

Forms of loss:

- Competitive advantage (CA) – losses associated with diminished competitive advantage. Within the commercial world, examples would include trade secrets, merger and acquisition plans, etc. Outside the commercial world, examples would include military secrets, secret alliances, etc.
- Reputation – losses associated with an external perception that an organization's leadership is incompetent, criminal, or unethical.

THANK YOU FOR YOUR ATTENTION

ANY QUESTIONS?