How to do Risk Assessments ?

Risk assessment is the process of identifying, analyzing, and evaluating risks. It aims to understand potential threats, their impact, and likelihood. ISO 31000 provides principles, a framework, and a process for managing risk.

ISO 31000 provides a solid foundation, but does not recommend any specific tool / model. Organizations can choose the most suitable model based on their specific needs and context

Key Steps

Identification: Structured process to recognize and record risks, assessing their impact on people, the environment, assets, or reputation.

Analysis: Examining risks in-depth, considering their causes, consequences, and likelihood.

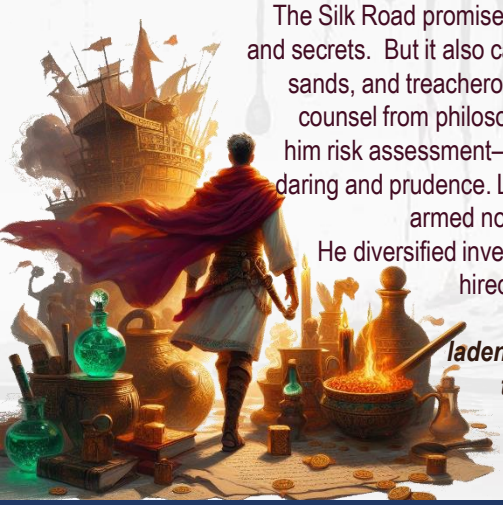
Evaluation: Determining the significance of risks and prioritizing them based on severity and probability.

Treatment: Developing strategies to mitigate, transfer, or accept risks.

Monitoring and Communication: Continuously tracking risks and sharing relevant information within the organization.

Remember Lucius when you stand at crossroads.

In ancient Rome, lived a merchant named Lucius. His eyes held the fire of adventure, and his ledger bore scars of countless voyages. His wealth grew from calculated risks—the kind that could fill coffers or leave him destitute. One day, a parchment arrived—a whisper from distant lands. The Silk Road promised untold riches: jade, spices, and secrets. But it also carried peril—bandits, shifting sands, and treacherous mountains. Lucius sought counsel from philosopher Marcus. Marcus taught him risk assessment—the delicate dance between daring and prudence. Lucius chose the Silk Road, armed not blindly but with knowledge. He diversified investments, insured cargo, and hired skilled guards. ***Years later, Lucius returned to Rome, laden with riches, in spite of all thefts, tactical losses, and Misfortunates on his way.***



Commonly Used Models/Frameworks for Risk Assessment:

Bowtie Analysis: Visual method that links causes, consequences, and controls to assess risk.

Failure Mode and Effects Analysis (FMEA): Systematic approach to identify and prioritize failure modes.

Hazard and Operability Study (HAZOP): Used for identifying hazards in process systems.

Event Tree Analysis (ETA): Evaluates potential outcomes of specific events.

Fault Tree Analysis (FTA): Analyzes system failures and their causes.

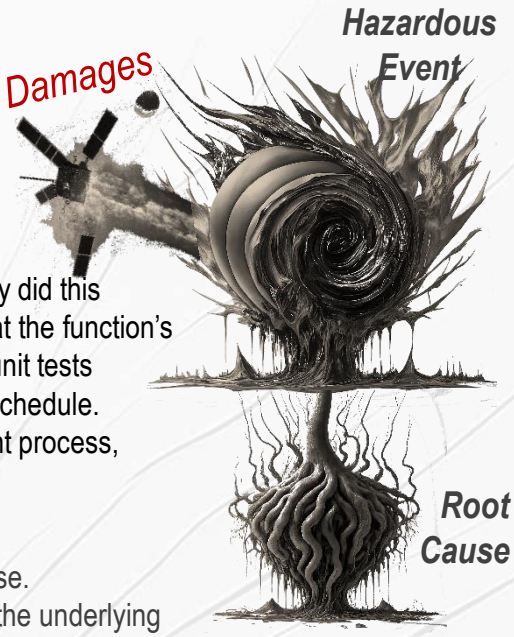
Quantitative Risk Assessment (QRA): Uses mathematical models to quantify risks.

Scenario Analysis: Examines various scenarios and their associated risks.

Monte Carlo Simulation: Generates multiple risk scenarios using random sampling.

SWIFT (Structured What-If Technique): Assesses risks through structured brainstorming.

Root Cause Analysis



Root Cause Analysis is a systematic approach used to identify the fundamental reasons behind a risk. For Example, imagine a critical bug occurs in the production system; Let's walk through the process.

(1) *Initial Investigation* (Proximate Cause): You discover that a specific function is causing the crash due to an unhandled edge case.

(2) *Digging Deeper* (Root Cause): Instead of stopping there, you ask: "Why did this function fail to handle the edge case?" You investigate further. You find that the function's original design lacked proper error handling. The lack of comprehensive unit tests allowed the bug to slip through because the team's rushed development schedule.

(3) *The real issue* lies not just in the function but in the overall development process, including design, testing, and code review practices.

Why Are Root Causes Often Hidden?

Real systems are intricate, making it challenging to pinpoint the exact cause.

Symptoms vs. Causes: Symptoms (like system crashes) are visible, but the underlying causes may remain hidden. Fixing symptoms without addressing root causes leads to recurring issues.

Blame Culture: Focusing on who made the mistake rather than why it happened can obscure the real causes.

Multiple Factors: Often, several factors contribute to risks. Identifying the primary one requires thorough investigation.

Time Pressure: In fast-paced development environments, teams may prioritize quick fixes over in-depth analysis

Hazardous Event

A hazardous event refers to any situation that leads to the creation of a hazard or worsens the impact of existing hazards. These events can result in bodily harm, injury, data breach, or financial damage.

For example: -

Slip and Fall: Imagine a worker slipping on an oil spill in the plant. The oil spill is a symptom, but the root cause might be a lack of effective mechanical integrity programs to prevent or detect leaks.

Chemical Spill: A sudden release of hazardous chemicals due to equipment failure or improper handling.

Power Outage: Interruption to the power supply can lead to safety risks, especially in critical systems.

Natural Disasters: Earthquakes, floods, or storms can cause significant damage and endanger lives.

Root causes are the fundamental behind incidents. There is a certain likelihood of occurrence of hazardous events if root cause exists.

What Are Damages?

The detrimental effects arising from hazardous events, impacting people, property, the environment, and other factors.

Risk Assessment and Damage Evaluation:

Identify potential hazards, analyze their potential impact, and quantify the resulting damages. Both Quantitative (i.e., *assigning monetary values to damages for cost-benefit analysis and resource allocation*) and Qualitative (*severity of damages e.g., minor, moderate, severe*) assessments are used.

Likelihood of Damages:

This analysis assesses the chance of damages after hazardous events occurring, often using historical data, expert judgment, and predictive models. Risk Score is a single numerical value derived from combining likelihood and severity, aiding in risk prioritization and decision-making.

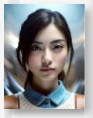
Risk Matrix is often employed that is a visual tool combining likelihood and severity to prioritize risks.

Do not forget about Indirect Damages:

Considering cascading effects beyond immediate impacts (e.g., a cyberattack disrupting operations causing financial losses and reputational damage). Similarly, intangible damages are worth considering in many industries, such as reputational harm, loss of trust, and psychological distress.

Conclusion

Risk assessment is not about avoiding risks, but about managing them. Root cause analysis is not about blaming others, but about learning from mistakes. Risk assessment is not a one-time event, but a continuous process.



Please refer to **Risk Assessment and Management** *by Dr Ian Messenger* to learn more about **f**undamentals of effective Risk Management.

Ji-Won (지원)