OptimaWell

Introductory Guide to Risk Management Systems For Asset Optimization

From OptimaWell Toolbox
(Toolboxes for Outperformers)

OptimaWell

José Luis Ortiz Volcán
Consultant & CEO OptimaWell

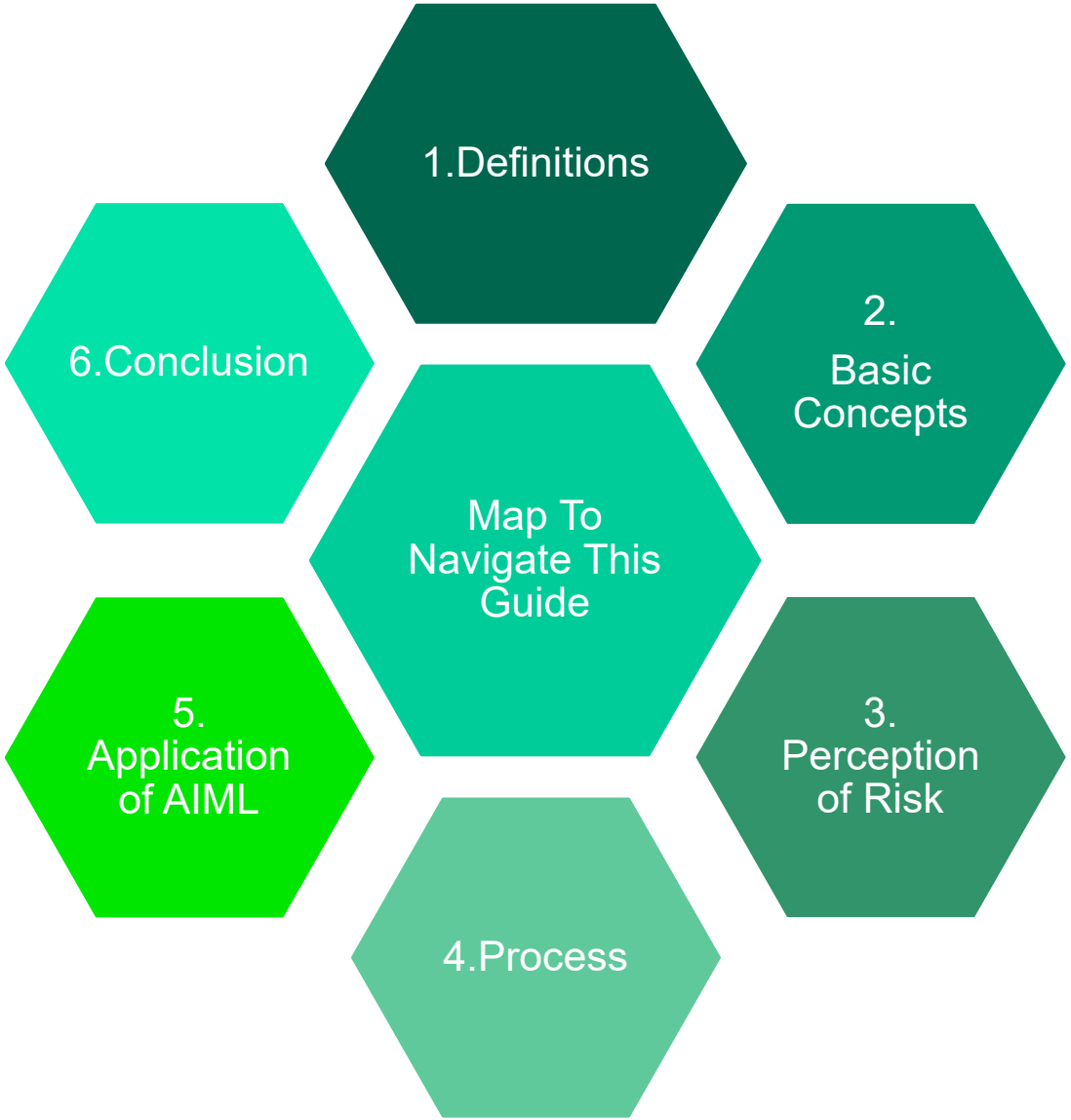
Purpose of this document

This introductory guide to risk management systems for asset optimization, lays the ground for understanding the analysis of risks, uncertainties and failures, and its practical application in projects and processes, during life cycle of assets from value identification to value realization.

Map To Navigate This Guide

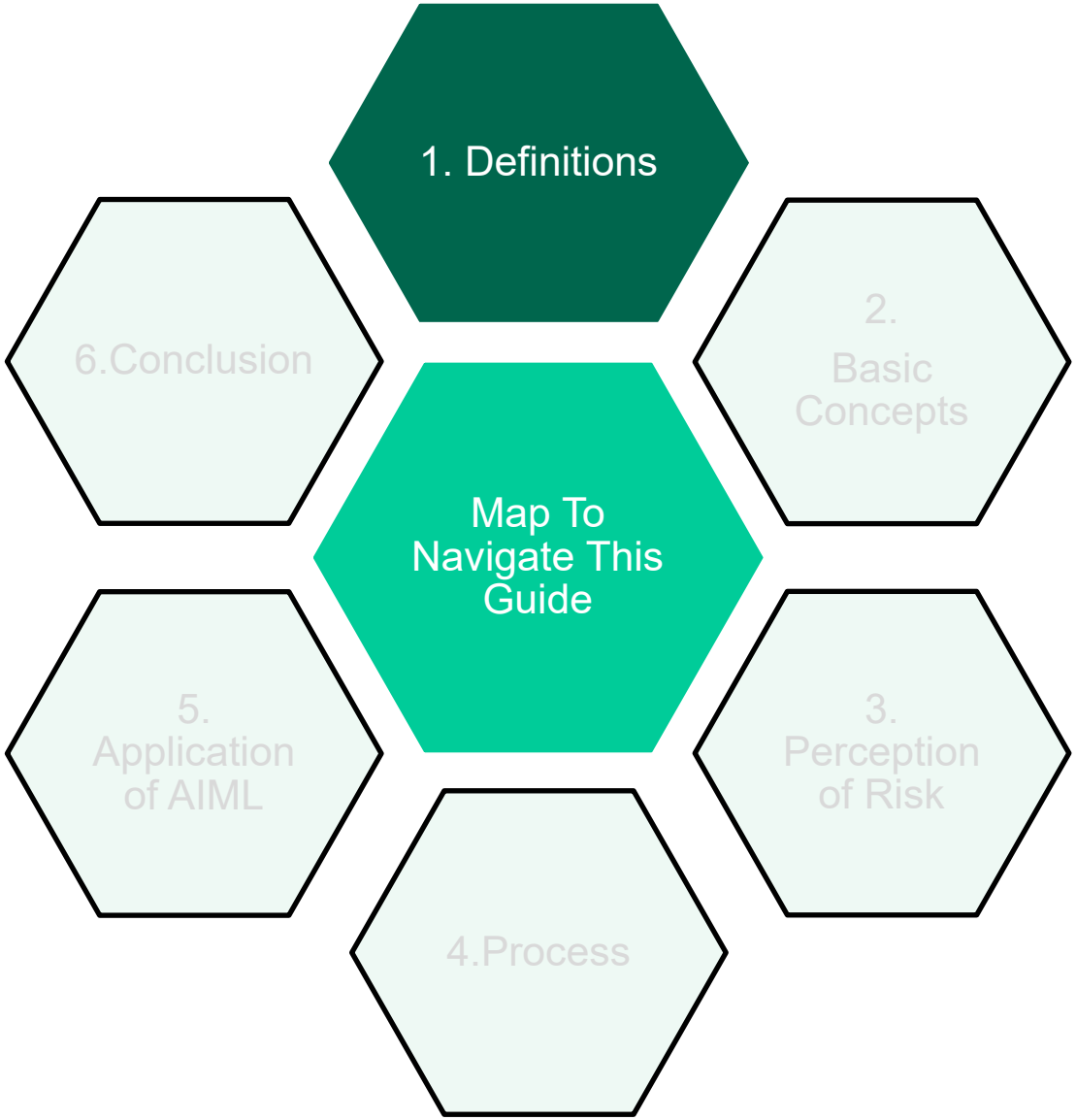
Map

Use The Links Above To Navigate



Click In Any Part of The Map To Navigate

Map To Navigate This Guide



1. Definitions

Definitions – Part 1 of 5

Asset – is a resource that has economic value, a life cycle and can be used to produce future benefits to its owner. Assets can be natural, physical and intellectual.

Asset Life Cycle – Sequence of stages or phases that assets undergo from value identification to value realization, i.e., from its creation, growth, development, maturity, decline until its end or termination.

System – a collection of interrelated and interconnected components or elements that work together to achieve a specific set of goals or objectives. These components can include tangible entities like physical objects, as well as intangible elements like processes, information, and relationships. Examples of systems include biological systems, computer software systems, infrastructure systems, ecosystems, supply chain business systems and a system of assets (natural and physical assets interacting as an integrated system).

Reliability of a System – In the context of systems, refers to the ability of a system to perform its intended function under specified conditions for a given period.

Failure – refers to the inability of a system, component, process or organization to meet its intended or expected function or performance. It encompasses a wide range of scenarios, from minor malfunctions to catastrophic breakdowns.

1. Definitions

Definitions – Part 2 of 5

Hazard – condition, substance, activity, or event with the potential to cause harm, injury, or adverse effects. It can be natural or caused by man. Hazards exist regardless of whether they pose an immediate threat or not.

Incident – unexpected event that disrupts normal activities, routine operations, or compromises the safety, security, or integrity of a system, organization, or individual. Not all incidents turn into accidents.

Accident – an unplanned, undesirable event that results in injury, damage, or loss that occurs due to hazards and the lack of adequate control or mitigation of associated risks.

Consequence – impacts or negative effects that may arise from a hazard, incident or accident. It also refers to the result of an event, action or decision.

Consequence Modeling – quantitative or qualitative assessment of the consequences of specific events, hazards, incidents or scenarios, to understand the magnitude and nature of potential damage or harm that may result from them.

Scenario – plausible sequence of events or circumstances that describe a potential situation or future state.

1. Definitions

Definitions – Part 3 of 5

Risk Analysis – systematic process of identification, assessment and evaluation of risks. It involves identifying hazards, analyzing their probability and consequences, and determining their level of risk, to support decision-making and risk mitigation strategies.

ESG – Environmental, Social and Corporate Governance (ESG) is a framework designed to be integrated into an organization's strategy to create business value by expanding organizational objectives to include the management of sustainability-related risks and opportunities with respect to the organization and interested parties, including, but not limited to customers, suppliers and employees, and the environment.

RAROC – Risk Adjusted Return on Capital (RAROC) is a financial measure to evaluate the profitability of an investment or a business activity considering the associated risks. Originally used by the banking and industrial sectors and adopted by numerous sectors.

1. Definitions

Definitions – Part 4 of 5

ISO 31000 – developed by the International Organization for Standardization (ISO) . Provides principles, framework, and process guidelines to manage risk effectively. Link: https://www.iso.org/publication/PUB100426.html

IEC 31010 – International Electrotechnical Commission (IEC) standard, complements ISO 31000 by providing guidance on risk assessment techniques. Covers various methods to identify, assess and treat risks. Link: https://www.internationalsos.com/

COSO ERM – the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the Enterprise Risk Management (ERM) framework. Offers a comprehensive approach to risk management across the organization, focusing on achieving strategic objectives. Link: https://www.coso.org/SitePages/Home.aspx

OHSAS 18001/ISO 45001 – these occupational health and safety management system standards require organizations to identify and manage risks related to safety and health in the workplace. Link: https://www.iso.org/news/ref2271.html

FAIR – (Factor Analysis of Information Risk) is a quantitative risk assessment model that provides a structured approach to assess and analyze information and cybersecurity risks. Link: https://www.fairinstitute.org/

1. Definitions

Definitions – Part 5 of 5

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG) - STANDARDS

Global Reporting Initiative (GRI) – Link: https://www.globalreporting.org/

Task Force on Climate-related Financial Disclosures (TCFD) – Link: https://www.fsb-tcfd.org/

Sustainability Accounting Standards Board (SASB) – Link: https://sasb.org/

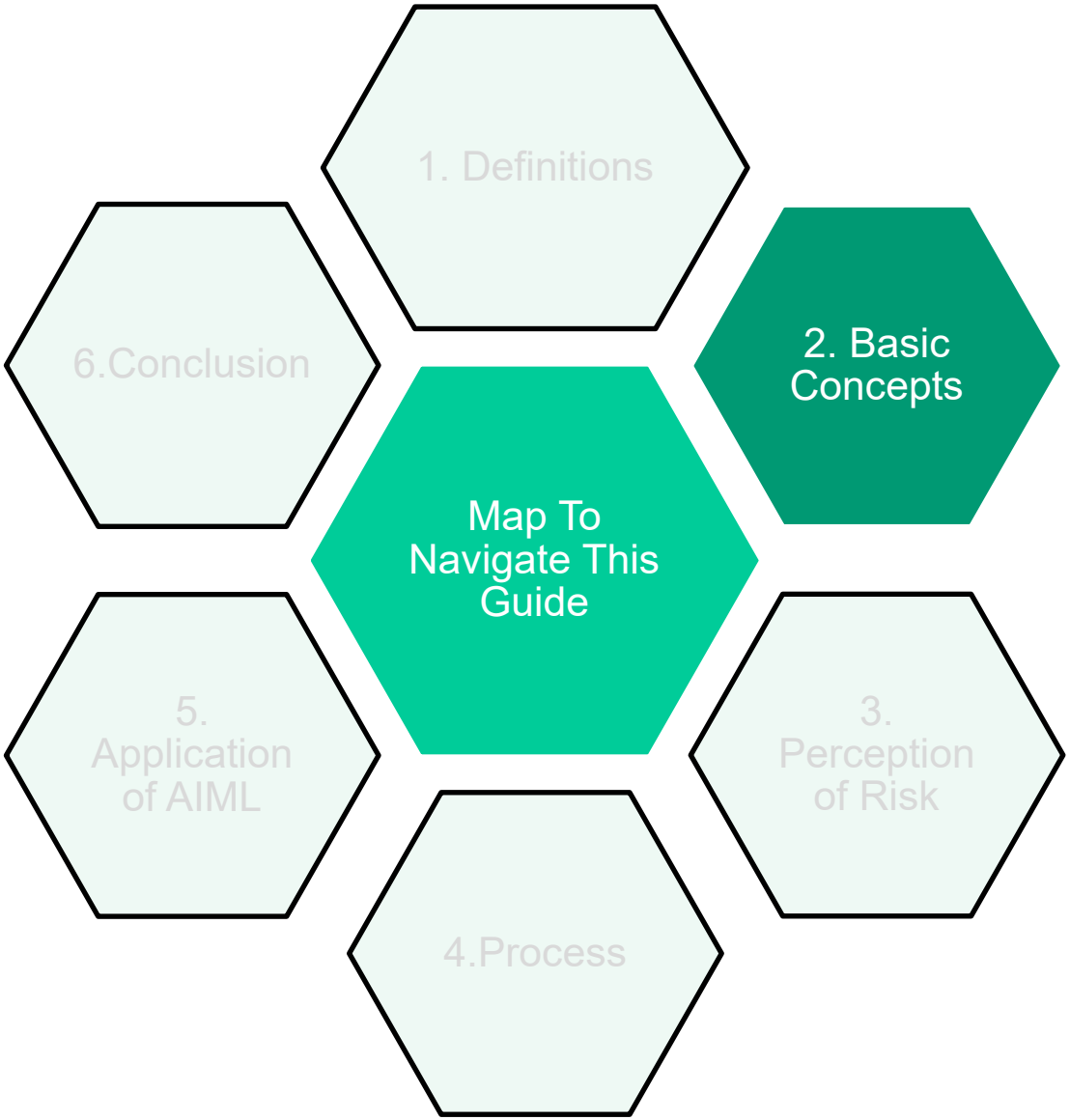
The International Integrated Reporting Framework (IIRC) – Link: https://www.integratedreporting.org/resource/international-ir-framework/

The Science Based Targets Initiative (SBTi) – Link: https://www.wri.org/initiatives/science-based-targets

Carbon Disclosure Project (CDP) – Link: https://www.cdp.net/en

The Climate Disclosure Standards Board (CDSB) - Link: https://www.cdsb.net/

Map To Navigate This Guide



2. Basic Concepts

Basic Concepts – Part 1 of 8

- Probability
- Uncertainty Vs. Risk - Examples
- Cone of Uncertainty, Precision and Accuracy
- Reliability
- Risk Components, Frequency, Consequence and Exposure
- Petroleum Asset Life Cycle: Maturation, Decisions and Challenges

Basic Concepts – Part 2 of 8

Probability

Blaise Pascal
1623-62

Pierre de Fermat
1607-65

Probability is the mathematical heart of risk theory and is defined as the study of the possibility of an event occurring.

The probability of an event occurring is obtained simply by dividing the number of ways the event can occur by the total number of possible occurrences.

Probability equal to 0 represents the impossibility of the occurrence of the event and probability equal to 1 represents the total certainty of the occurrence of the event. The numbers in between represent the chance of occurrence.

Basic Concepts – Part 3 of 8

Uncertainty vs. Risk

Frank Knight
1885-1972

Source: Frank Knight.: "Risk Uncertainty and Profit". 1921. ISBN 0486447758.

In 1921, Frank Knight in his famous dissertation "Risk, Uncertainty and Profit" distinguished between:

Risk, in which the probability of occurrence of an event and its consequences can be estimated,

vs.

Uncertainty, in which the probability of the occurrence of an event is unknown and cannot be estimated.

Basic Concepts – Part 4 of 8

Examples of Uncertainty and Risk Statements

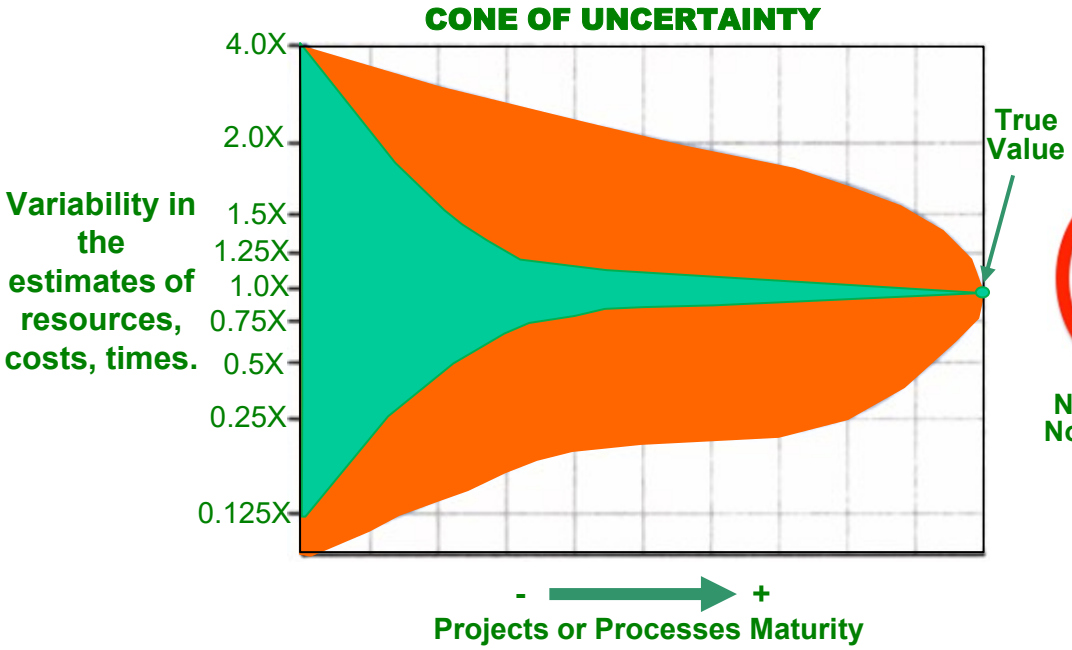
Example Statement of Uncertainty: There is a 60% chance that oil production will double in five years, a 30% chance that it will grow at a slower rate, and a 10% chance that it will decline in the same period.

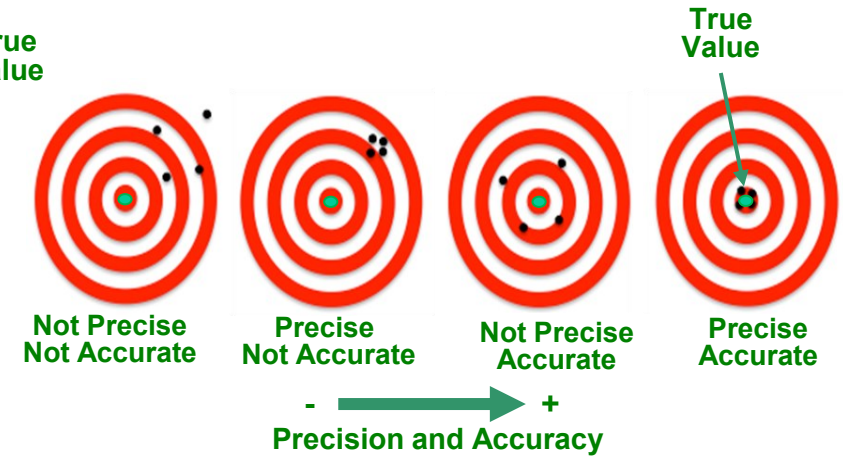
Example Statement of Risk: There is a 40% chance that the proposed oil well will be "dry" at a loss of $12 million in exploratory drilling costs.

2. Basic Concepts

Basic Concepts – Part 5 of 8

Cone of Uncertainty, Precision and Accuracy





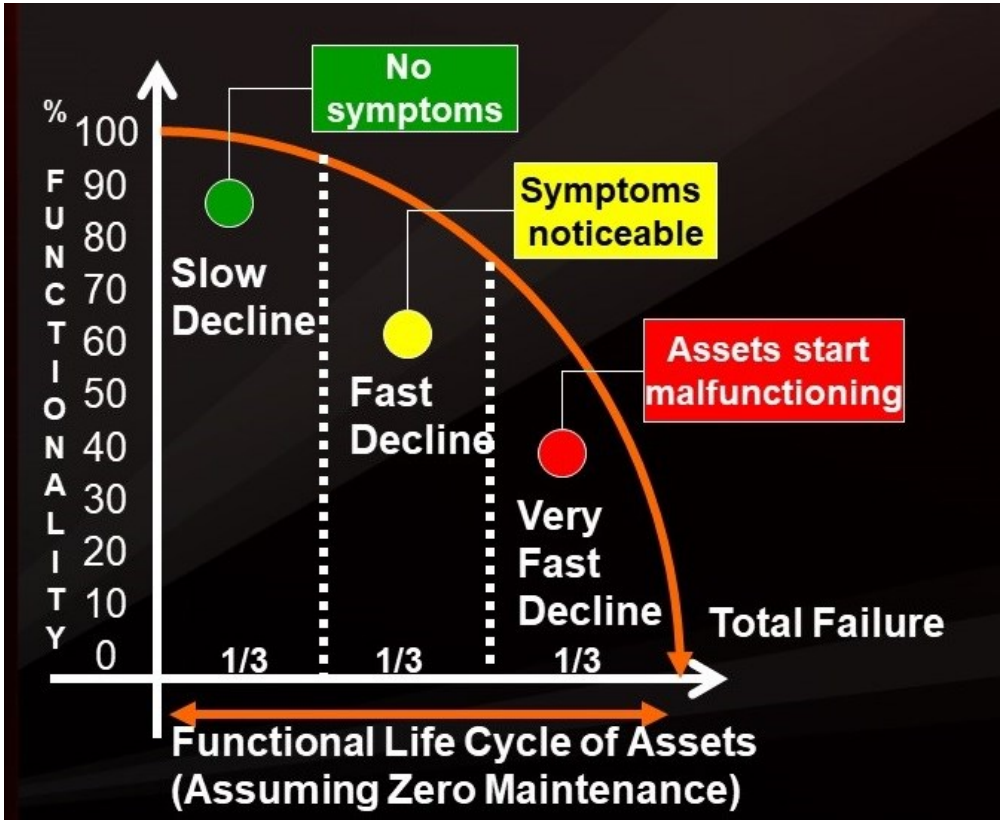
It is necessary to assess the maturity of projects or processes

2. Basic Concepts

Basic Concepts – Part 6 of 8

Reliability

- Reliability is the probability that a system will complete a given period without failure, performing the function for which it was designed.
- Reliability allows predicting failures related to the age (in the life cycle) of a system for which its architecture and the reliability of its components are known.
- Reliability was initially developed to describe failure and aging of complex military systems and has been successfully applied to world-class petroleum asset systems.

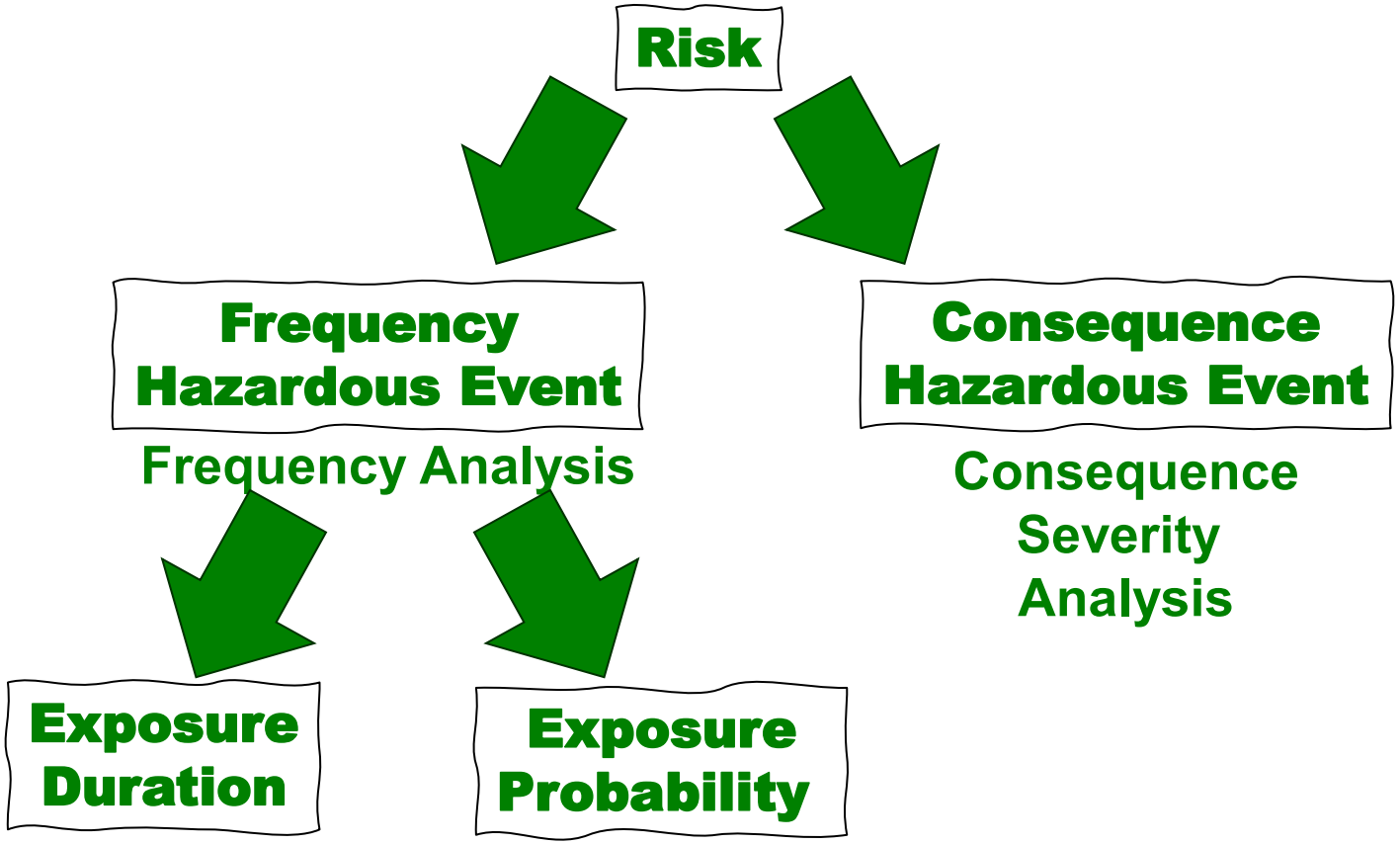


Source: Adapted from KC Leong, 2004 – The Essence of Asset Management- A Guide – UNDP Malaysia, EAROPH & APIGAM

2. Basic Concepts

Basic Concepts – Part 7 of 8

Risk Components

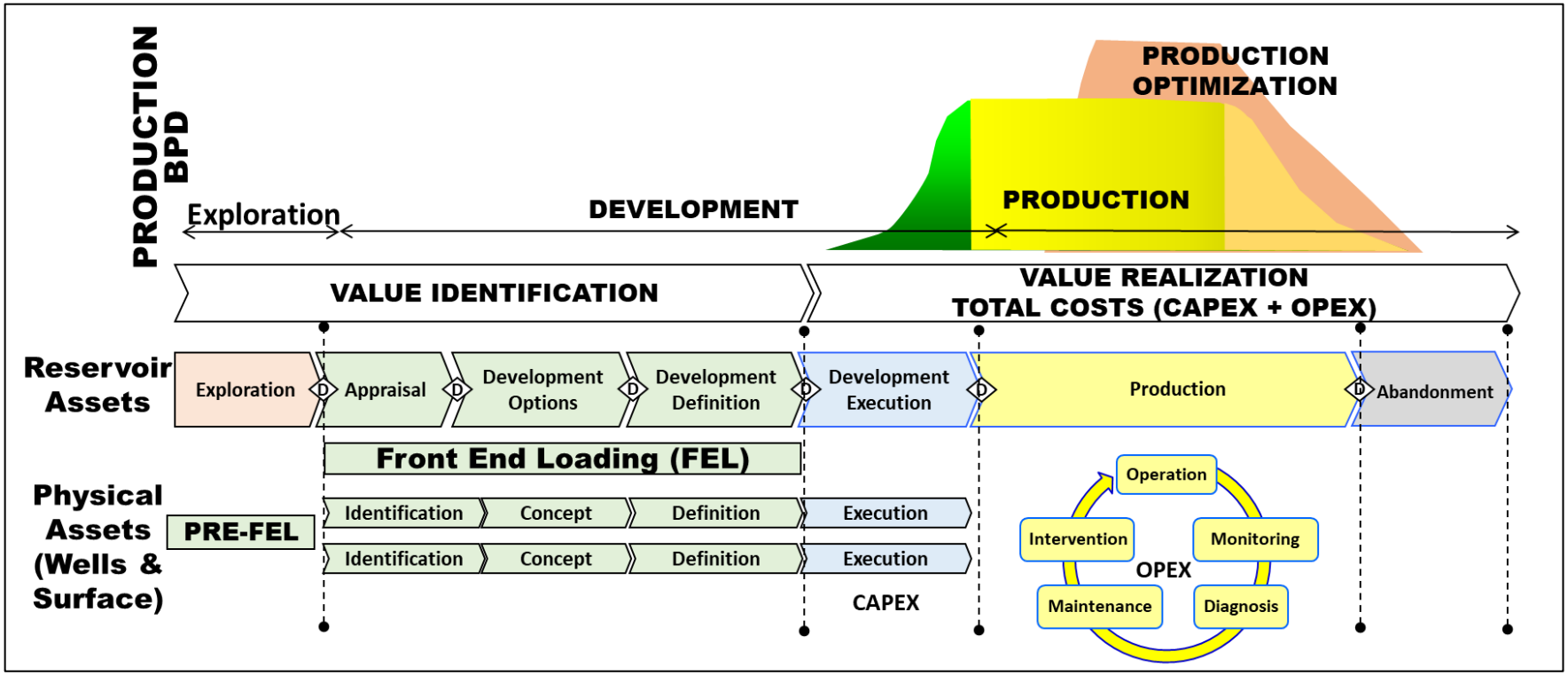


"there is a 10% probability that the hazardous event will occur within the 10-hour duration"

2. Basic Concepts

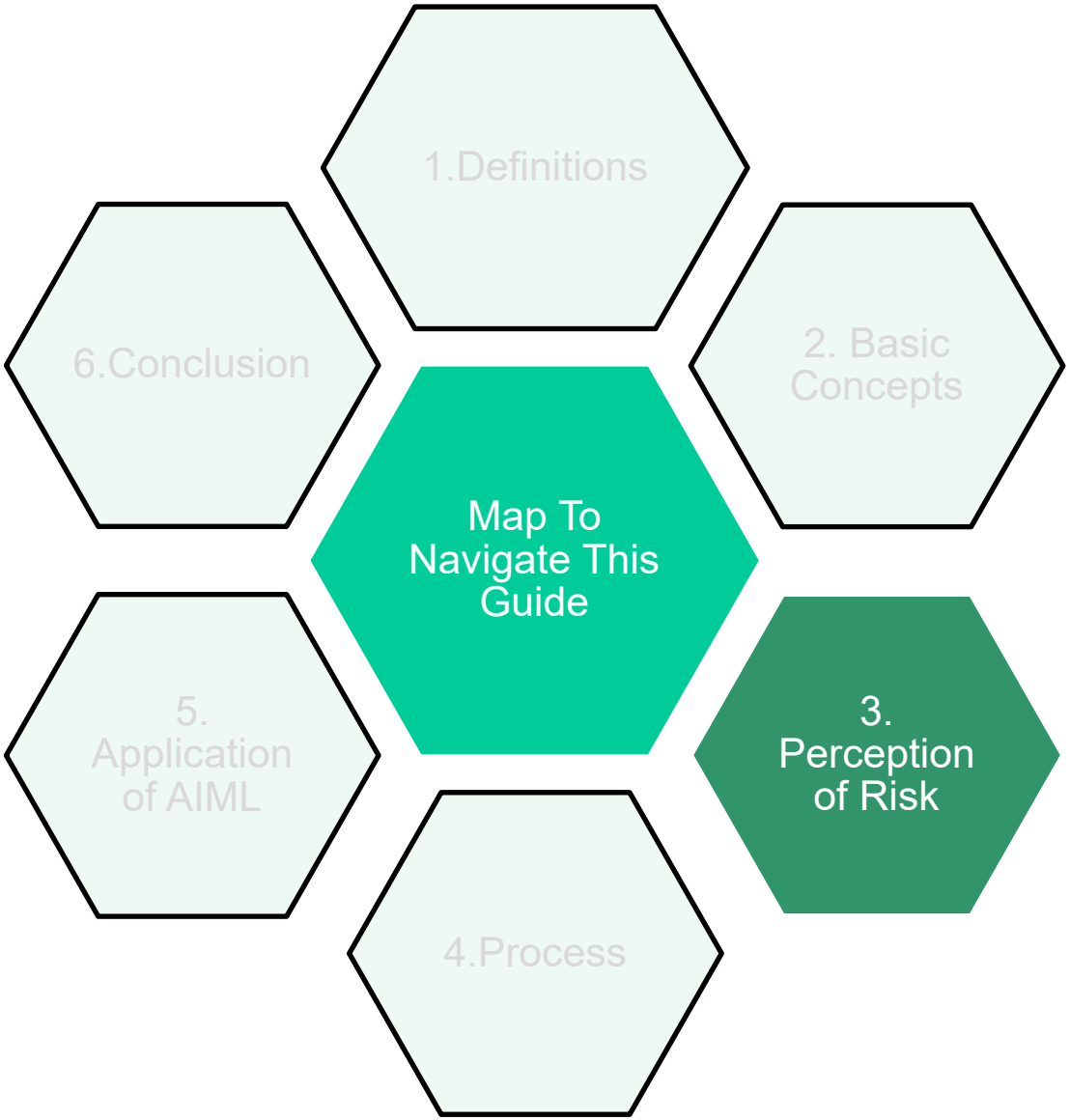
Basic Concepts – Part 8 of 8

Petroleum Asset Life Cycle From Value Identification to Value Realization



Source: J.L. Ortiz-Volcan, K. Ahmed, S. Azim, Y. Issa, R. Pandit, A.K. Al-Jasmi, M.O. Hassan, A. Sanyal, Kuwait Oil Company, S. Taduri, Kuwait Gulf Oil Company.:" Opportunity Assessment of A Deep Extra Heavy Oil Green Field: Scenarios for Life Cycle Cost Optimization under Uncertainty and Risk". Paper SPE-193675-MS.

Map To Navigate This Guide



3. Perception of Risk (Part 1 of 3)

- The perception of risk has several elements that we must understand in order to analyze uncertainties and risks. One of these elements is the biological mechanism programmed by evolution into our DNA, to be alert and to react to what is perceived as threats or dangers, keeping in mind that not all threats are dangers, but all dangers are threats. It is a basic survival mechanism that was especially useful in prehistoric times when the threat of physical danger loomed.
- This mechanism is our amygdala which is a threat detection instrument and is one of the most primitive parts of our brain that is constantly monitoring our environment to assess our level of security and alert us to any signs of threat, danger or risk.
- Because of the way our brains are wired, the amygdala often bypasses the prefrontal cortex, the newest part of our brain, quickly alerting the body to danger. This is how the amygdala takes control of our body and makes us go into action even before we realize what is happening.

Source: Adapted from : **https://www.cfcliving.com/brain-threat-detector/**

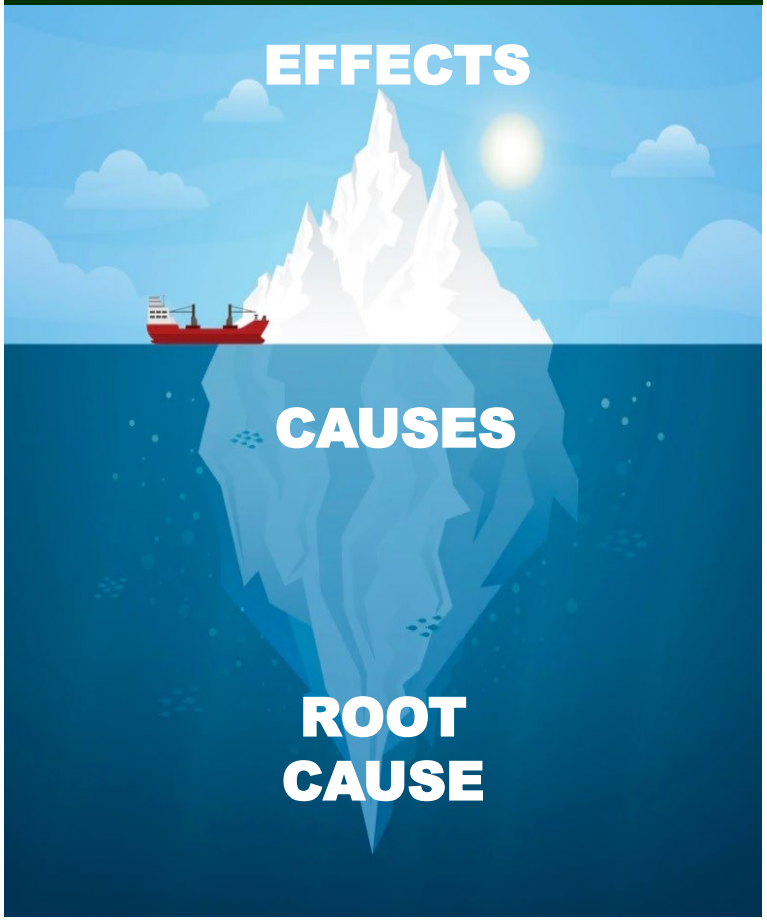
3. Perception of Risk (Part 2 of 3)

HAZARDS

- What we know
- What we know that we don't know

- What we don’t know that we know
- What we don’t know we don’t know

The Uncertainty Iceberg



EVENTS

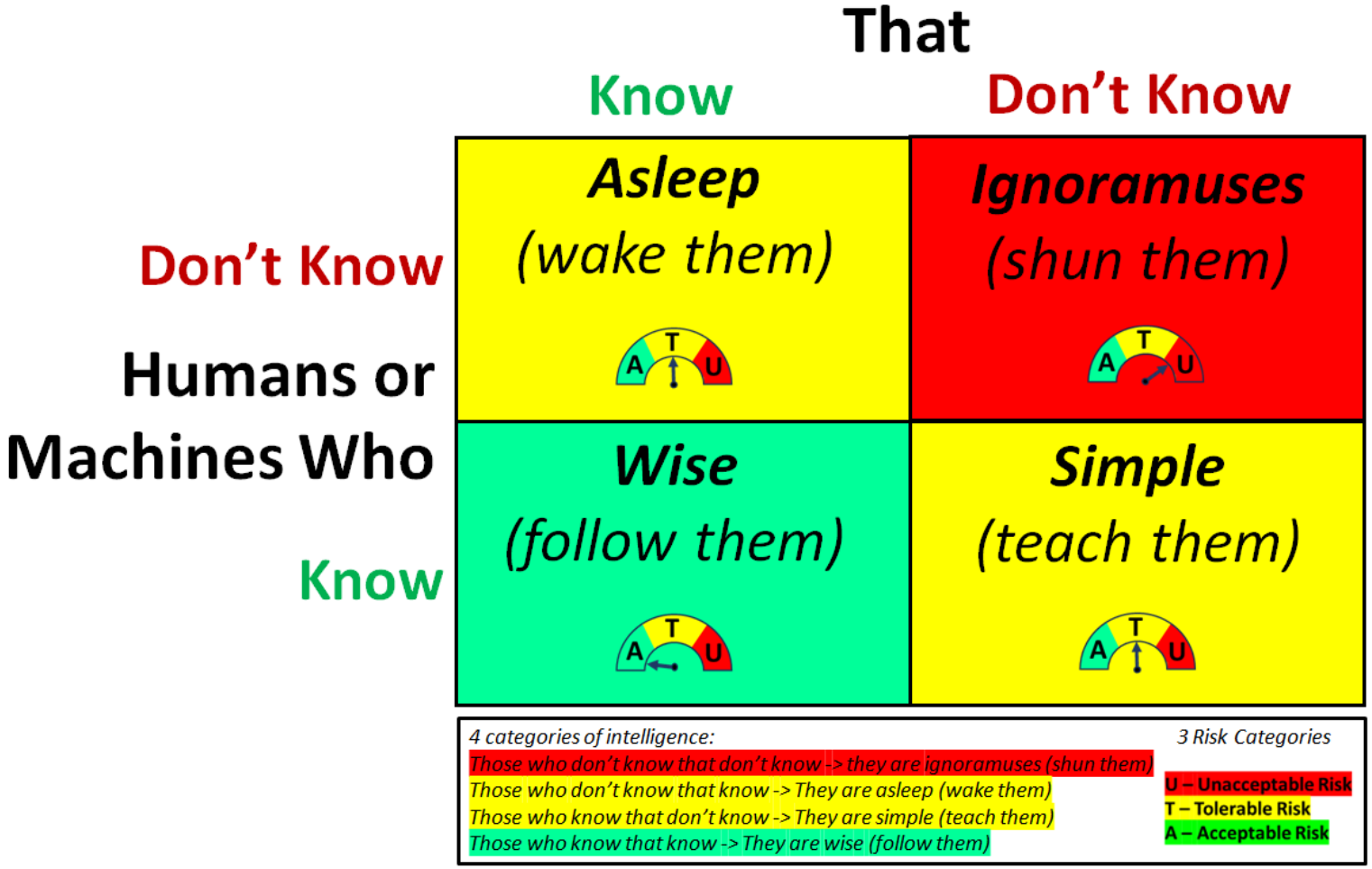
“What we see that can happen”

“What we do not see what can happen”

Iceberg Image by freepik - https://www.freepik.com

3. Perception of Risk (Part 3 of 3)

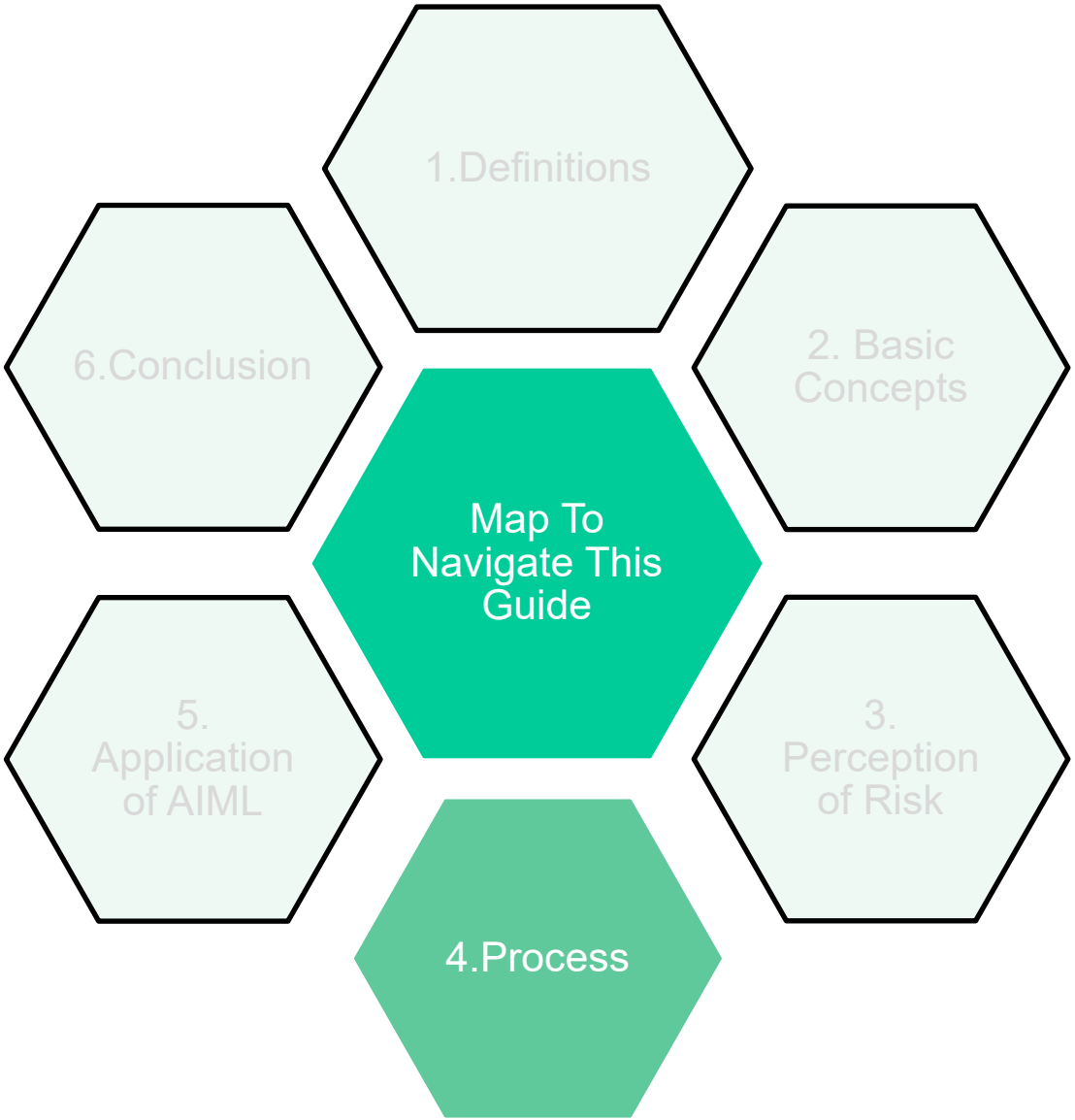
Intelligence – Risk Matrix Metaphor



Adapted by OptimaWell from Arabian Proverb and Risk Assessment Matrix

Link: https://www.linkedin.com/feed/update/urn:li:activity:7081517762379952128/

Map To Navigate This Guide



4. Process

Risk Management System Mission

Safeguard organizations, their stakeholders, their resources, assets, and income by identifying, assessing and mitigating potential risks.

This is achieved by implementing strategies to minimize the likelihood and impact of adverse events, maintaining financial stability, and ultimately creating a resilient environment where uncertainties are proactively managed, enabling the organization to navigate challenges and seize opportunities.

4. Process

Risk Baseline Assessment

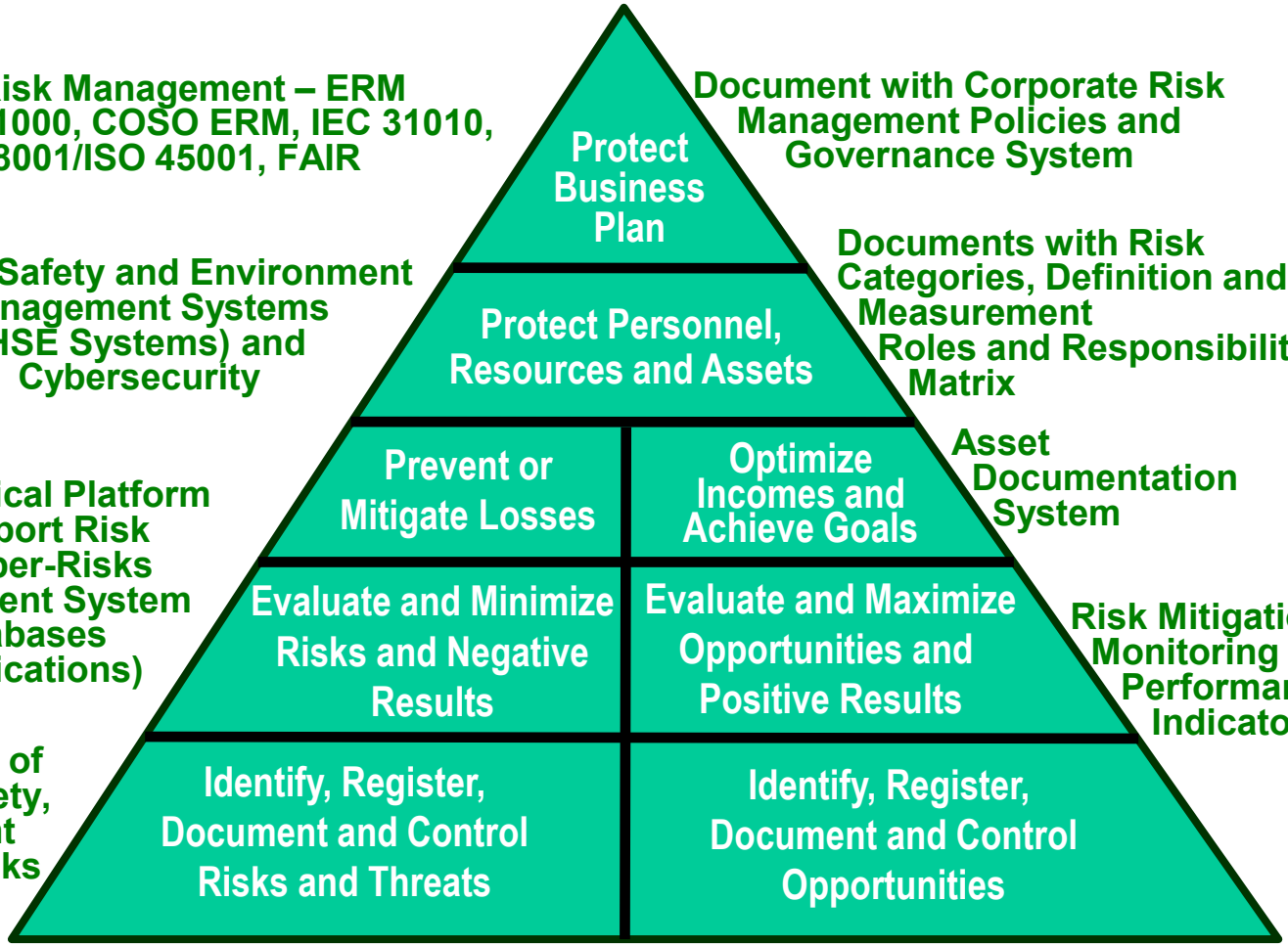
- Each organization or asset unit must establish which are the greatest or most important risks.
- Define the priorities and the program to control the risks.
- If the risks are not known, a general evaluation must be carried out that allows the organization or asset unit to initiate more in-depth and detailed studies.
- General evaluations must be updated every year or two, incorporating the results of more in-depth or detailed studies.
- The organization has the responsibility to apply the best practices of Cybersecurity, to protect equipment, networks, software applications, critical systems and data from possible digital threats.

Evaluation by Key Themes

- Changing circumstances, or specific needs may require separate risk assessment studies.
- Key issues are usually associated with a system that requires change management; some examples are:
  - A new technology, machinery, or plant is introduced into an existing system that changes current operations.
  - Immediately after an accident that came close to disaster.
  - New knowledge becomes available and produces information that can influence known risk levels.

4. Process

Risk Management Pyramid



Enterprise Risk Management – ERM
Standards: ISO 31000, COSO ERM, IEC 31010, OHSAS 18001/ISO 45001, FAIR

Document with Corporate Risk Management Policies and Governance System

Health, Safety and Environment Management Systems (HSE Systems) and Cybersecurity

Documents with Risk Categories, Definition and Measurement
Roles and Responsibilities Matrix

Technological Platform To Support Risk and Cyber-Risks management System (Databases & Applications)

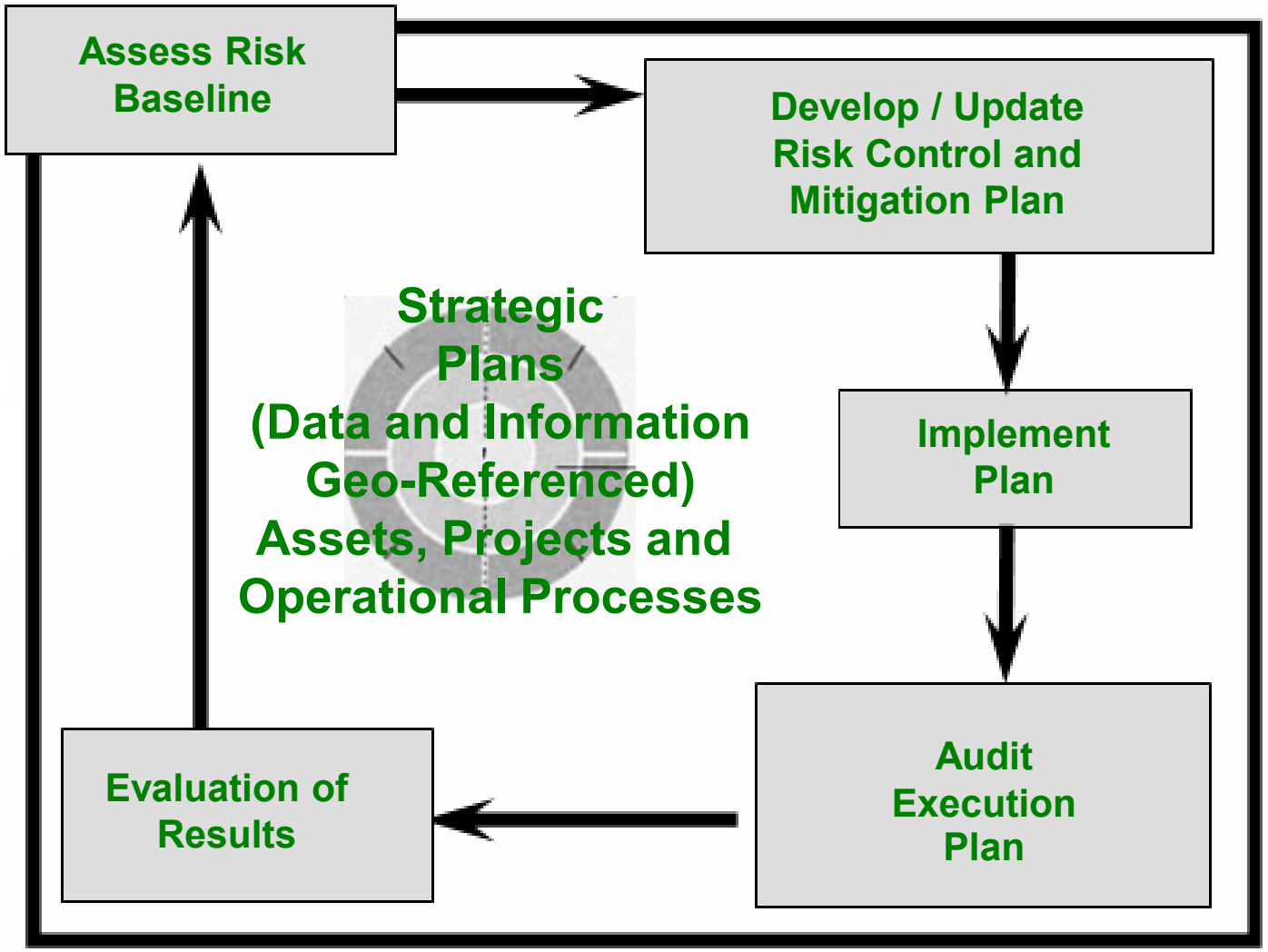
Asset Documentation System

Risk Register of of Health, Safety, Environment and Cyber-risks

Risk Mitigation Monitoring and Performance Indicators

4. Process

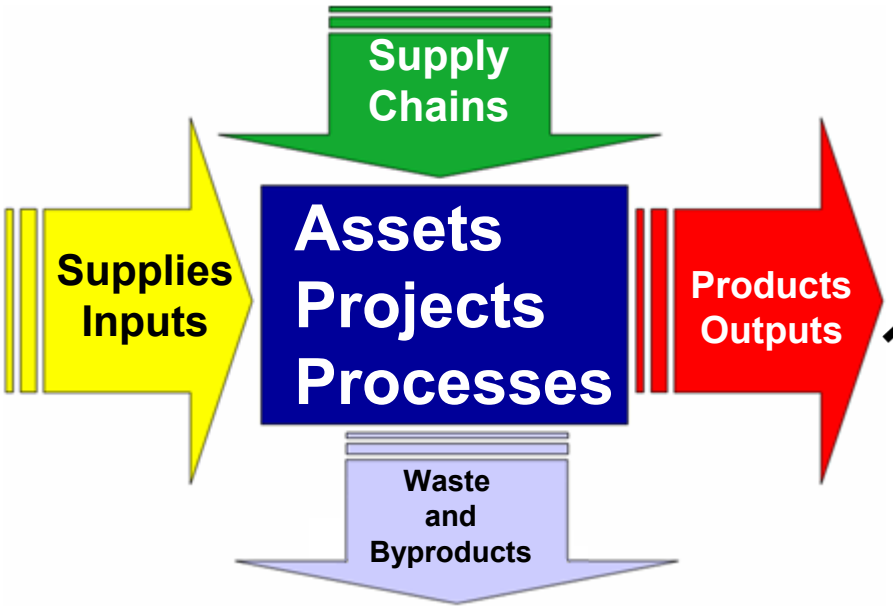
Strategic Framework

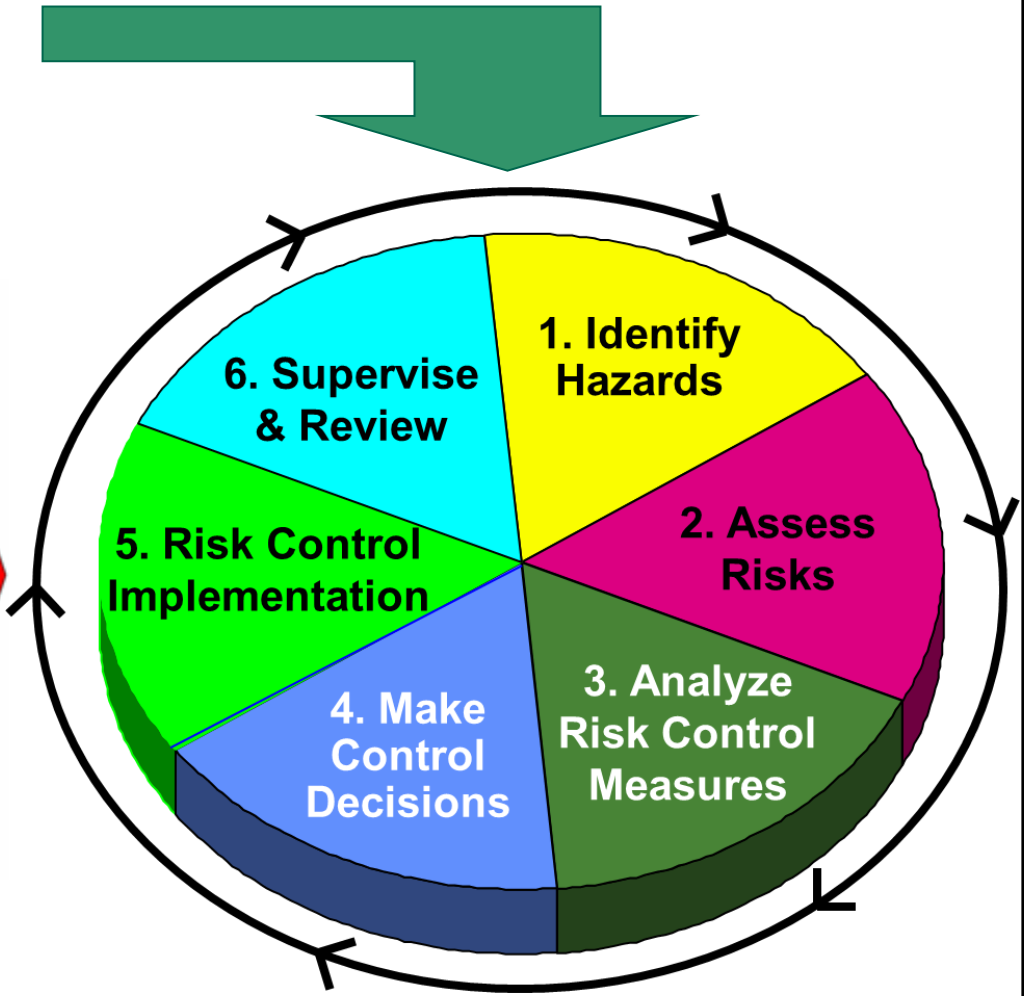


4. Process

General Methodological Framework

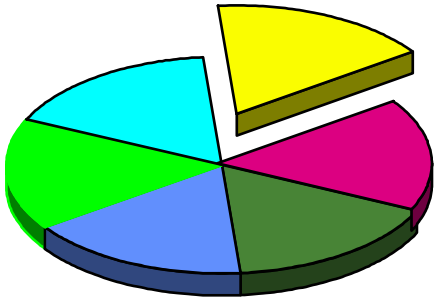
For Every Asset, Project and Process





General Methodological Framework

Step 1 of 6. Identify, Classify Hazards and Analyze Risks

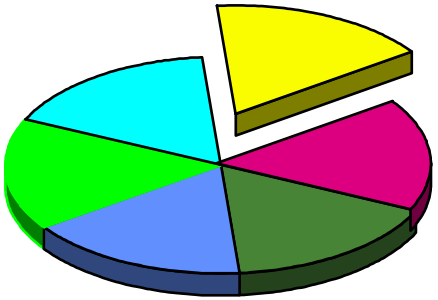


- Process: Apply procedures and techniques to analyze the sources that generate hazards. These procedures and techniques add rigor and allow for early identification. For Assets, a recommended technique is the Integration Workshop with 3 parts (Divergent, Systemic and Convergent Thinking).

- Output: Significant number of identified risk sources, Options and Scenarios/Actions to Address Risks and Uncertainties.

General Methodological Framework

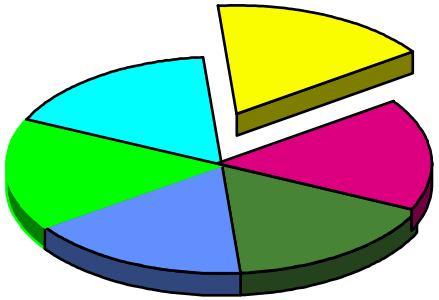
Step 1 of 6. Identify, Classify Hazards and Analyze Risks



- Run an integration workshop, a value enhancing practice to support decision making, by identifying challenges, level of definition, complexity, completeness and resources for existing value creation strategy and plan.
- Identify what can go wrong or what opportunities can be missed by events and use credible scenarios to describe those events by identifying the hazards.
  - Describe each scenario on a piece of paper and group the hazards by classifying them according to their perspective (asset, project or process).
  - Share your scenarios on a flip chart.
- Consider for each event the frequency, consequences, and assign a severity to the consequences using the definitions used in the risk ranking matrix (RAM – Risk Assessment Matrix).
- Estimate the probability that such consequences can materialize within the company and its units of assets and locate that risk in the RAM matrix.

General Methodological Framework

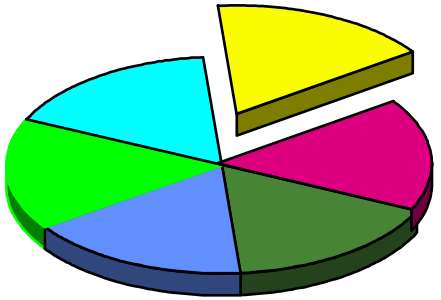
Step 1 of 6. Some Tools to Identify Hazards and Analyze Risks

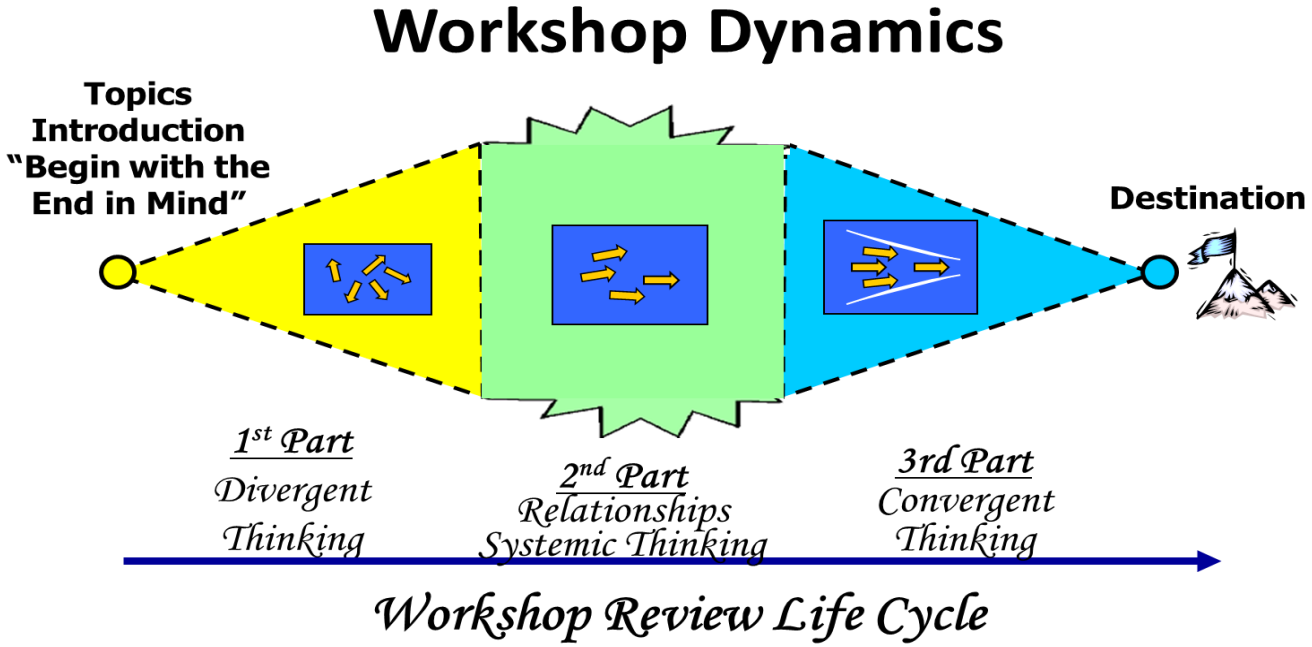


- Bow-Tie
- SCHIRP (Structured, Comprehensive Hazard Identification and Risk Profiling)
- HAZOP (Hazard and Operability Studies)
- HAZID (Hazard Identification)
- FMEA (Failure Mode and Effect Analysis)
- FTA (Fault Tree Analysis)
- What if / Cause and Effect / Causal Chains
- Integration Workshop for Identification of Challenges for Value Creation (Uncertainties, Risks, Opportunities, Issues), Decisions, Options & Scenarios
- Operational Processes Analysis – Flow Diagrams - Logic Diagrams
- Inspections to Establish Physical Conditions of Critical Parts
- Accident Investigation Reports
- Analysis of Critical Tasks

General Methodological Framework

Step 1 of 6. Some Tools to Identify Hazards and Analyze Risks – Integration Workshop

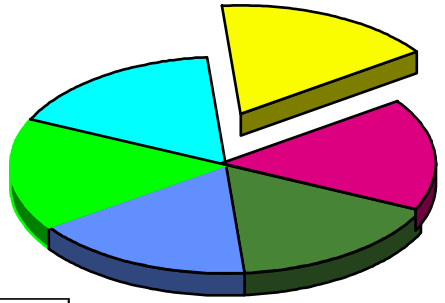


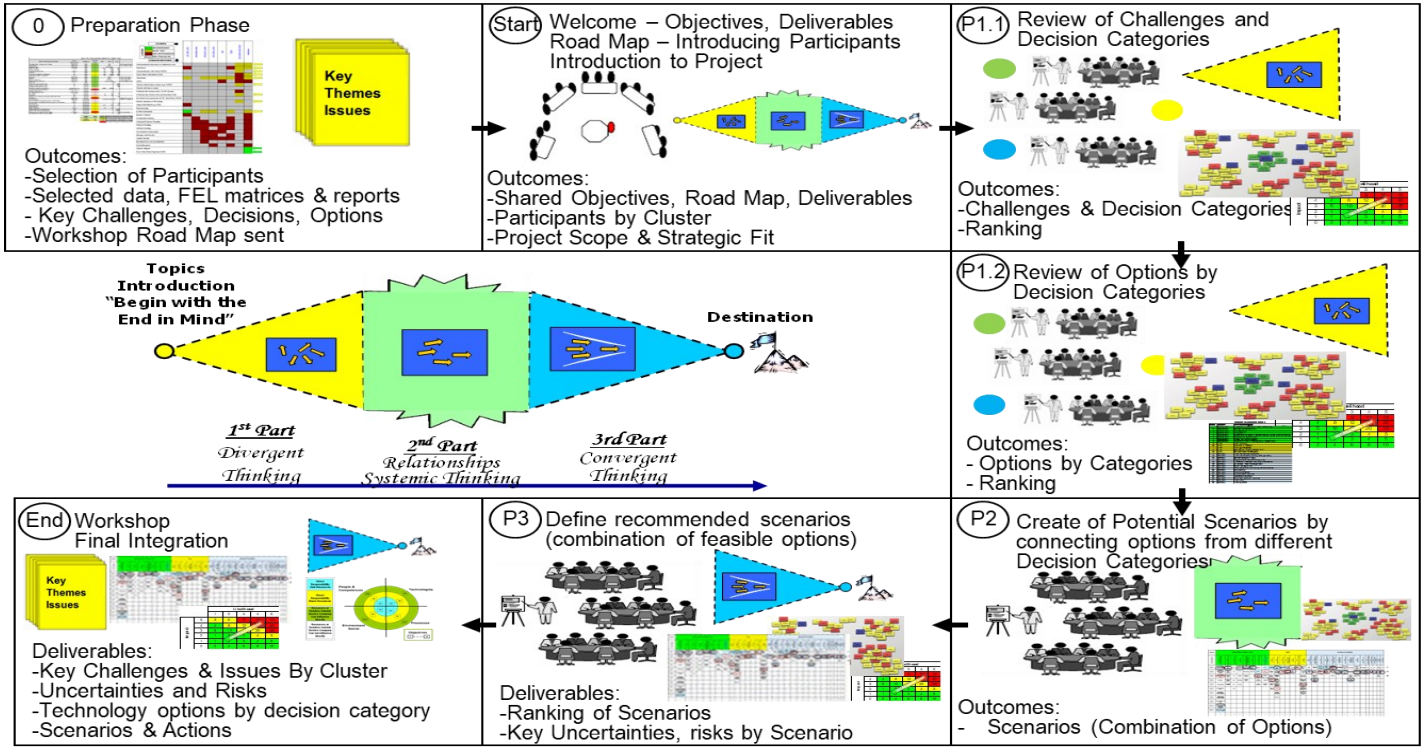


4. Process

General Methodological Framework

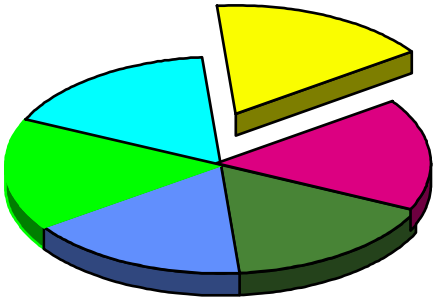
Step 1 of 6. Some Tools to Identify Hazards and Analyze Risks – Integration Workshop





General Methodological Framework

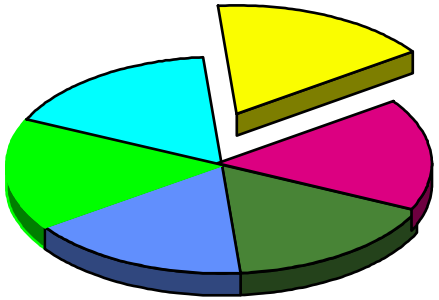
Step 1 of 6. Some Public Risk Databases



- **FACTS** (Failure and Accidents Technical information System): created in Norway, it contains information on more than 25,700 (industrial) accidents (incidents) involving hazardous materials or dangerous goods that have happened all over the world during the past 90 years. Link: http://www.factsonline.nl/
- **AIID** (Artificial Intelligence Incident Database): dedicated to indexing the collective history of harms or near harms realized in the real world by the deployment of artificial intelligence systems. Link: https://incidentdatabase.ai/
- **CBS** (U.S. Chemical Safety Board): Created in 1990 as an independent, nonregulatory federal agency that investigates the root causes of major chemical incidents. Link: https://www.csb.gov/
- **FOG** (Fatalities in Oil and Gas Extraction): The National Institute for Occupational Safety and Health (NIOSH) database that collects detailed information about worker fatalities in the U.S. oil and gas extraction industry. Link: https://www.cdc.gov/niosh/topics/fog/default.html
- **SINTEF** (Selskapet For Industriell og Tecknisk Forsking) – Report No. STF50 F06112. – The Foundation for Scientific and Industrial Research at the Norwegian Institute of Technology Referenced in OGP Report No. 434-2, "Blowout Frequencies", Oil & Gas Producers, London (UK), March 2010
- **OREDA** (Offshore Reliability Data): A comprehensive databank of reliability data collected on Topside (and Subsea) equipment from offshore and onshore operations in the North Sea, GOM, WOS, Angola, Adriatic, Caspian, etc. Link: https://www.oreda.com/
- **NTSB** (National Transportation Safety Board) - civil aviation accidents and selected incidents within US and international waters since 1962. Link: https://www.ntsb.gov/Pages/AviationQuery.aspx

General Methodological Framework

Step 1 of 6. Examples of Events in the Oil Sector, with Lessons Learned from Accidents and Failures



Norway

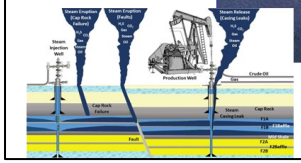
Lessons Learned: Alexander Kielland Platform – Norwegian North Sea, 1980
123 workers killed

United Kingdom

Lessons Learned: Piper Alpha Platform – UK North Sea, 1988
167 workers killed

Canada and Indonesia

Lessons Learned: Impact of Heavy Oil Blowouts - Steam Eruption, Duri Steamflood, Indonesia,1999 - Bitumen Blowout Alberta Tar Sands, Canada, 2013

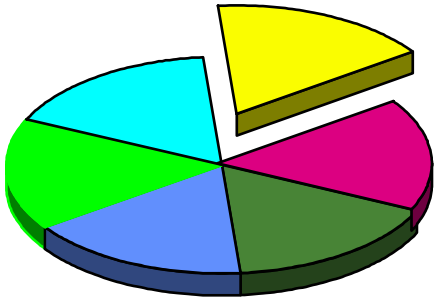


United States (Gulf Of Mexico)

Lessons Learned: Understanding Root Causes of Failure Modes Deepwater Horizon Oil Spill, 2010: One of the worst environmental disasters in US history

General Methodological Framework

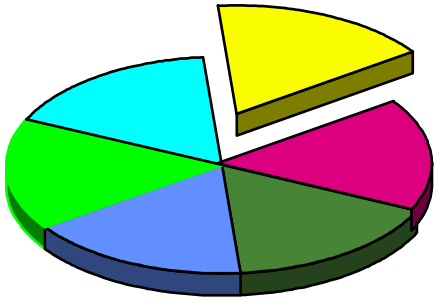
Step 1 of 6. Example with Blowouts Statistics comparing conventional vs. heavy oils



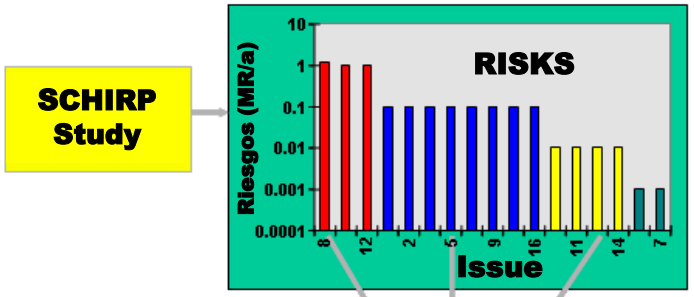
Legend	Source	Country	Period of Time	Number of Wells Or Operations	Type of Oil - Type of Operations At Time Of Blowout	Number of Occurrences
HO1	Alberta Energy and Utilities Board (EUB)	Canada	1975 to 1990	87,944	Heavy Oil - All types	96
HO2	Alberta Energy and Utilities Board (EUB)	Canada	2002 to 2006	88,856	Heavy Oil - All types	39
HO3	Lawrence Berkeley National Laboratory	USA (California)	1994 to 2003	78,100	Heavy Oil - All types	37
HO4	Lawrence Berkeley National Laboratory	USA (California)	1994 to 2003	45,000	Heavy Oil - Thermal	18
HO5	Lawrence Berkeley National Laboratory	USA (California)	1994 to 2003	33,000	Heavy Oil - Non Thermal	19
HO6	Pacific RIM Drilling - Chevron	Indonesia (Duri)	1999 to 2003	7,000	Heavy Oil - Steamflood	4
CO1	SINTEF Offshore Blowout Database	GoM,UKCS,Norway	1980 to 2005	211,142	Conventional Oil - Production	7
CO2	SINTEF Offshore Blowout Database	GoM,UKCS,Norway	1980 to 2005	22,833	Conventional Oil - Drilling	8

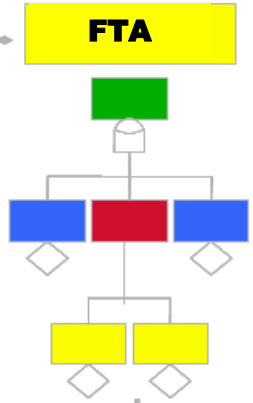
Fuente: **Paper SPE-175376. SPE Kuwait Oil and Gas Show and Conference. Link: https://doi.org/10.2118/175376-MS**

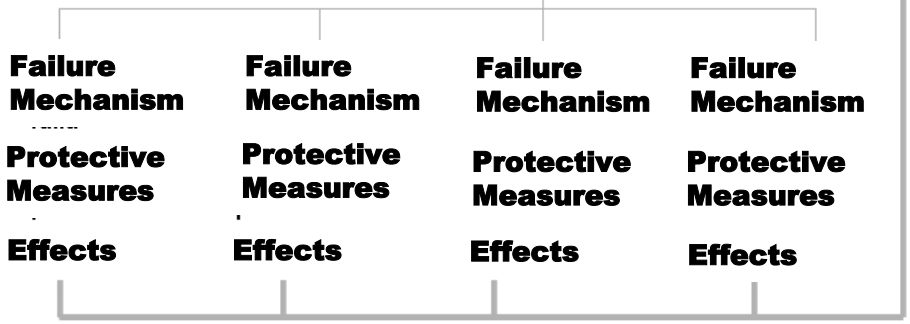
General Methodological Framework

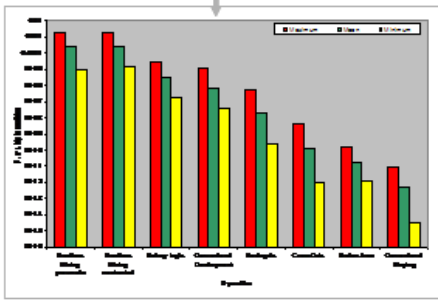


Step 1 of 6. Example with Some Tools to Identify Hazards and Analyze Risks



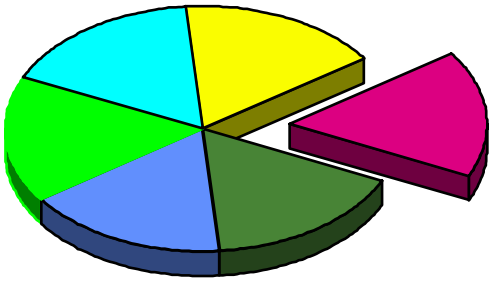


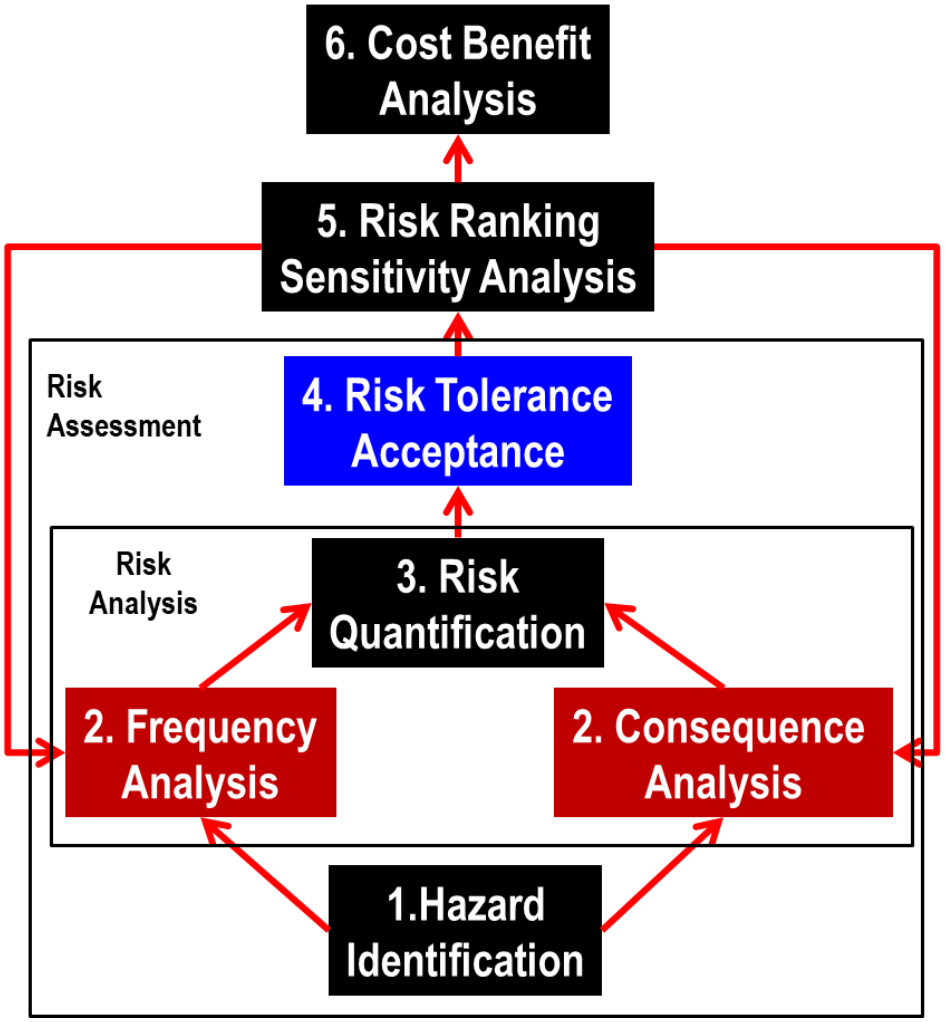




General Methodological Framework

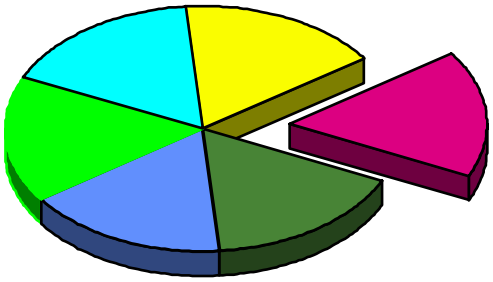
Step 2 of 6. Assess Risks





General Methodological Framework

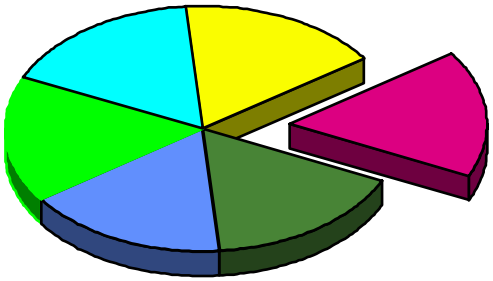
Step 2 of 6. Assess Risks



- Process: All hazards are evaluated based on their total impact on the mission of the project, process or activity under analysis. Root causes are determined, and risk values assigned:
  - Qualitative: Extreme High (EH), High (H), Medium (M), Low (L)
  - Quantitative: Scale from 1-20
- Output: Prioritization of the most important risks

General Methodological Framework

Step 2 of 6. Assess Risks

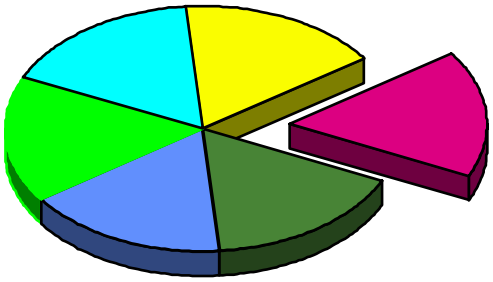


Risk Measurements / Quantification

- Qualitative
  - Exceptional, low, medium, high, continuous.
  - Acceptable, tolerable, unacceptable
  - Frequent, many, few
- Quantitative
  - 1 x 10^{-6}/Year
  - 5/1000000 kilometers
- Risk Ranking Matrix
  - Frequency and Severity Index, range 1 to 5
  - Risk Index
- Risk Indices
  - R10m Many fatalities
  - R1m One fatality
  - R0,5m Very serious disabilities

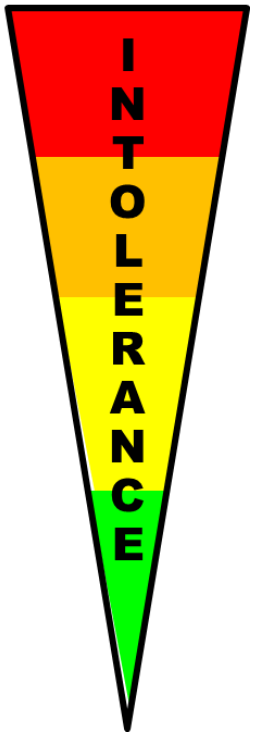
General Methodological Framework

Step 2 of 6. Assess Risks



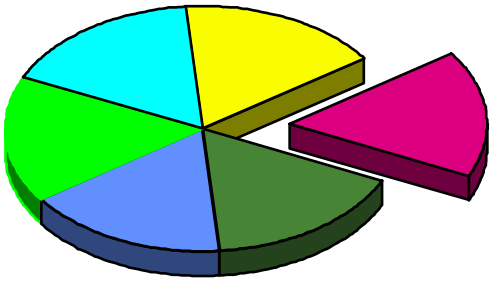
Simple Ranking

HIGH Consequence	HIGH Frequency
HIGH Consequence	LOW Frequency
LOW Consequence	HIGH Frequency
LOW Consequence	LOW Frequency



General Methodological Framework

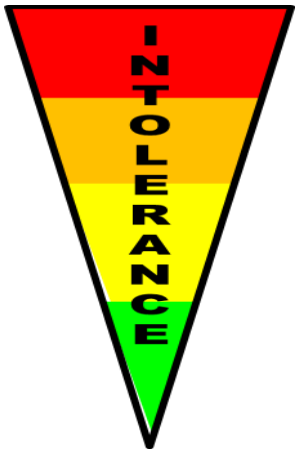
Step 2 of 6. Assess Risks



RISK ASSESSMENT MATRIX

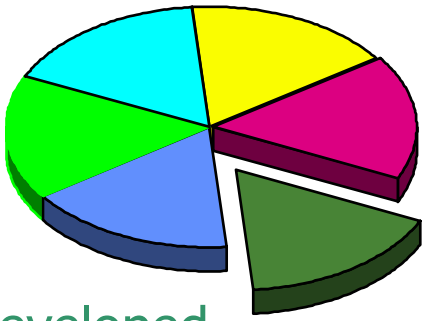
Risk Index		Likelihood				
		1	2	3	4	5
Impact	5	5	10	15	20	25
	4	4	8	12		20
	3	3	6		12	15
	2	2	4	6	8	10
	1	1		3	4	5
	0	0	0	0	0	0

INCREASING RISK



General Methodological Framework

Step 3 of 6. Analyze Risk Control Measures



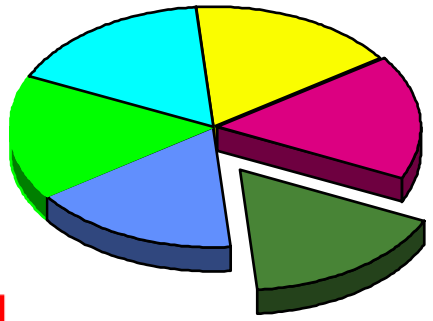
Risk Assessment Matrix

- Process: Comprehensive risk control options are developed to mitigate and manage each risk.
- Output: Risk control options to be considered by the decision maker.

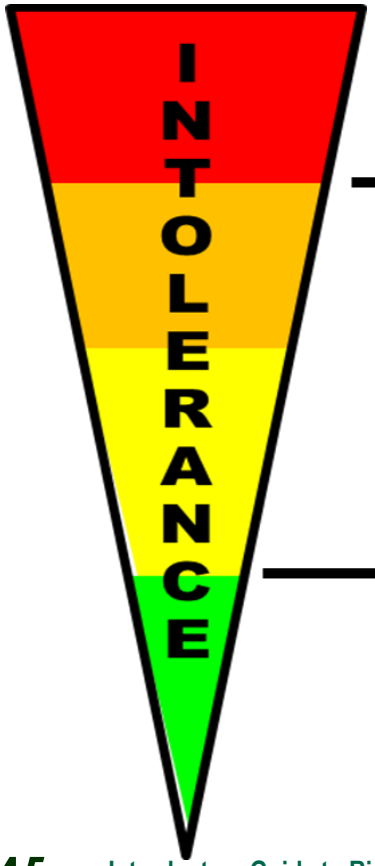
RI	Risk Level	Type of Control
>= 15	Unacceptable	Assess each threat that could cause the risk to occur. Implement a program to address each threat, eg plans, resources, objectives, hazard review
<15 & >=10	Tolerable if reasonable& feasible	Evaluate cost of options to control risk and verify that it is less than the cost of loss or damage, implement controls.
<10 & >=5	Tolerable if reasonable& feasible	Establish a control program by hazard category, conduct exposure/impact assessments, communicate at the local level, review hazards.
<5	Acceptable	Keep record of events and their consequences to identify hazards

General Methodological Framework

Step 3 of 6. Analyze Risk Control Measures



Inverted Pyramid of Risk Intolerance
(ALARP – As low as reasonably practicable)



Unacceptable risk level: Cannot be accepted or tolerated under any circumstances.

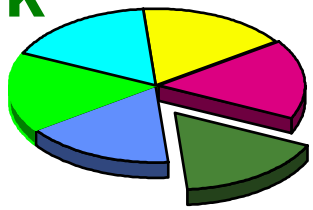
(ALARP – As Low as reasonably practicable)

Tolerable residual risk as technically and economically reasonably feasible, that is, tolerable risk in practice, if it is reasonably possible.

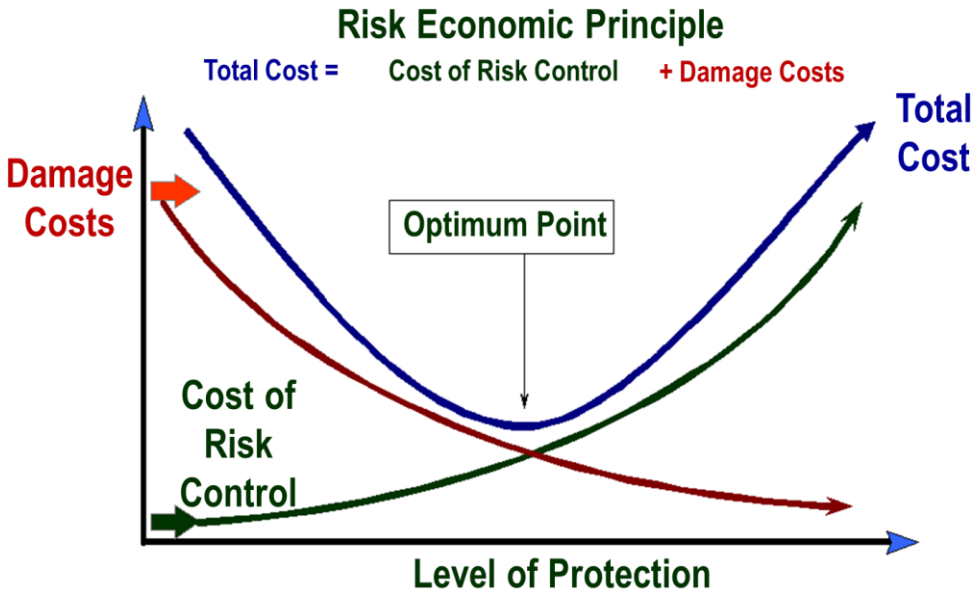
Acceptable, negligible level of risk that is widely accepted and does not require demonstration of ALARP analysis.

4. Process

General Methodological Framework



Step 3 of 6. Analyze Risk Control Measures



Risk Adjusted Return on Capital (RAROC)

$$RAROC = \frac{RISK\ ADJUSTED\ RETURN}{RISK\ ADJUSTED\ CAPITAL}$$

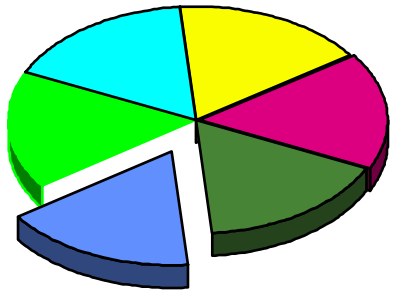
Risk Adjusted Return =
Revenues – Expenses – Expected Losses + Return on Economic Capital + Transfer Values / Prices

Risk Adjusted Capital =
Credit Risk
Market Risk
Operational Risk

RAROC – The Heart of Integrated Risk Management

General Methodological Framework

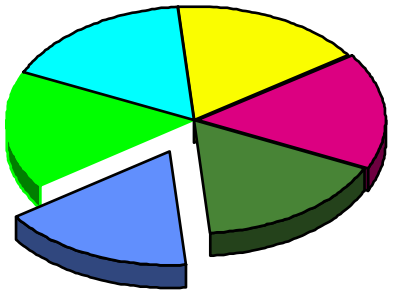
Step 4 of 6. Make Control Decisions



- Process: Delegate risk decisions to the right person, at the right time, with the right support.
- Exit: Personnel with knowledge of their level of authority for decision-making, limitations and knowing what risks they can assume.

General Methodological Framework

Step 4 of 6. Guide to establish the decision-making process for risk control

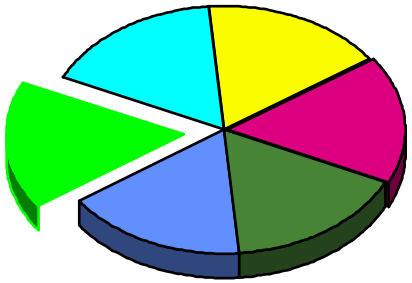


Risk Level	Decision Level
Extremely High	Board of Directors or Asset Owner
Very High	Authorized Personnel by the Board of Directors or Owner of the Asset
High	Vice-President, Business Manager, Asset Manager
Medium	Middle Manager, Project Leader, Team Leader in the Operational Theater
Low	Anyone in leadership position

4. Process

General Methodological Framework

Step 5 of 6. Implement Risk Control Measures



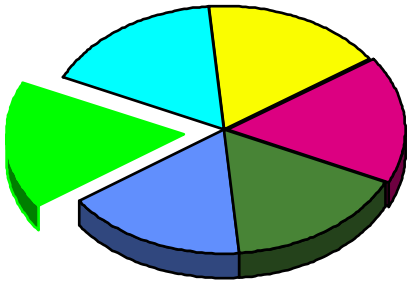
- Process: Development of implementation strategies to define individual responsibility, accountability and participation.

- Output: Risk controls tailored to positively impact the corporation's mission.

4. Process

General Methodological Framework

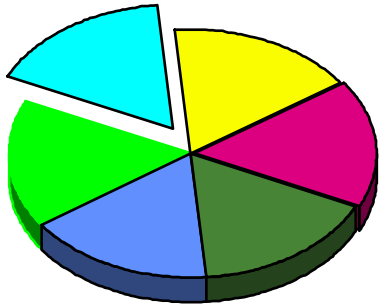
Step 5 of 6. Tools to Support the Implementation of Risk Control Measures



- Competency development plan
- Package of tools to support work processes
- Risk management performance measurement tools
- Risk control policy
- Tools for motivation
- Tools to empower (delegate authority)
- Application of artificial intelligence and machine learning tools for monitoring and risk management follow-up

General Methodological Framework

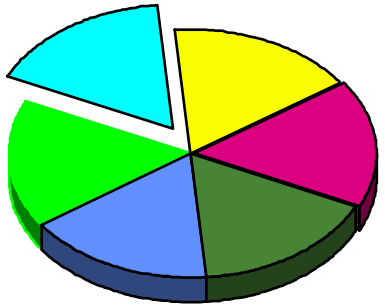
Step 6 of 6. Supervise and Review the Results of the Implementation of Risk Control Measures and Provide Feedback



- Process: Systematic evaluation of the results that support the risk management mission.
- Output: Risk monitoring system, failure data and information, and lessons learned available for future decisions.

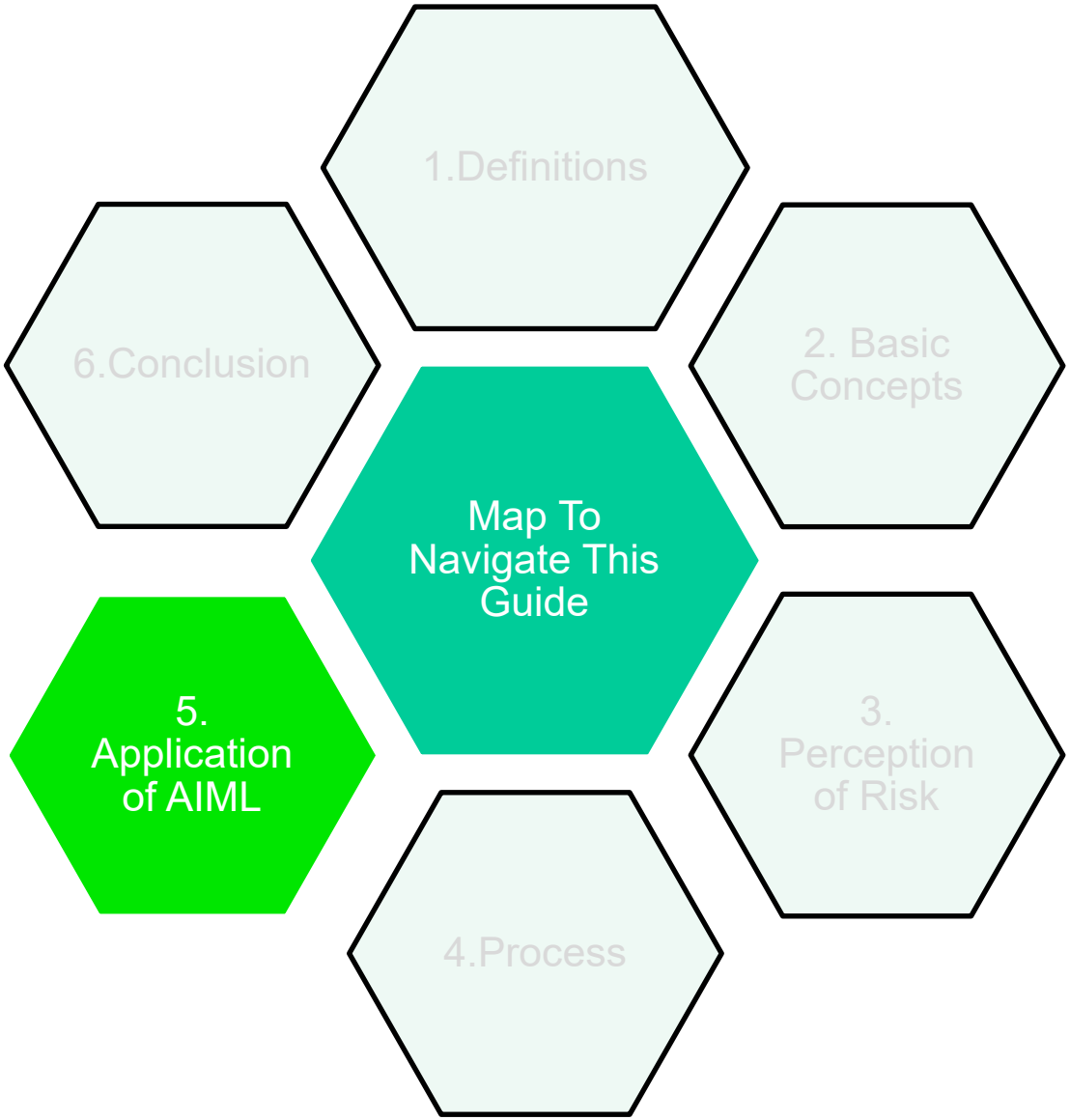
General Methodological Framework

Step 6 of 6. Guide to Supervise, Review and Feedback the Implementation of Risk Control Measures and Feedback



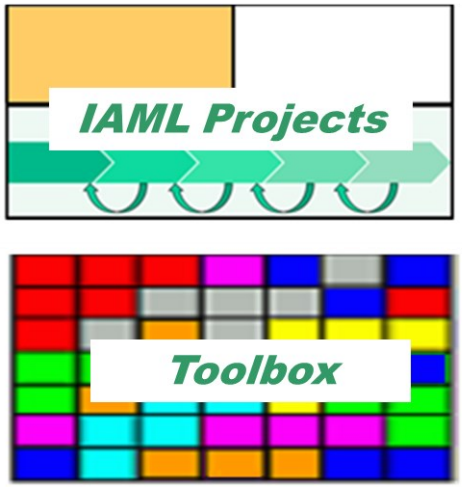
- Monitor activities during the execution of projects and operations, not risks.
- Measure risks directly.
- Use statistical tools as accurately as possible and reduce variability in processes.
- Improve the effectiveness of feedback to stimulate learning (lessons learned)
- Apply best practices, data and information technologies, as well as artificial intelligence to ensure effective feedback and closure of the individual and organizational learning loop.

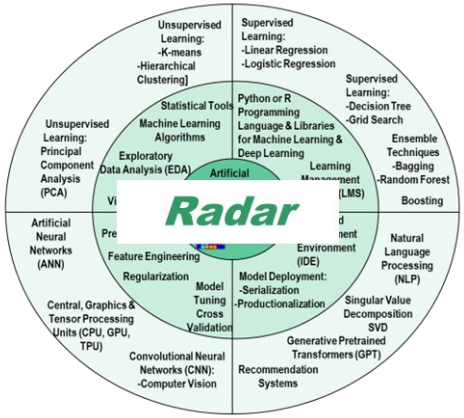
Map To Navigate This Guide

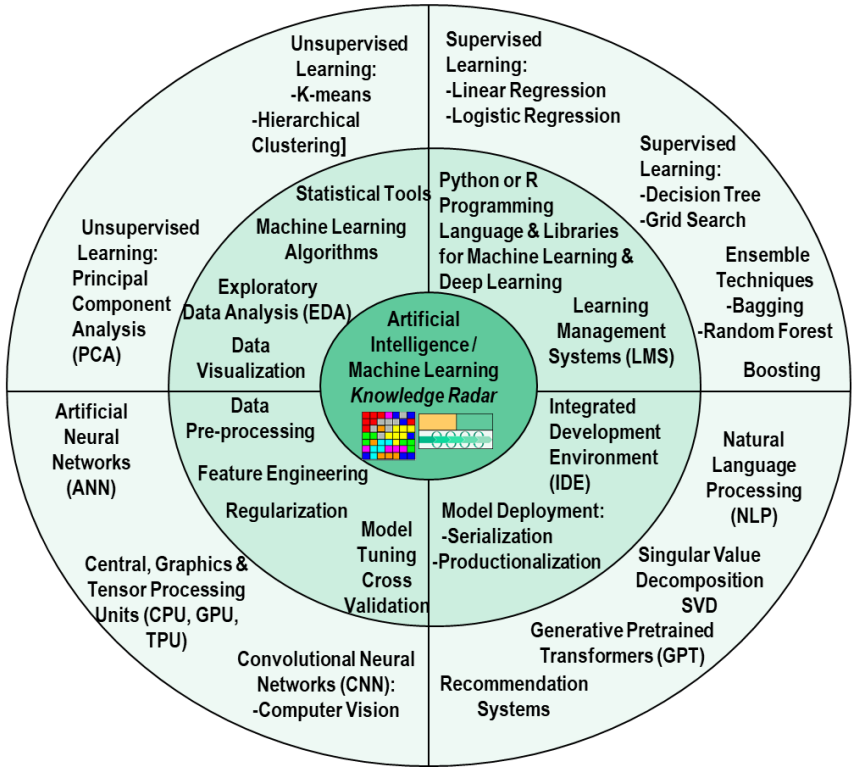


5. Application of AIML

AIML Project, Toolbox and Radar (AIML-PTR)

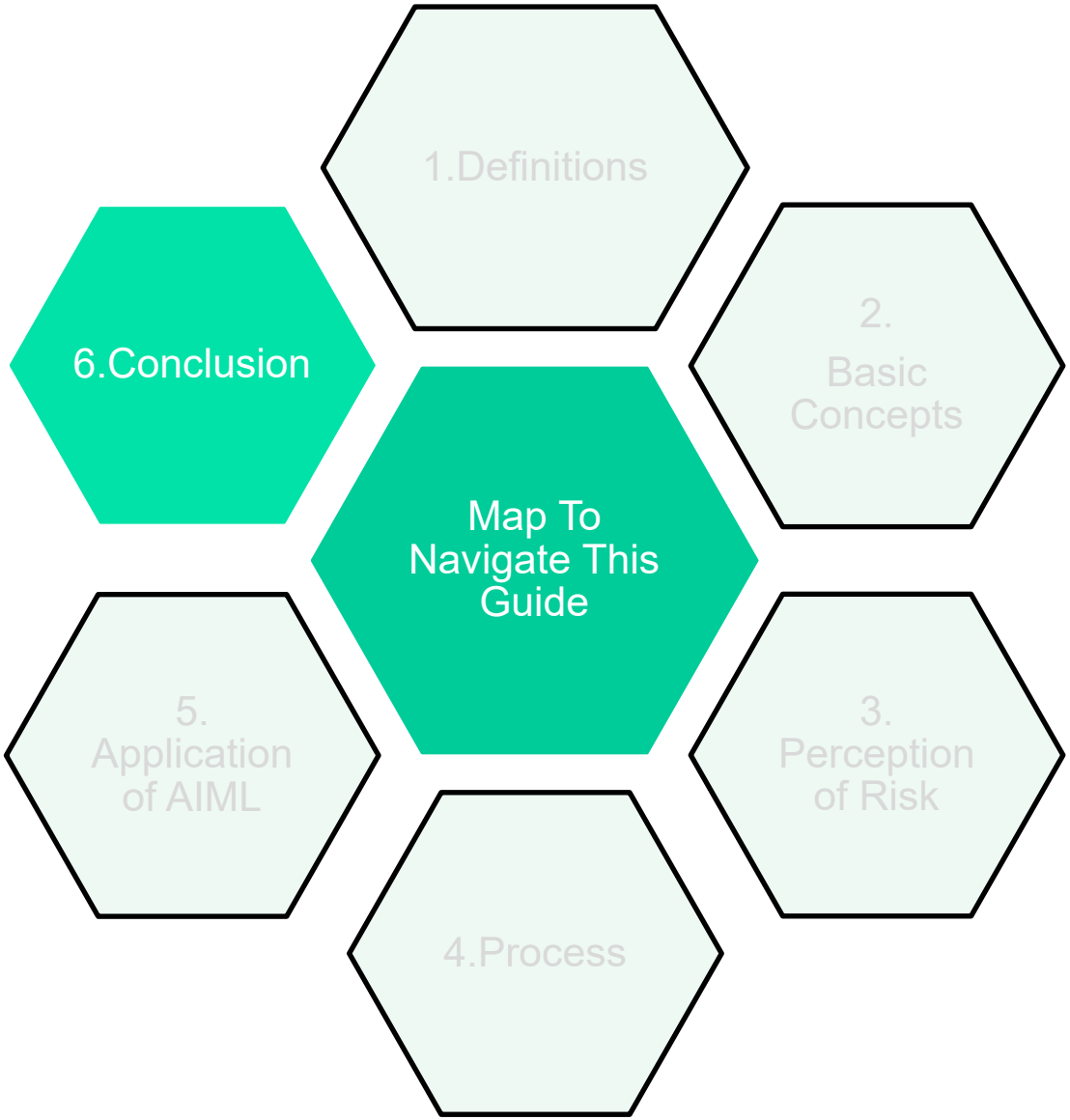






AIML application is made with a project, selecting the applicable tools and libraries for each case – Visit www.optimawell.us for more information

Map To Navigate This Guide



6. Conclusion

Food for Thought - Six Questions

- Do you possess a list of the most critical risk scenarios for the assets for which you hold responsibility and accountability?
- Have you proactively identified and documented these critical risk scenarios in a Risk Assessment Matrix (RAM)?
- Are you confident that you and your team are taking all possible measures promptly to mitigate or eliminate risks that exceed the tolerance threshold?
- Can you and your team demonstrate that the risks falling within the 'As Low As Reasonably Practicable' (ALARP) zone are either tolerable or acceptable to your business or organization?
- Do you actively promote a culture of risk awareness and accountability, with achievements being acknowledged and celebrated?
- Is there an established process in place for periodically reviewing and refining the risk management system?

Food for Thought – Two Groups

There are two categories of companies and organizations:

- The first category proactively and systematically applies risk management to their assets, processes, or projects. They demonstrate higher levels of success, creating sustainable value for their clients and asset owners.
- The second category lacks a risk management system, resulting in low returns in value creation, customer dissatisfaction with their products and services, and unsustainable business models over time.

Let's carefully consider which category we want to engage with for work, investment, or the purchase of products and services.

6. Conclusion

Closing Remark

This document is part of the support offered by OptimaWell for a range of products, consulting services, and training programs designed to prepare your team for effective asset management. Our aim is to increase the likelihood of success in your business endeavors, projects, and value creation processes.

For more details, please consult our catalog of services, products, and training available on our website at www.optimawell.us

If you require further information, don't hesitate to reach out to us via email at jlov@optimawell.us