t-Risk

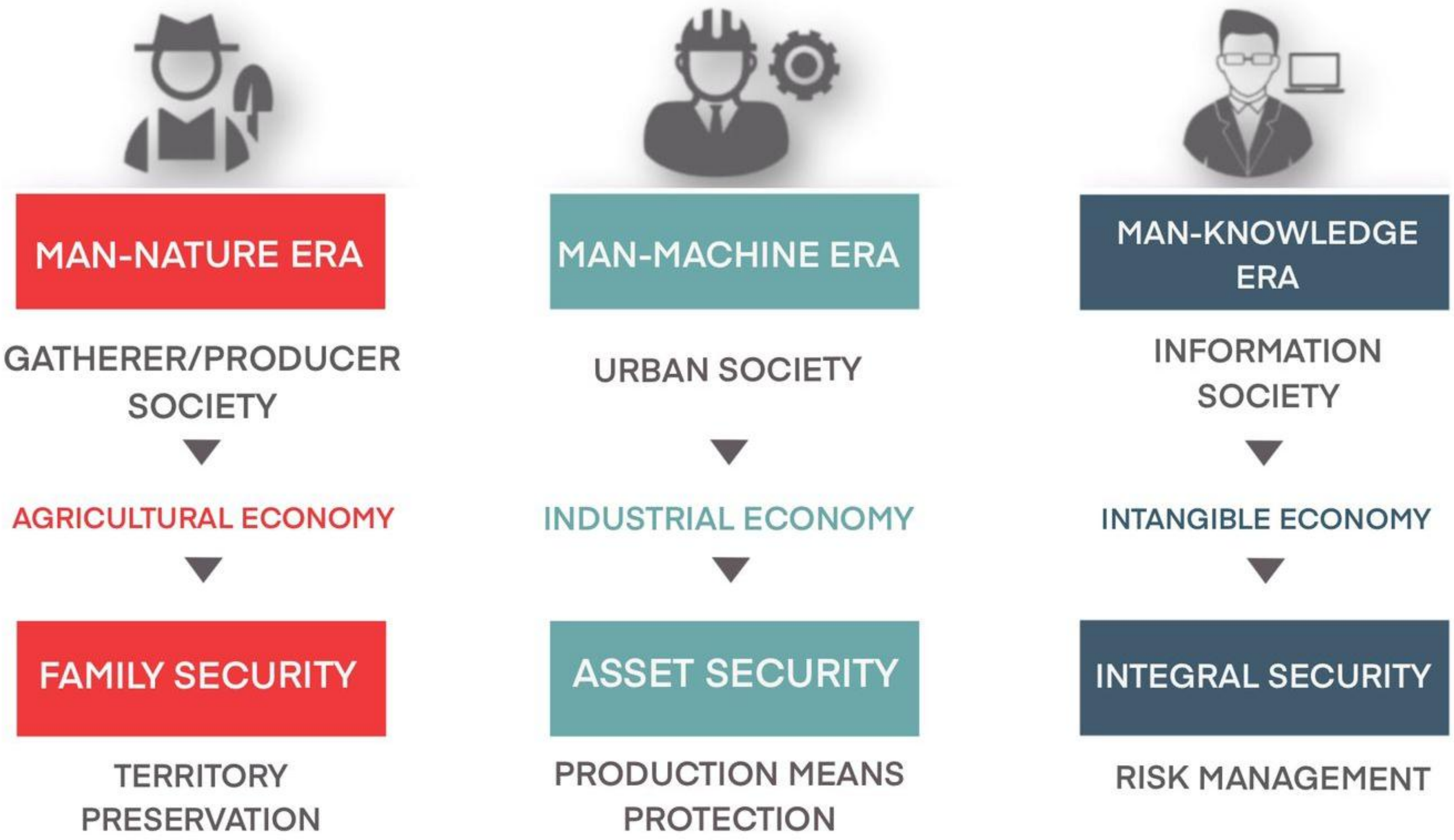
Método de Avaliação de Riscos

# *INTRODUCTION*

# Risk Management According to ISO 31000 & t-Risk Platform

Reviewed: June 2025

# Evolution of security



MAN-NATURE ERA

GATHERER/PRODUCER SOCIETY

AGRICULTURAL ECONOMY

FAMILY SECURITY

TERRITORY PRESERVATION

MAN-MACHINE ERA

URBAN SOCIETY

INDUSTRIAL ECONOMY

ASSET SECURITY

PRODUCTION MEANS PROTECTION

MAN-KNOWLEDGE ERA

INFORMATION SOCIETY

INTANGIBLE ECONOMY

INTEGRAL SECURITY

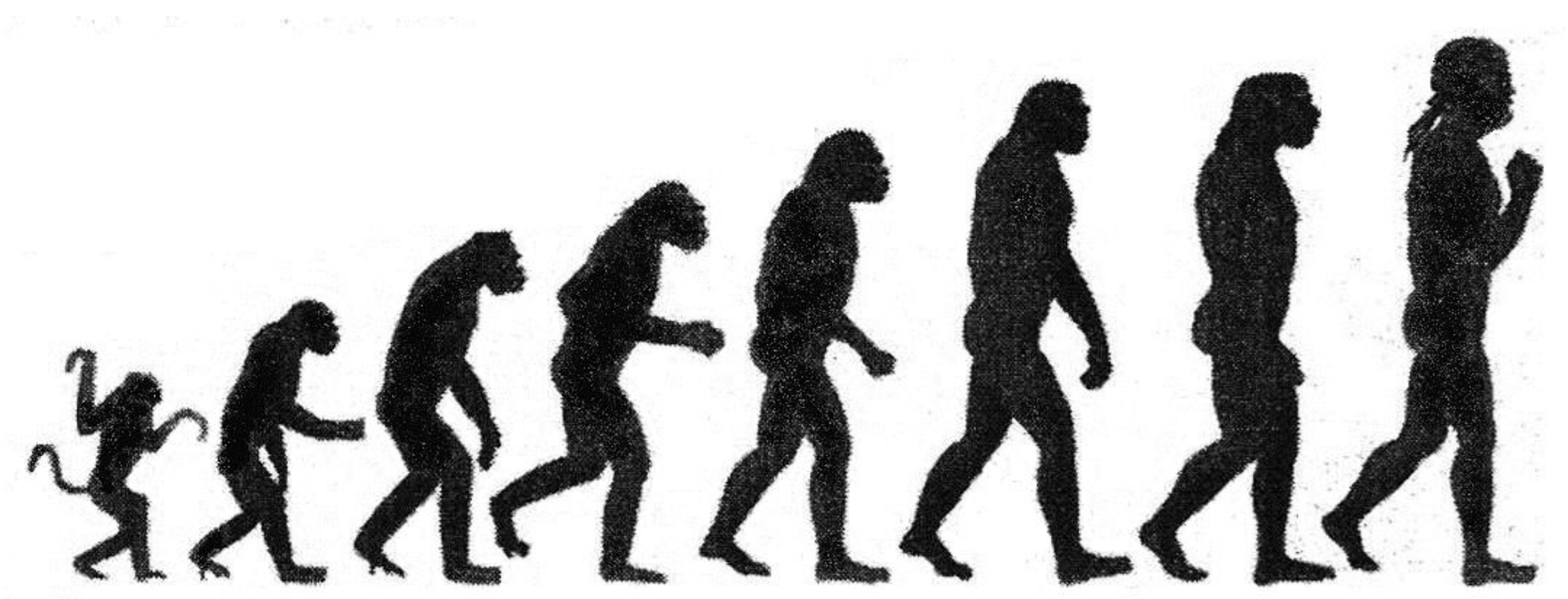
RISK MANAGEMENT

# Risk Equation (Total RISK® METHOD)

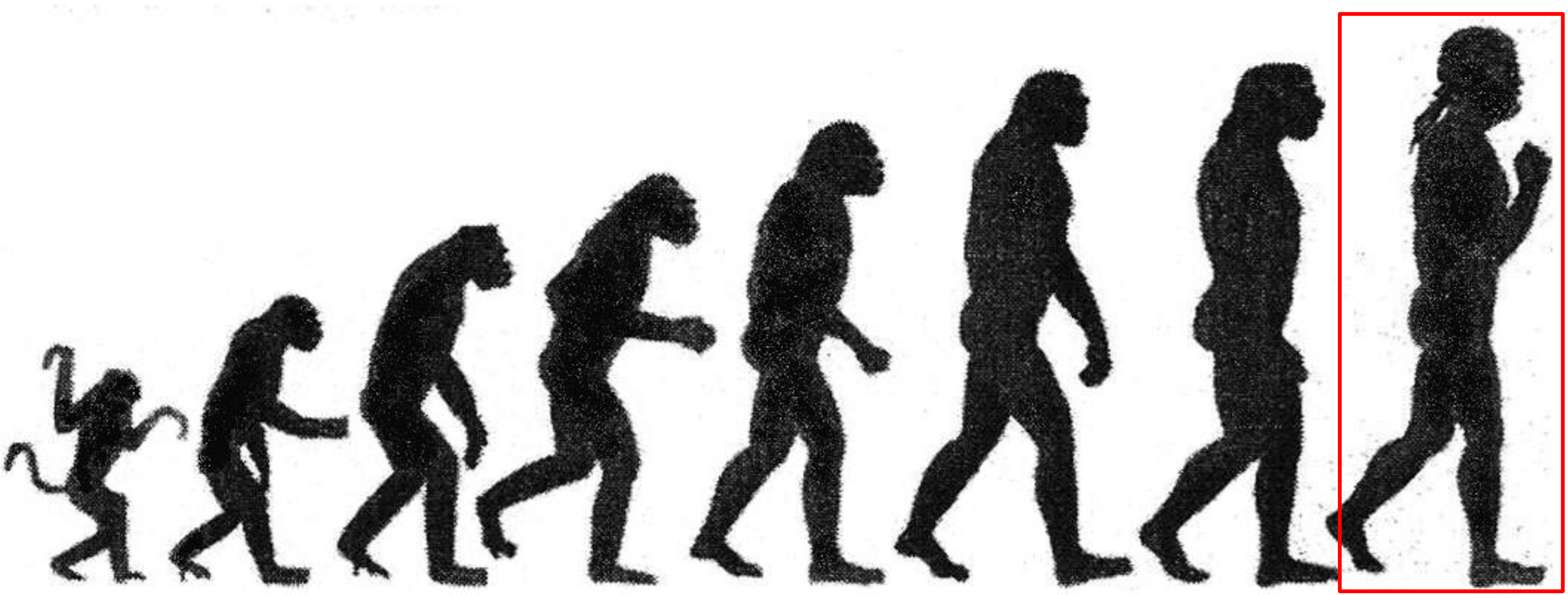
$$\text{RISK} = \frac{\text{THREAT} \times \text{VULNERABILITY} \times \text{IMPACT} \times \text{PROBABILITY}}{\text{EFFICIENT SECURITY CONTROLS}}$$

*The Risk Equation is described in Tácito Leite's book "Risk Management in Physical Security" and is part of the Total Risk® Method.*

# Why we're good at risk management?



# Why aren't we good at Risk Management TODAY?



# Examples of Risks in the Jewelry Production Chain

CARGO THEFT

THEFT

FRAUD

COMPLIANCE

ACCIDENTS

**ILLEGAL MINING**

**LOGISTICS**

**FACTORY**

**REPRESENTATIVE**

**STORE**

INFORMATION LEAKAGE

SABOTAGE

ROBBERY

IMAGE DAMAGE

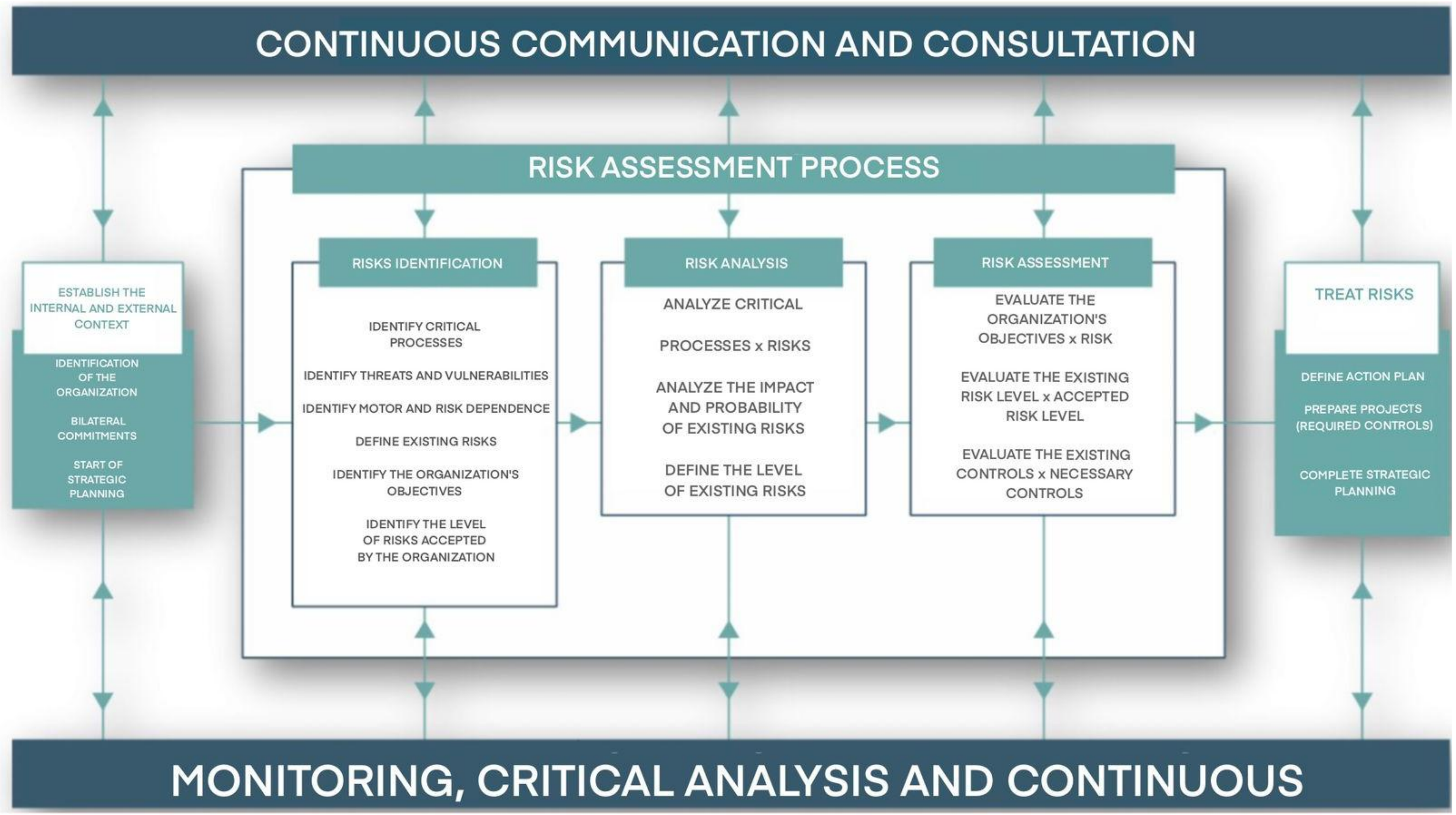
PERDA E QUEBRA

*The Universal Risk Standard*
*One framework for all risk types*
*All organization sizes*

# Evolution of the ISO 31000 family

- ISO Guide 73:2002
- ISO 31000: 2009
- ISO Guide 73:2009
- ISO 31010: 2012
- ISO 31004: 2015
- ISO 31000: 2018
- ISO 31010: 2021
- ISO 31073: 2022
- Handbook 31000: 2023
- ISO 31050: 2023

# Risk Management Process Overview



CONTINUOUS COMMUNICATION AND CONSULTATION

RISK ASSESSMENT PROCESS

ESTABLISH THE INTERNAL AND EXTERNAL CONTEXT

- IDENTIFICATION OF THE ORGANIZATION
- BILATERAL COMMITMENTS
- START OF STRATEGIC PLANNING

RISKS IDENTIFICATION

- IDENTIFY CRITICAL PROCESSES
- IDENTIFY THREATS AND VULNERABILITIES
- IDENTIFY MOTOR AND RISK DEPENDENCE
- DEFINE EXISTING RISKS
- IDENTIFY THE ORGANIZATION'S OBJECTIVES
- IDENTIFY THE LEVEL OF RISKS ACCEPTED BY THE ORGANIZATION

RISK ANALYSIS

- ANALYZE CRITICAL
- PROCESSES x RISKS
- ANALYZE THE IMPACT AND PROBABILITY OF EXISTING RISKS
- DEFINE THE LEVEL OF EXISTING RISKS

RISK ASSESSMENT

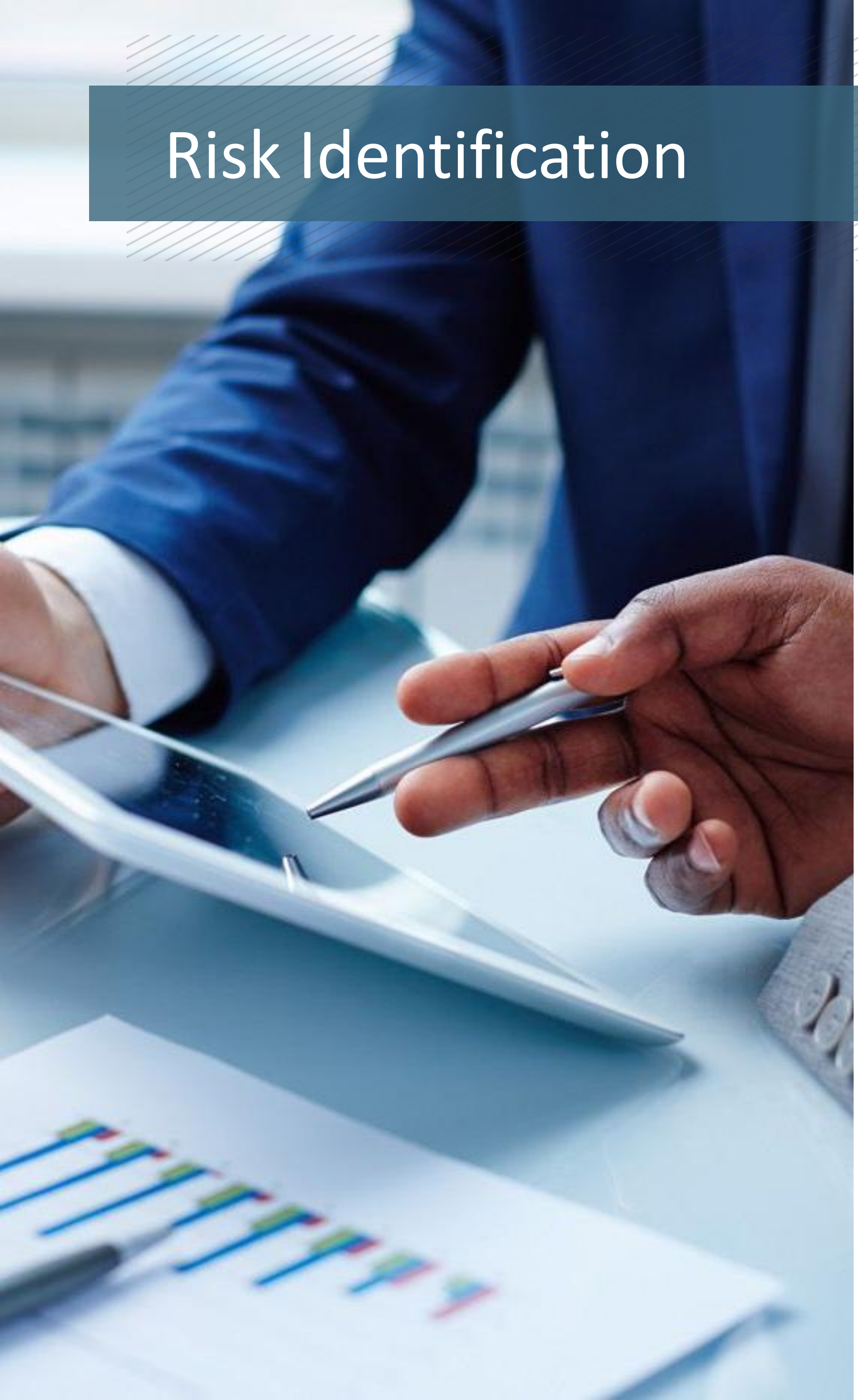
- EVALUATE THE ORGANIZATION'S OBJECTIVES x RISK
- EVALUATE THE EXISTING RISK LEVEL x ACCEPTED RISK LEVEL
- EVALUATE THE EXISTING CONTROLS x NECESSARY CONTROLS

TREAT RISKS

- DEFINE ACTION PLAN
- PREPARE PROJECTS (REQUIRED CONTROLS)
- COMPLETE STRATEGIC PLANNING

MONITORING, CRITICAL ANALYSIS AND CONTINUOUS

# Risk Identification

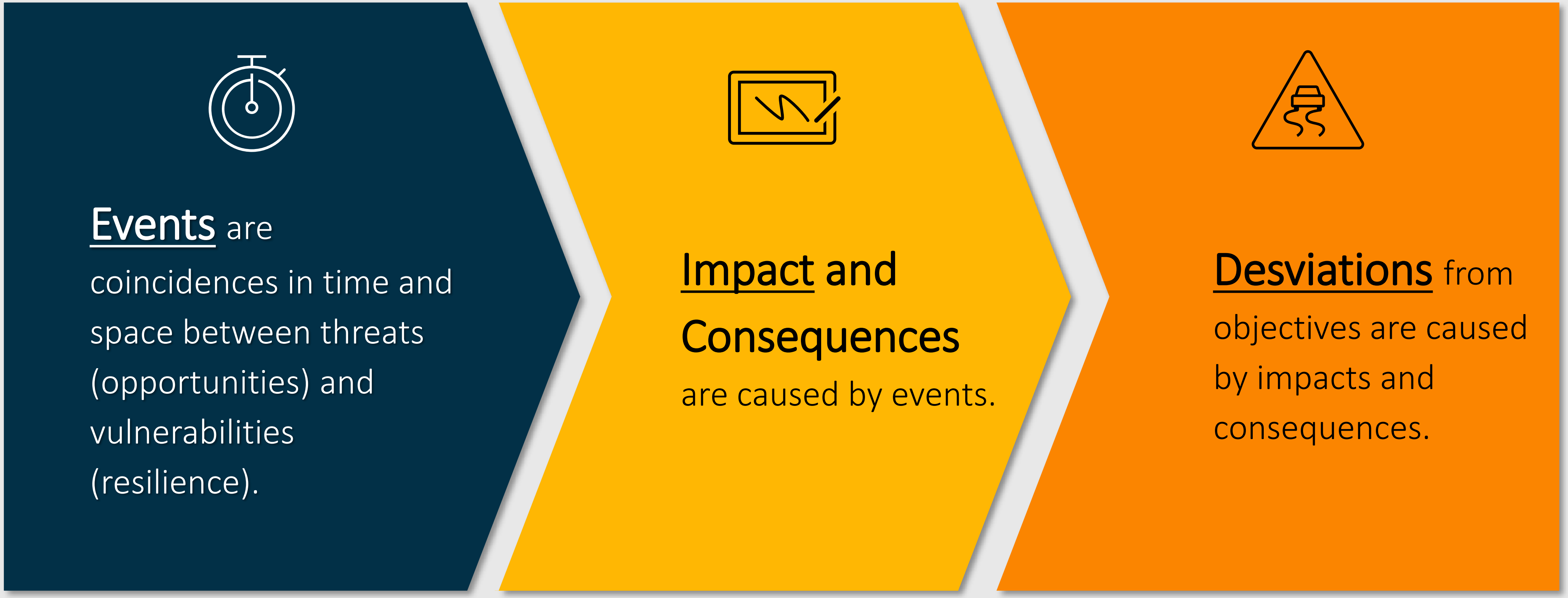


- The organization should identify risk sources, impact areas, events and their causes and potential consequences.
- The purpose of this stage is to generate a comprehensive list of risks based on these events that may create, increase, prevent, reduce, accelerate or **delay the achievement of the organization's objectives**.
- Include **chain reaction**, cumulative effect, cascading and cross-impact.
- It is important to use appropriate techniques and tools and involve personnel with compatible knowledge.

# Importance of Event Identification

Risk, based on its general meaning (ISO 31000:2018), is defined as **the effect of uncertainty on objectives**.

## WHERE DOES UNCERTAINTY COME FROM?

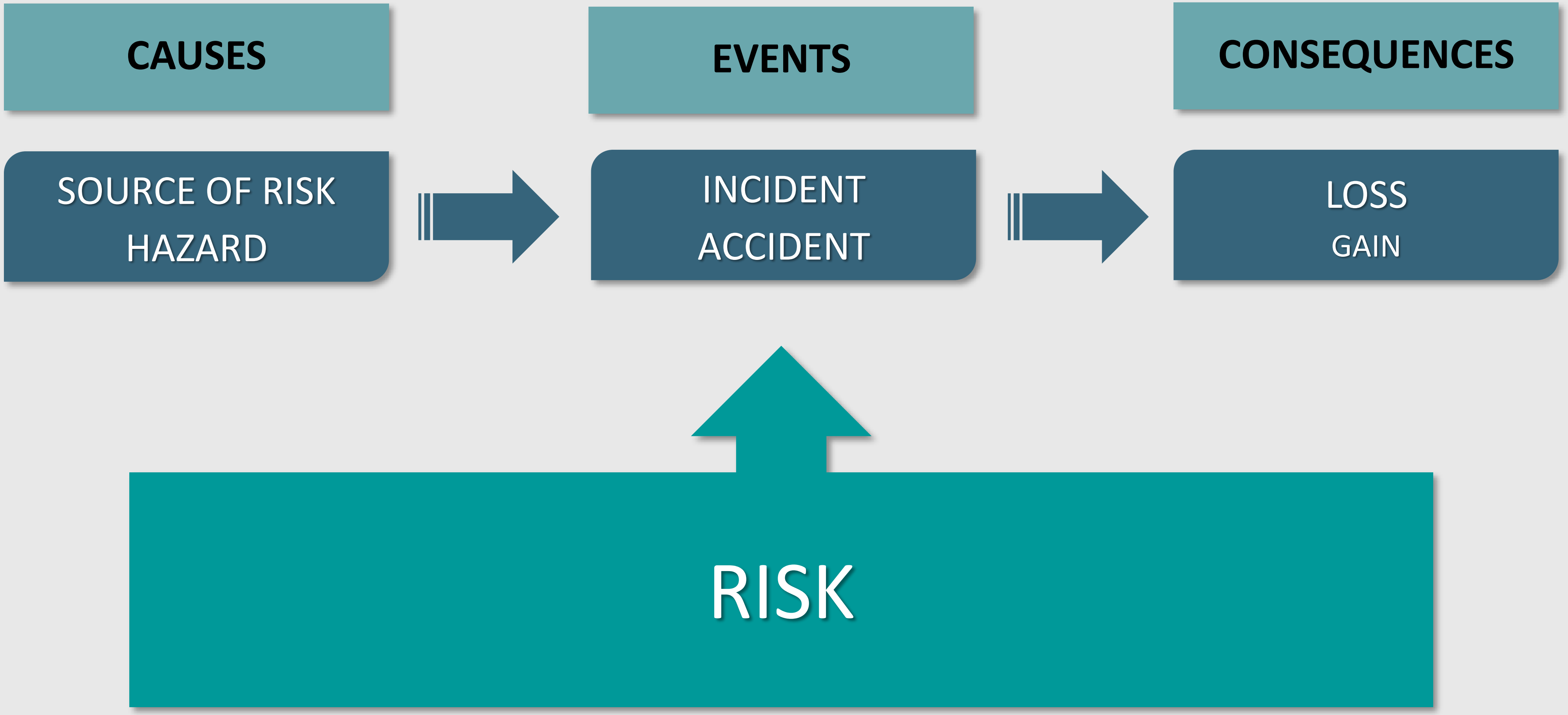


**Events** are coincidences in time and space between threats (opportunities) and vulnerabilities (resilience).

**Impact and Consequences** are caused by events.

**Desviations** from objectives are caused by impacts and consequences.

# Analysis of Cause, Event and Consequence Described in ISO 31000



CAUSES

SOURCE OF RISK
HAZARD

EVENTS

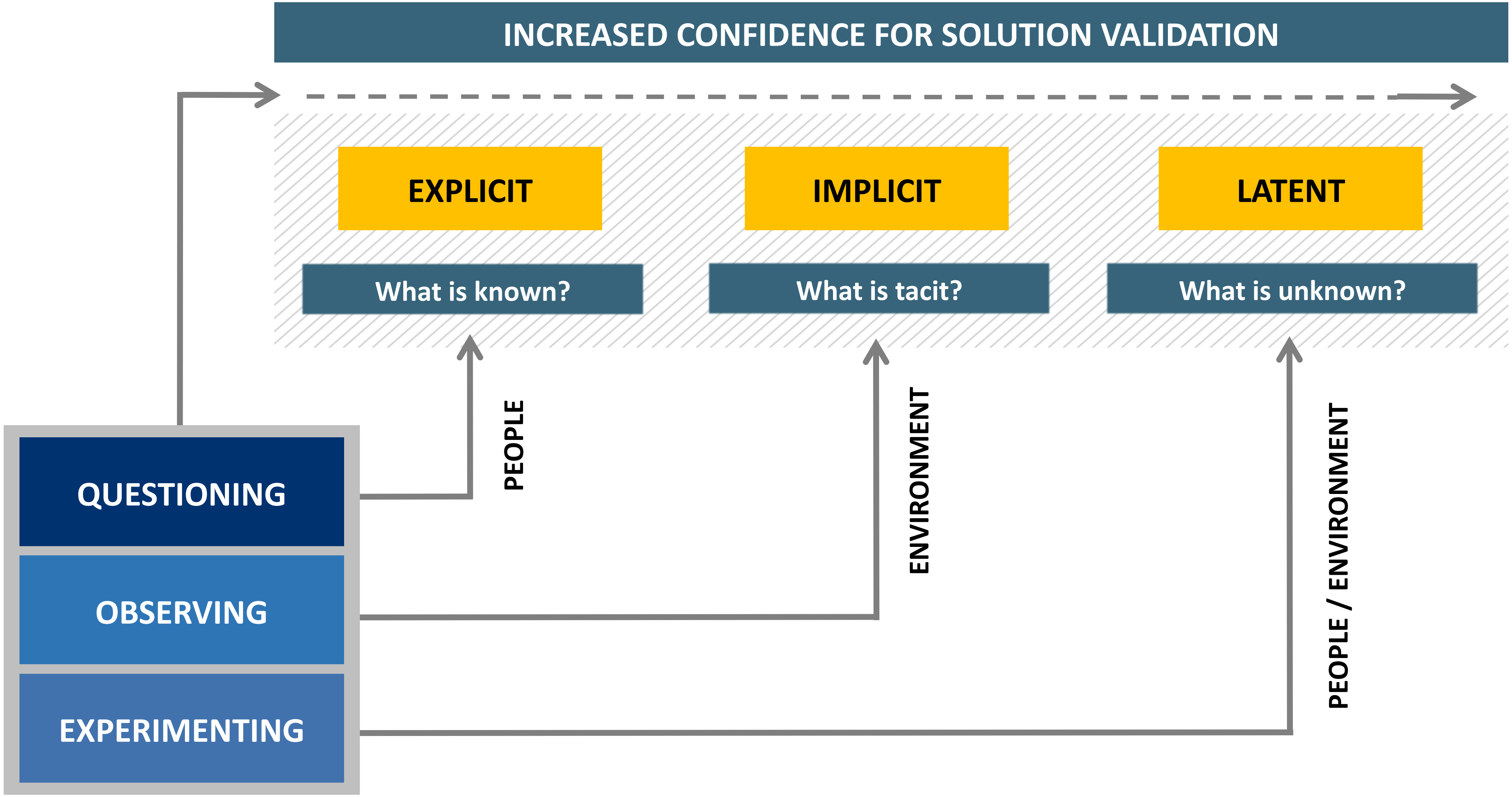
INCIDENT
ACCIDENT

CONSEQUENCES

LOSS
GAIN

RISK

# How to Identify Risks?



INCREASED CONFIDENCE FOR SOLUTION VALIDATION

EXPLICIT

What is known?

IMPLICIT

What is tacit?

LATENT

What is unknown?

PEOPLE

ENVIRONMENT

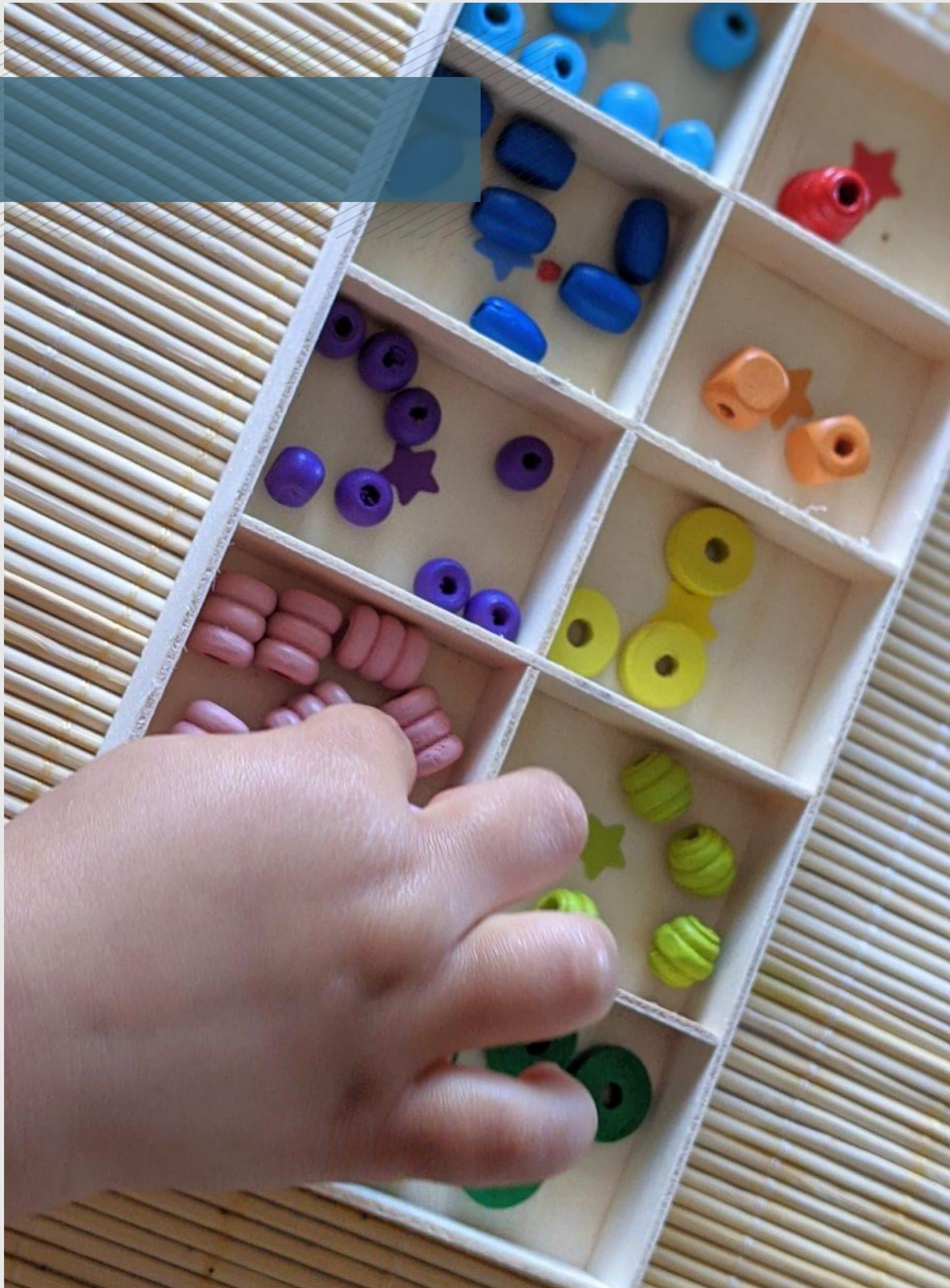
PEOPLE / ENVIRONMENT

QUESTIONING

OBSERVING

EXPERIMENTING

# Risk Classification



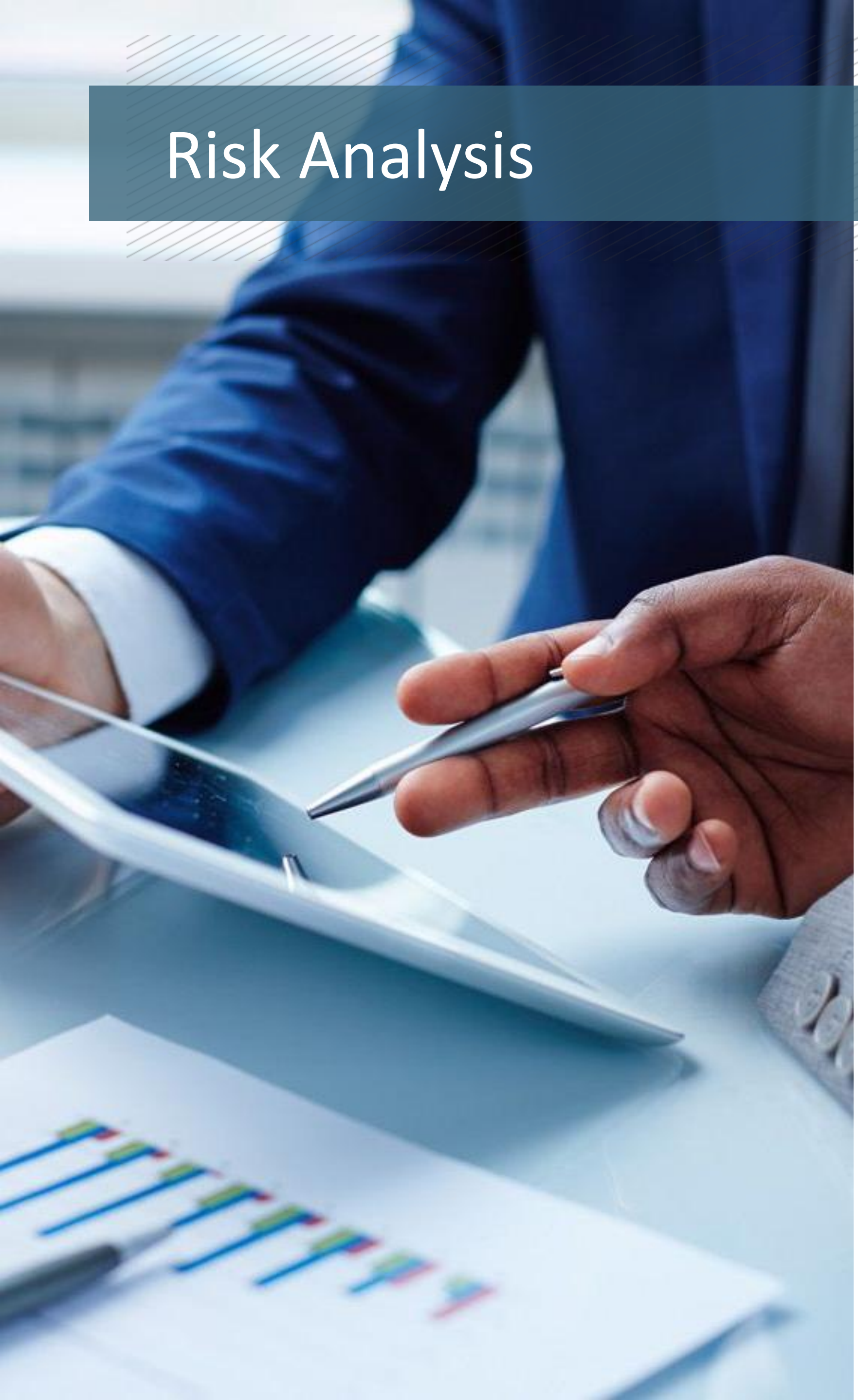
## What is risk classification?

- A process that consists of dividing identified risks into categories or groups based on predefined criteria, which may include the nature of the risk, its origin, its magnitude, among others.

## What is the purpose of risk classification?

- Prioritization
- Resource allocation
- Understanding and communication
- Mitigation strategy development
- Monitoring and analysis
- Continuous improvement
- Compliance assurance

# Risk Analysis

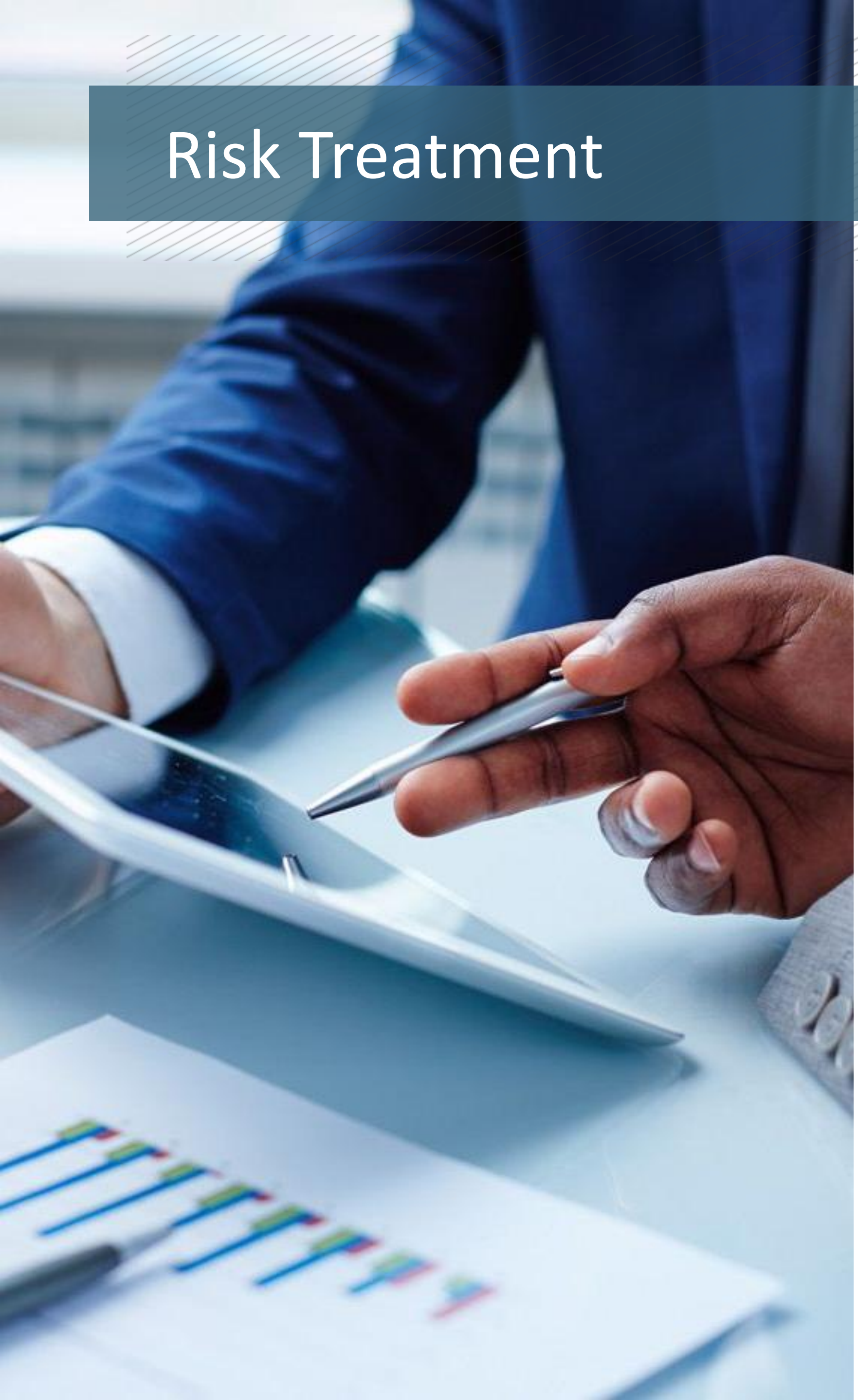


- Risk analysis involves developing an **understanding of risks**.
- Risk is analyzed by determining, at minimum, the **consequences** and their **probabilities** (**ISO 31000:2009**).
- Risk analysis considers **uncertainties**, **risk sources**, **consequences**, **probabilities**, **events**, **scenarios**, **controls**, and their **effectiveness** (ISO 31000:2018).
- Risk analysis can be performed at varying levels of detail. Depending on **circumstances**, the analysis may be **qualitative**, **semi-quantitative**, **quantitative** or a **combination** of these.

# Risk Assessment

- The **purpose** of risk assessment is to **support decision-making** (based on comparing risk analysis results with established risk criteria) regarding which risks require treatment and the implementation priority for such treatment.
- Risk assessment involves comparing the risk level identified during the analysis process with the risk criteria established when the context was defined.
- Decisions on treatment types will be influenced by **risk attitude**.

# Risk Treatment



- Risk treatment involves selecting one or more options to modify risks and implementing these options.
- Treating risks involves a cyclical process composed of:

- Assessment of previously implemented risk treatments

- Determination of whether residual risk levels are tolerable

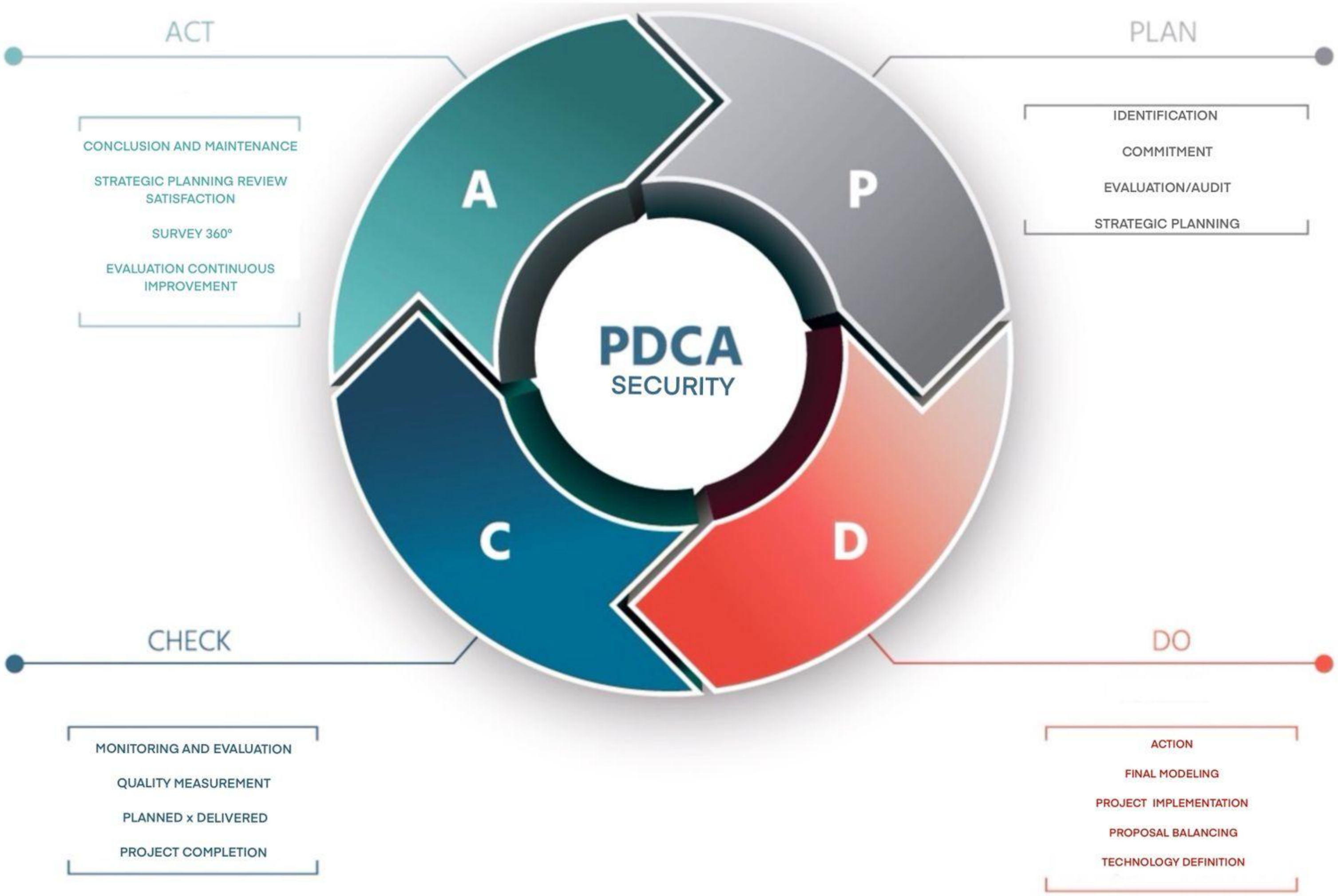
- Among other steps

# Options for Risk Treatment

1. AVOID the risk by not starting or discontinuing the activity that gives rise to the risk.
2. TAKE OR INCREASE the risk to take advantage of an opportunity (positive risk).
3. REMOVE THE SOURCE of the risk.
4. CHANGE THE LIKELIHOOD of the risk.
5. CHANGE THE CONSEQUENCES of the risk.
6. SHARE the risk (e.g., through contracts and insurance)
7. RETAIN the risk consciously and based on an informed decision.

***Note:** These options are NOT necessarily mutually exclusive.*

# Security PDCA based on Risk Management



ACT

CONCLUSION AND MAINTENANCE

STRATEGIC PLANNING REVIEW SATISFACTION

SURVEY 360º

EVALUATION CONTINUOUS IMPROVEMENT

PLAN

IDENTIFICATION

COMMITMENT

EVALUATION/AUDIT

STRATEGIC PLANNING

CHECK

MONITORING AND EVALUATION

QUALITY MEASUREMENT

PLANNED x DELIVERED

PROJECT COMPLETION

DO

ACTION

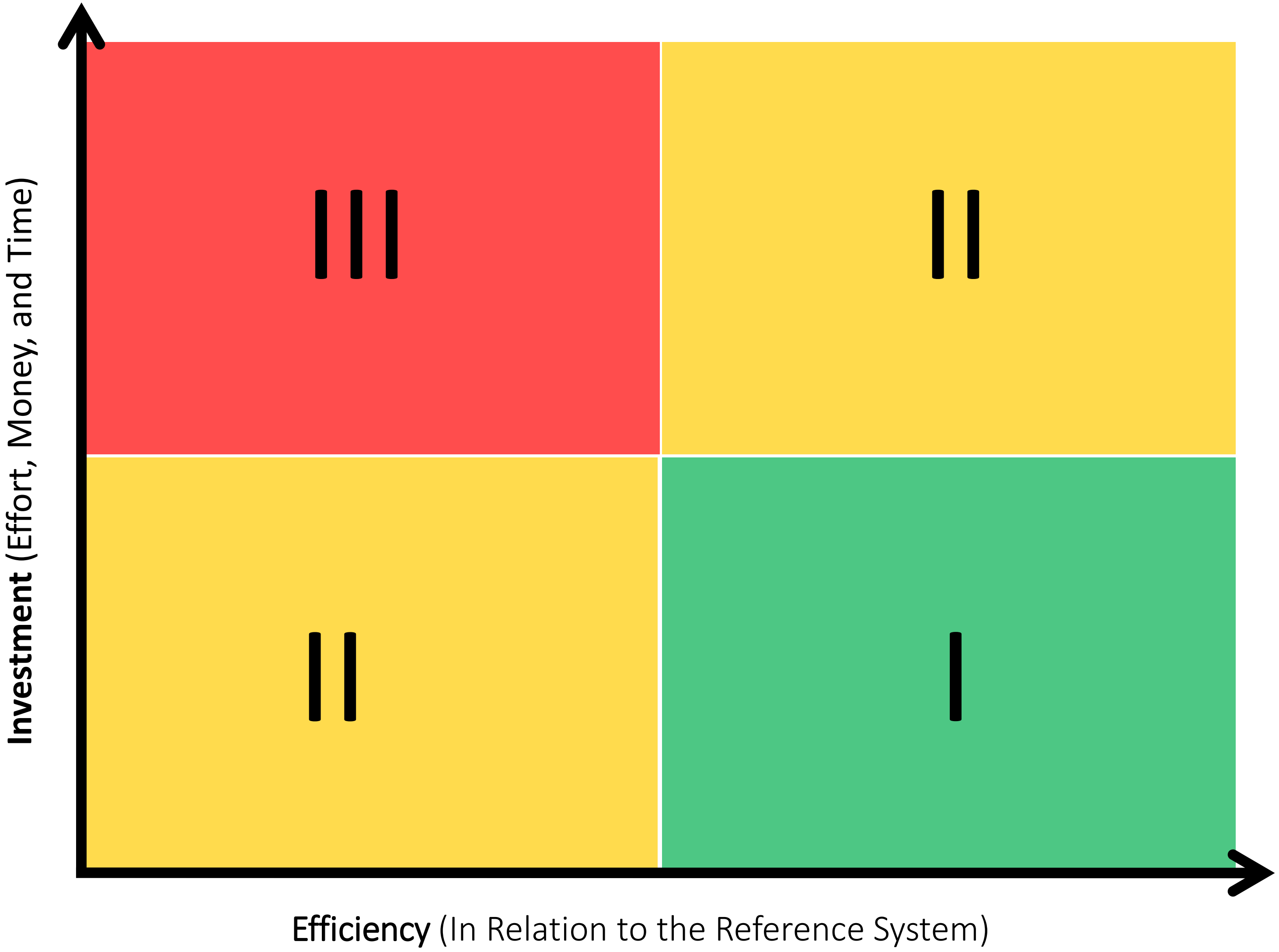
FINAL MODELING

PROJECT IMPLEMENTATION

PROPOSAL BALANCING

TECHNOLOGY DEFINITION

# Control Implementation & Investment Priority


III
II
II
I
Investment (Effort, Money, and Time)
Efficiency (In Relation to the Reference System)

**PARETO'S LAW**

**20%**
INDICATED SECURITY RESOURCES

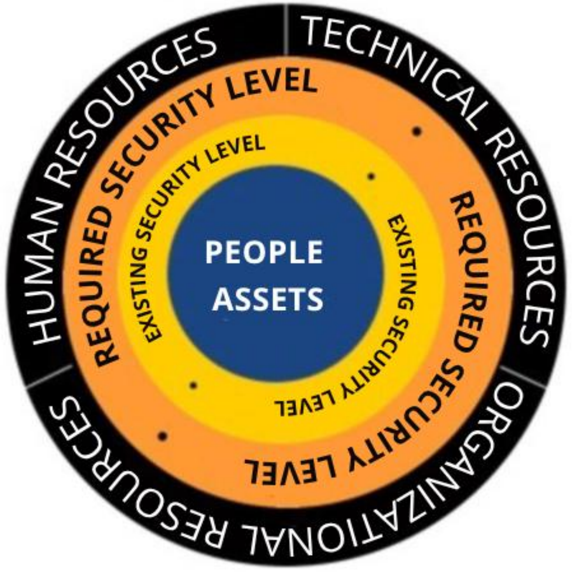
**80%**
EXISTING RISKS

**20%**
EXISTING RISKS

**80%**
EXPECTED LOSS

# Efficient Investment in Security Controls

## INADEQUATE SECURITY

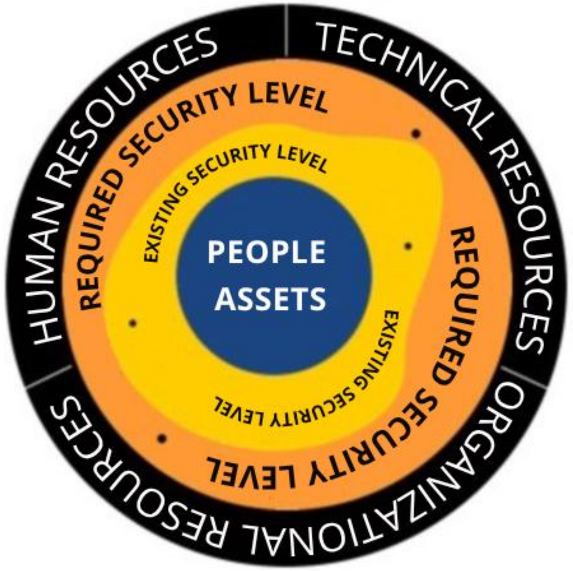


**LACK OF INVESTMENT IN SECURITY**

**N.S.N. ≠ N.S.E.**

| | |
|---|---|
| RISK | High |
| IMPACT | High |
| ROI | Imprecise |

## INADEQUATE SECURITY

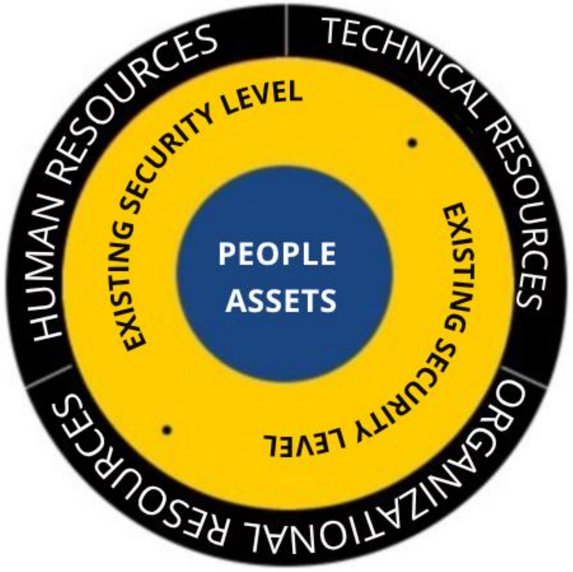


**INEFFICIENT INVESTMENT IN SECURITY**

**N.S.N. ≠ N.S.E.**

| | |
|---|---|
| RISK | Fluctuating |
| IMPACT | Fluctuating |
| ROI | Low |

## ADEQUATE SECURITY

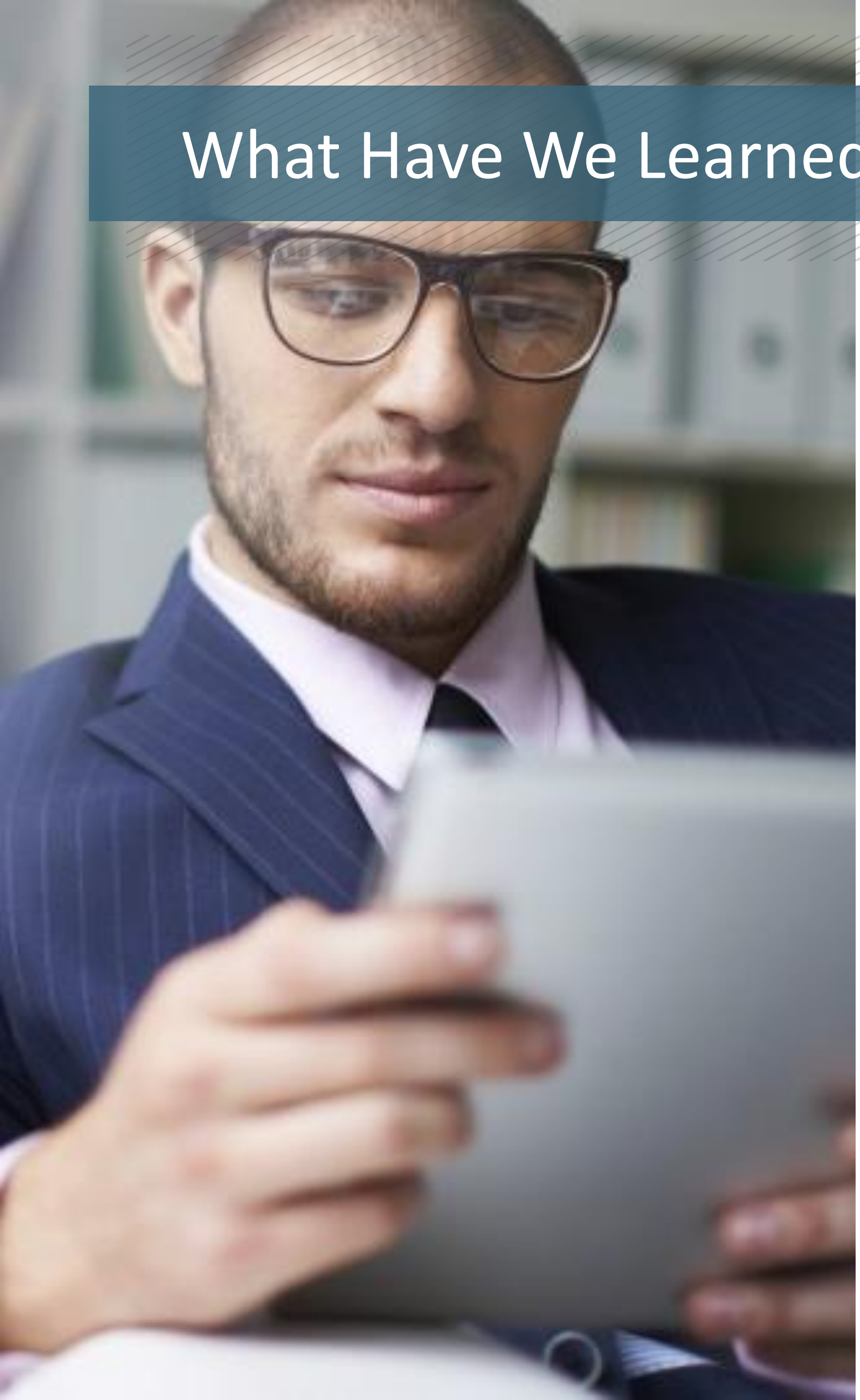


**EFFICIENT INVESTMENT IN SECURITY**

**N.S.N. = N.S.E.**

| | |
|---|---|
| RISK | Low |
| IMPACT | Low |
| ROI | High |

*NSN = Necessary Security Leve
I*NSE = Existing Security Level



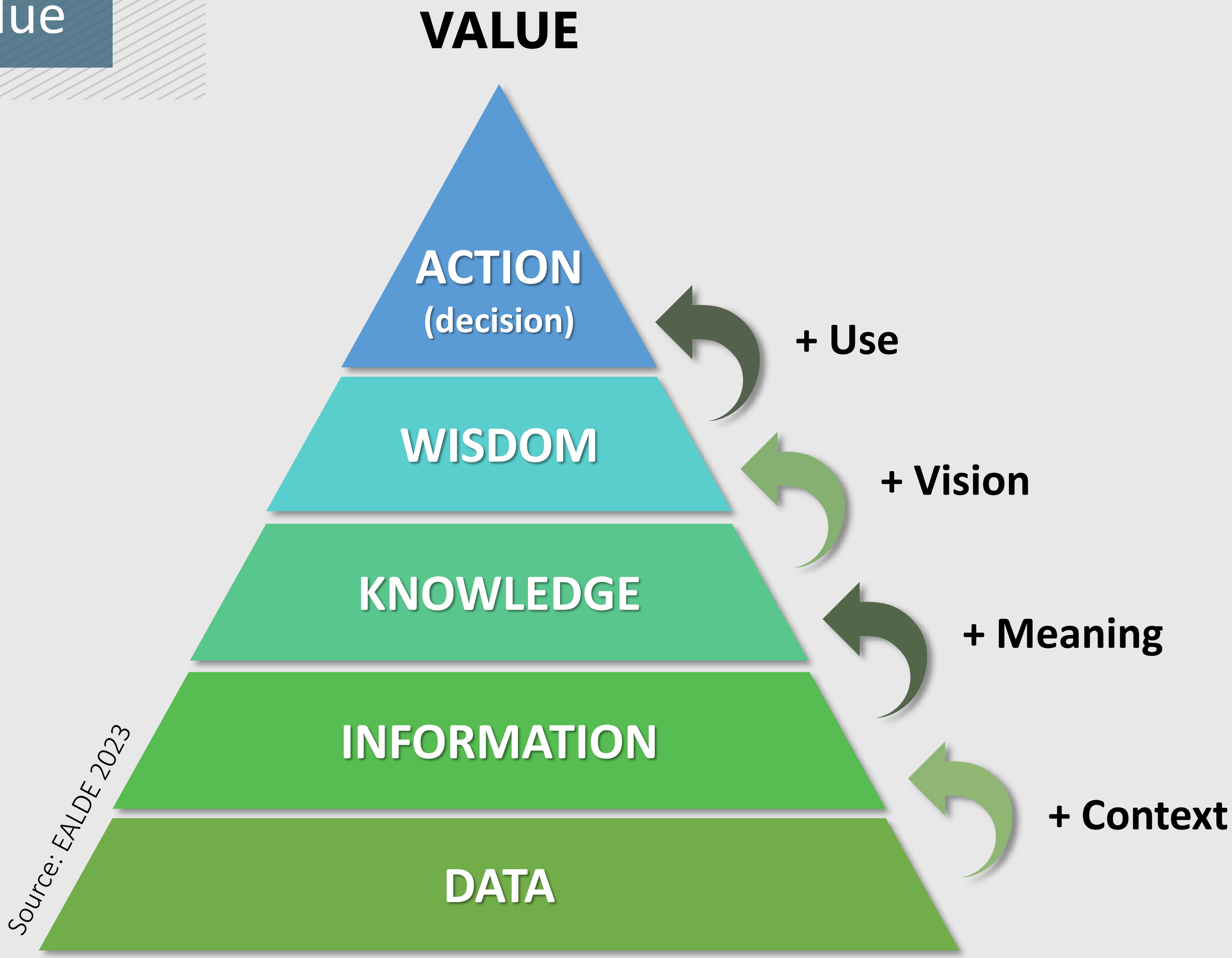
# What Have We Learned About Risk Management?

- Develop risk management and risk assessment processes in **compliance with ISO 31000**.

- The main steps for implementing the **Risk Management Process** are:

  1. **Communication and consultation;**
  2. **Establishing the context;**
  3. **Risk identification;**
  4. **Risk analysis;**
  5. **Risk evaluation;**
  6. **Risk treatment,**
  7. **Monitoring and review.**

# Communicate Value



Source: EALDE 2023

# Reflection: GRC – Governance / Risk / Compliance

1

**Governance –** What should and should not be done within the company for it to achieve its objectives.

2

**Risk –** What are the business risks (systemic & integrated) that can prevent (totally/partially) the realization of objectives.

3

**Compliance –** Are the desired actions being performed? Have undesired actions occurred? Are the controls defined in the risk assessment effective/efficient? Is the organization achieving its objectives?

## Security risk assessment software

Ideal tool for the corporate security risk manager to produce risk analysis and treatment plans.

https://totalrisk.com.br/en

Reference Bibliography

*See also:*
**www.bibliotecadeseguranca.com.br/en/**

GESTÃO DE RISCOS
NA SEGURANÇA PATRIMONIAL
Um guia para empresários e consultores
DE ACORDO COM ABNT NBR ISO 31000:2009
TOTAL RISK
MÉTODO DE AVALIAÇÃO DE RISCOS
Tácito Augusto Silva Leite
QUALITYMARK

t-Risk

Método de Avaliação de Riscos

*Badge t-Risk Practitioner*

Add the t-Risk Badge to Your Professional History and Share It!

For more information, contact us.