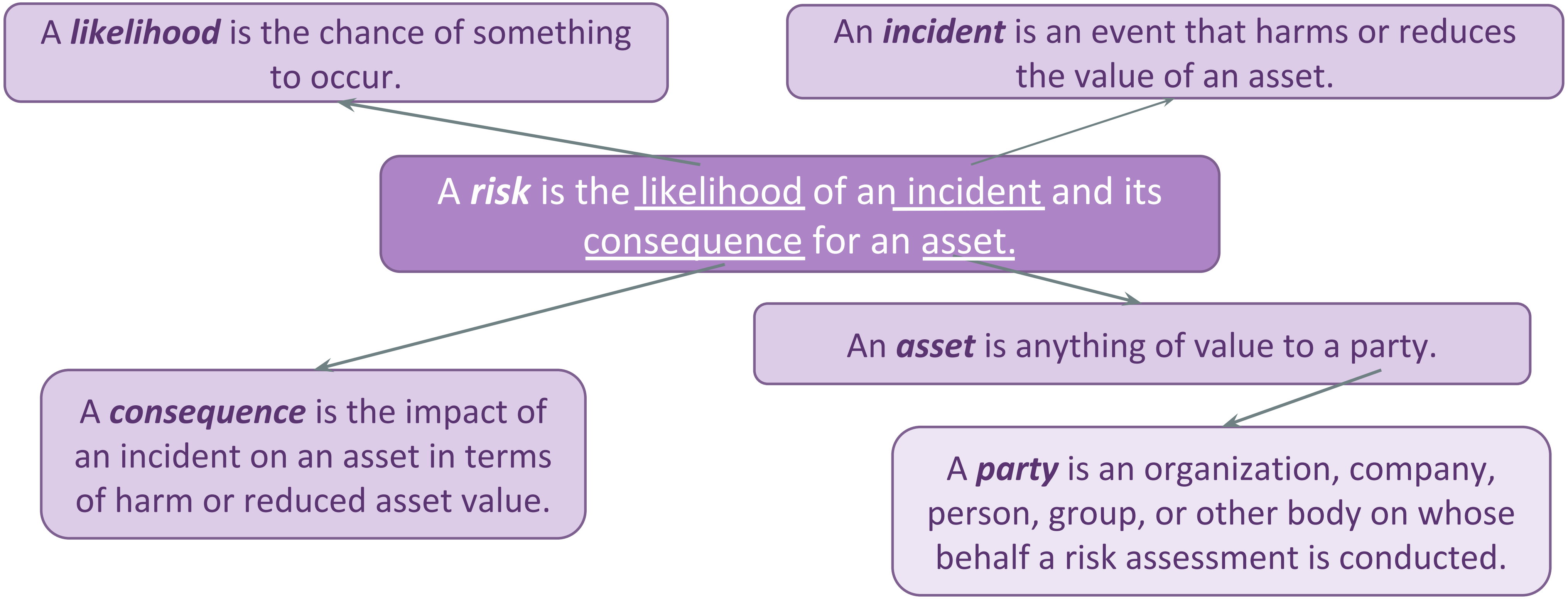
Security Governance
Master of Science in Cyber Security

AA 2023/2024

AN INTRODUCTION TO RISK MANAGEMENT

What is Risk?

Informally a *risk* is the potential that something goes wrong and thereby causes harm or loss.



A ***likelihood*** is the chance of something to occur.

An ***incident*** is an event that harms or reduces the value of an asset.

A ***risk*** is the likelihood of an incident and its consequence for an asset.

An ***asset*** is anything of value to a party.

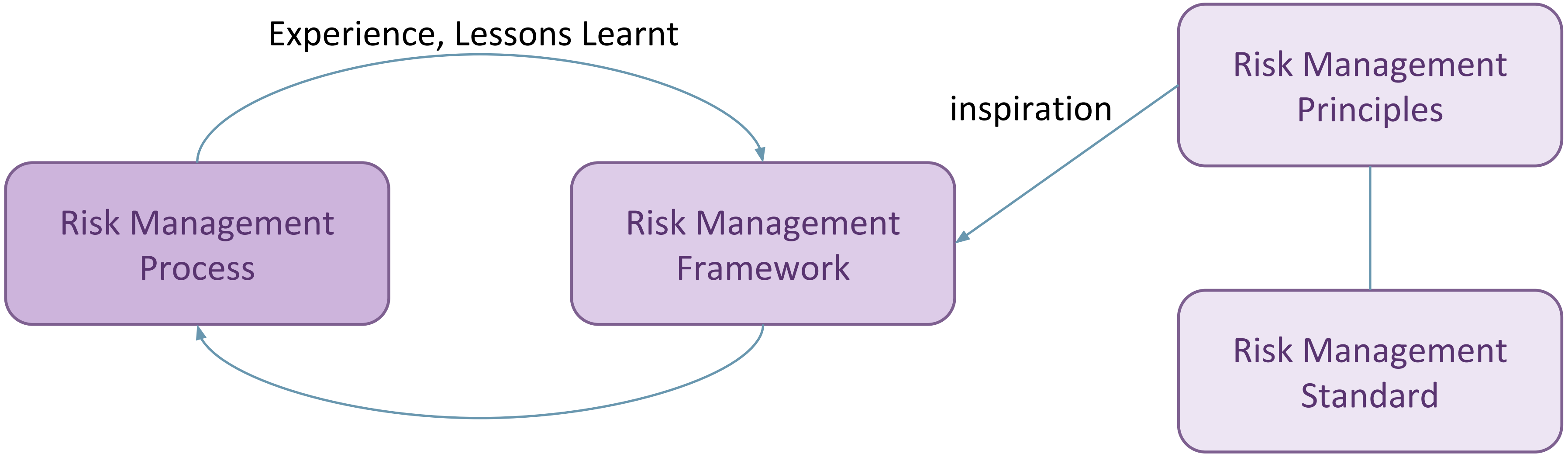
A ***consequence*** is the impact of an incident on an asset in terms of harm or reduced asset value.

A ***party*** is an organization, company, person, group, or other body on whose behalf a risk assessment is conducted.

What is Risk Management?

Risk management comprises coordinated activities to direct and control an organization with regard to risk.

Requirement: A risk management process must be adequate, efficient, and effective.



Experience, Lessons Learnt

inspiration

Risk Management Principles

Risk Management Process

Risk Management Framework

Risk Management Standard

A Standard for Risk Management: ISO 31000

ISO 31000 provides guidelines on managing risk faced by organizations and can be customized to any organization and its context.

It provides a common approach to managing any type of risk and is not industry or sector specific.

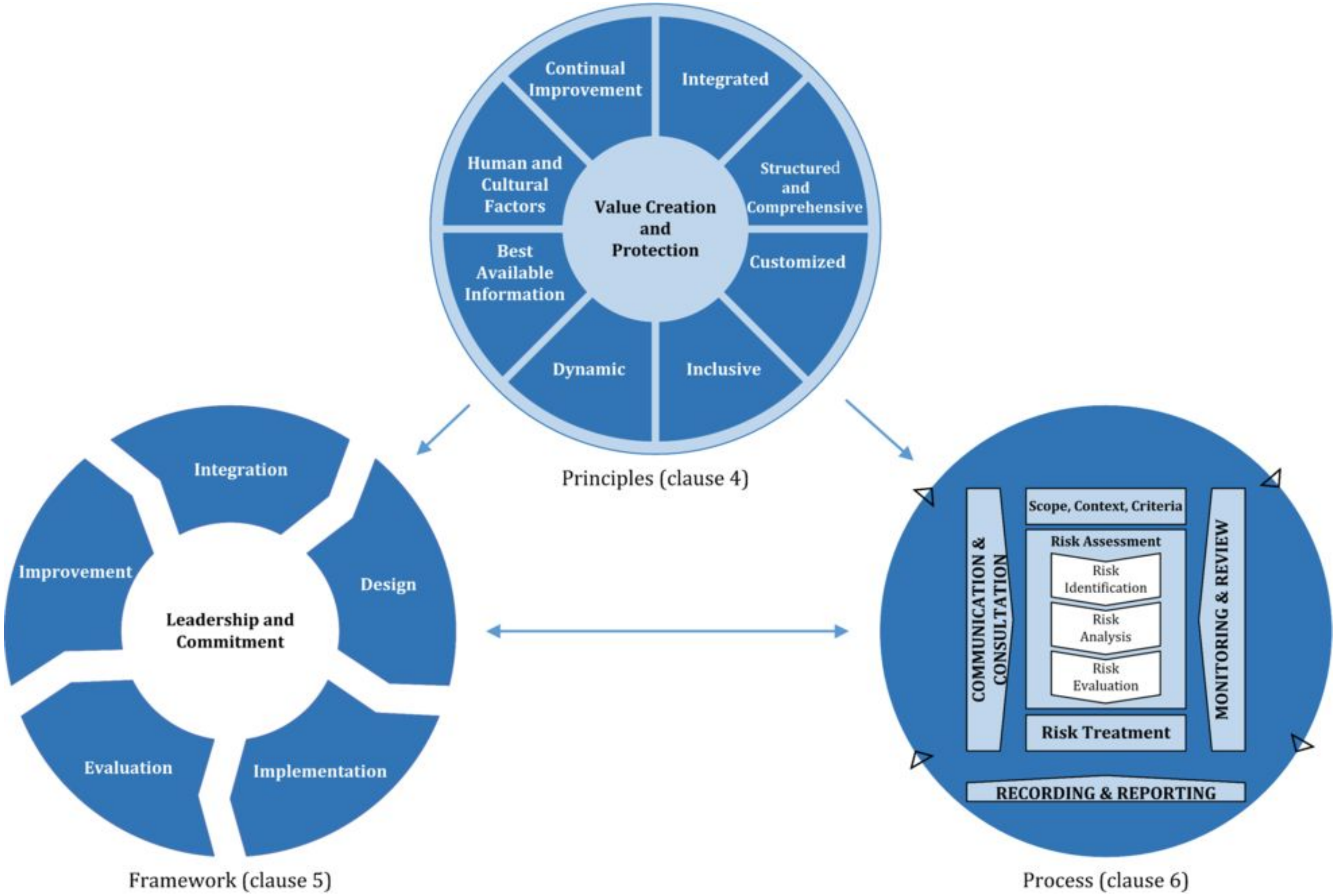
It can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes.

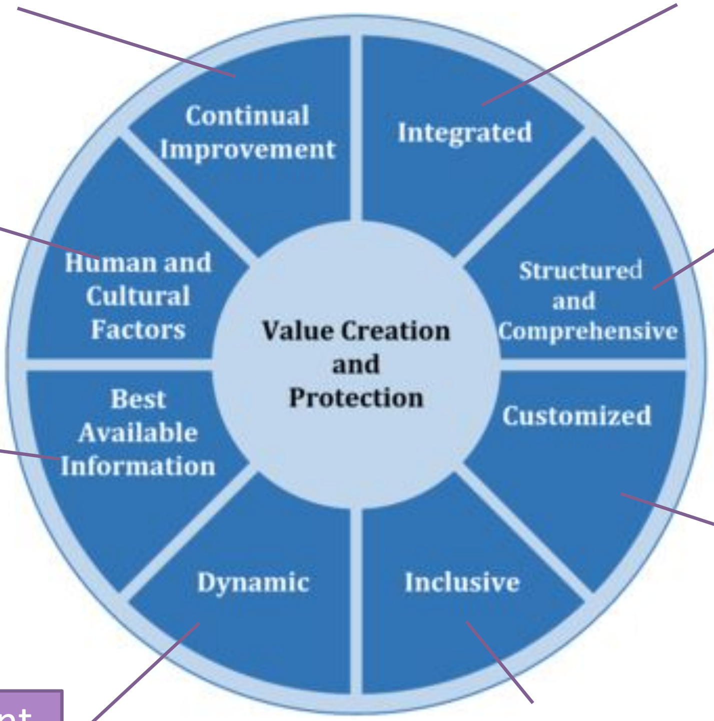
- Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance

Last Release: 2018

ISO 31000


Continual Improvement
Integrated
Human and Cultural Factors
Structured and Comprehensive
Value Creation and Protection
Best Available Information
Customized
Dynamic
Inclusive
Principles (clause 4)
Integration
Improvement
Design
Leadership and Commitment
Evaluation
Implementation
Framework (clause 5)
COMMUNICATION & CONSULTATION
Scope, Context, Criteria
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
MONITORING & REVIEW
RECORDING & REPORTING
Process (clause 6)

ISO 31000 - Principles


Continual Improvement
Integrated
Human and Cultural Factors
Value Creation and Protection
Structured and Comprehensive
Best Available Information
Customized
Dynamic
Inclusive

Through learning and experience

Risk Management is an integral part of all organizational activities

Influence all aspects of risk management

A structured and comprehensive approach to risk management contributes to consistent and comparable results

Information and uncertainty is the base for RM activities. They must be timely, clear and available to relevant stakeholders

RM framework and processes are customized and proportionate to the organization’s external and internal context related to its objectives

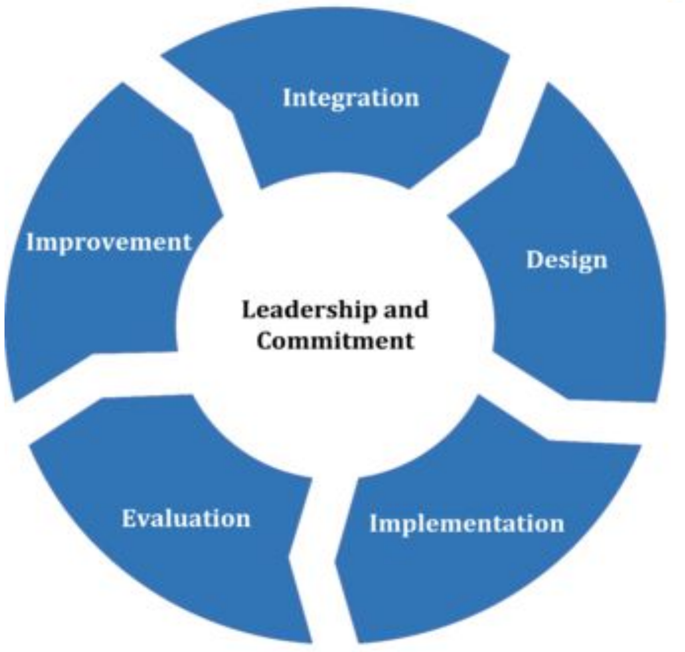
Changes must be taken in to account and managed in an appropriate and timely manner

Involving stakeholders increases awareness and informed risk management

ISO 31000 - Framework

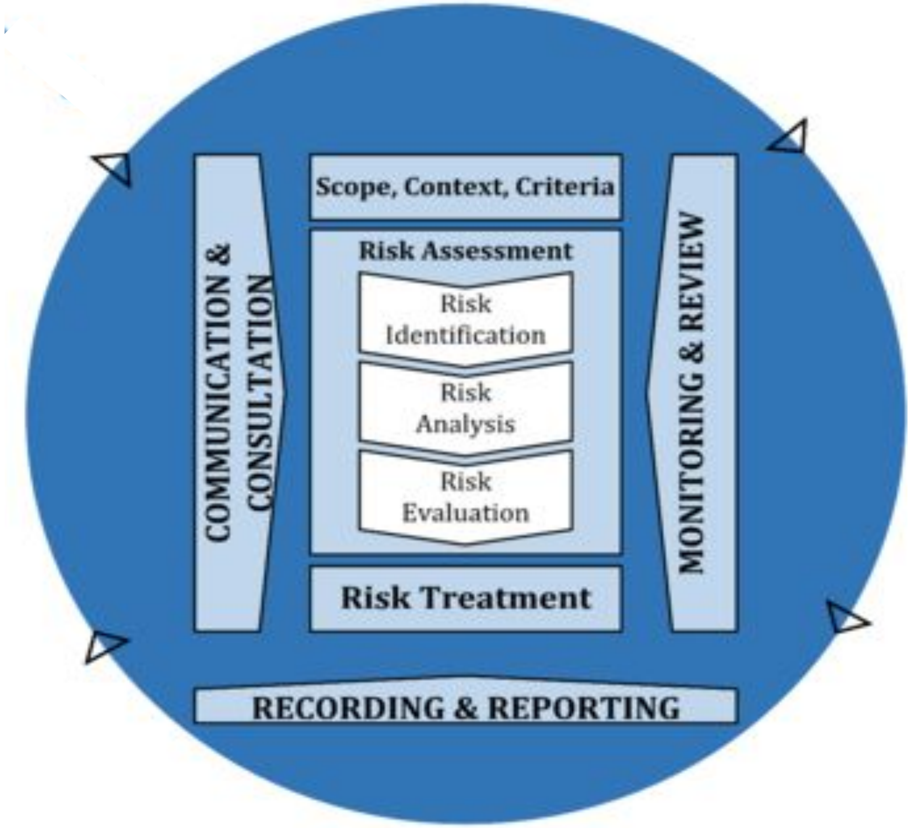
Purpose - assist the organization in integrating risk management into significant activities and functions

Effectiveness - depends on the framework integration into the governance of the organization, including decision-making.



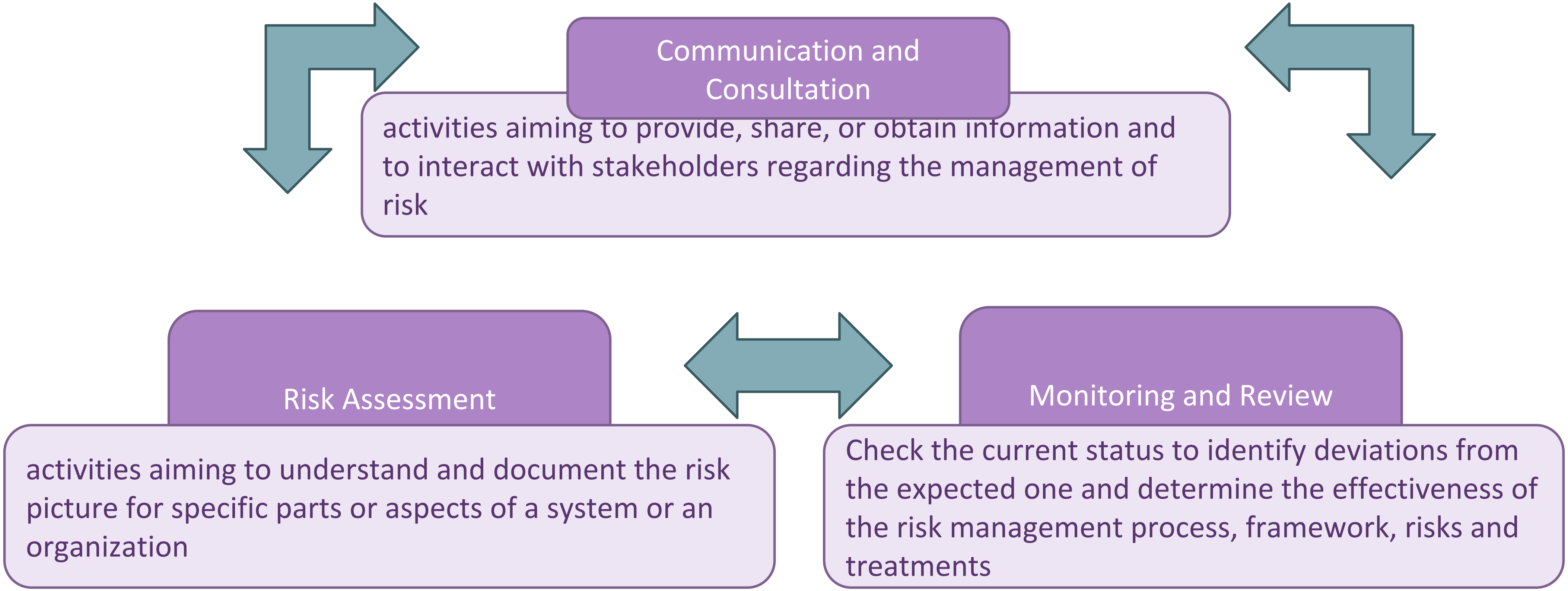
ISO 31000 - Process

Suggests how to structure processes involved in the risk management activities



Risk Management General Process

It is composed by 3 main sub-processes



Communication and Consultation

activities aiming to provide, share, or obtain information and to interact with stakeholders regarding the management of risk

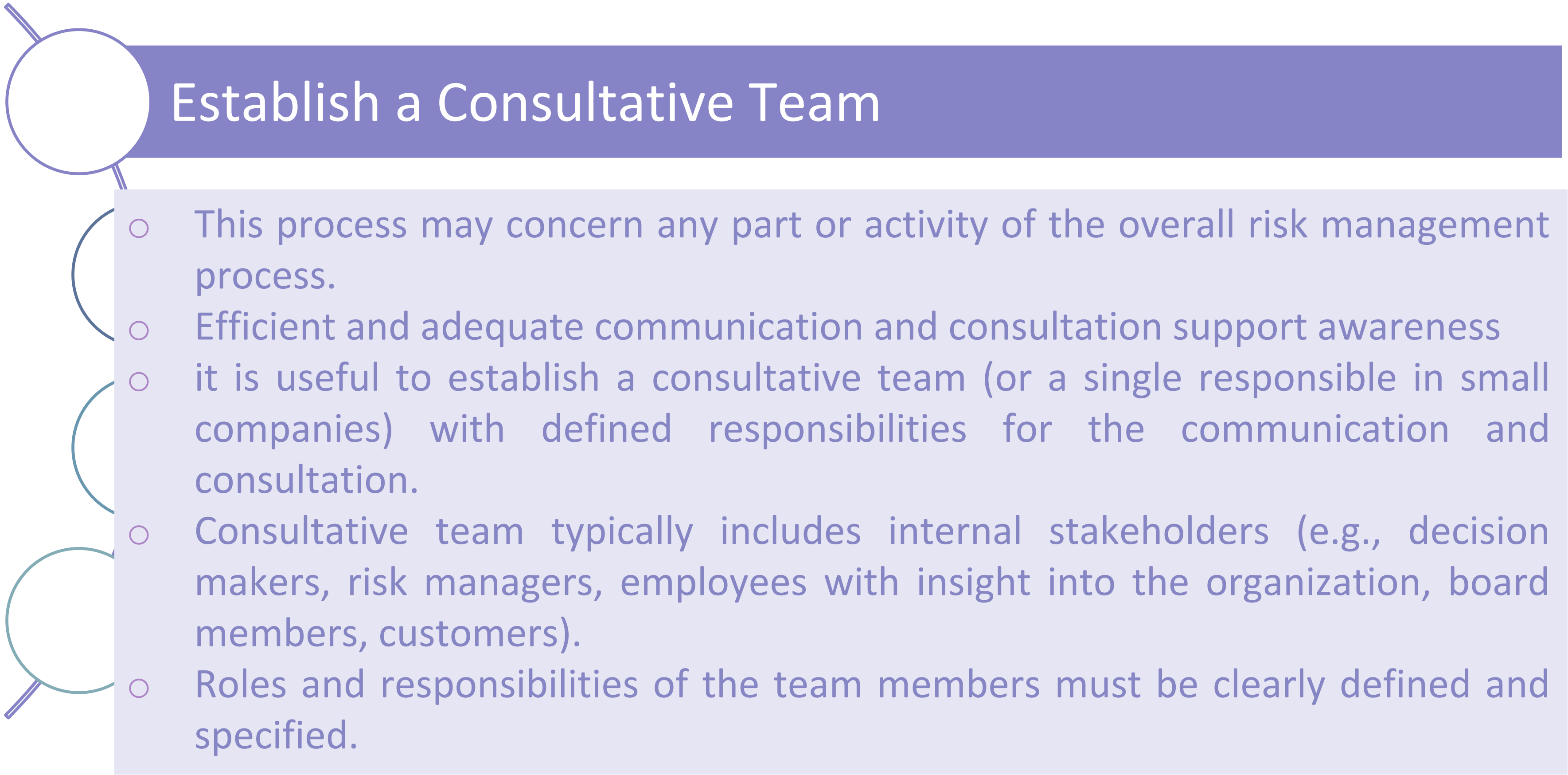
Risk Assessment

activities aiming to understand and document the risk picture for specific parts or aspects of a system or an organization

Monitoring and Review

Check the current status to identify deviations from the expected one and determine the effectiveness of the risk management process, framework, risks and treatments

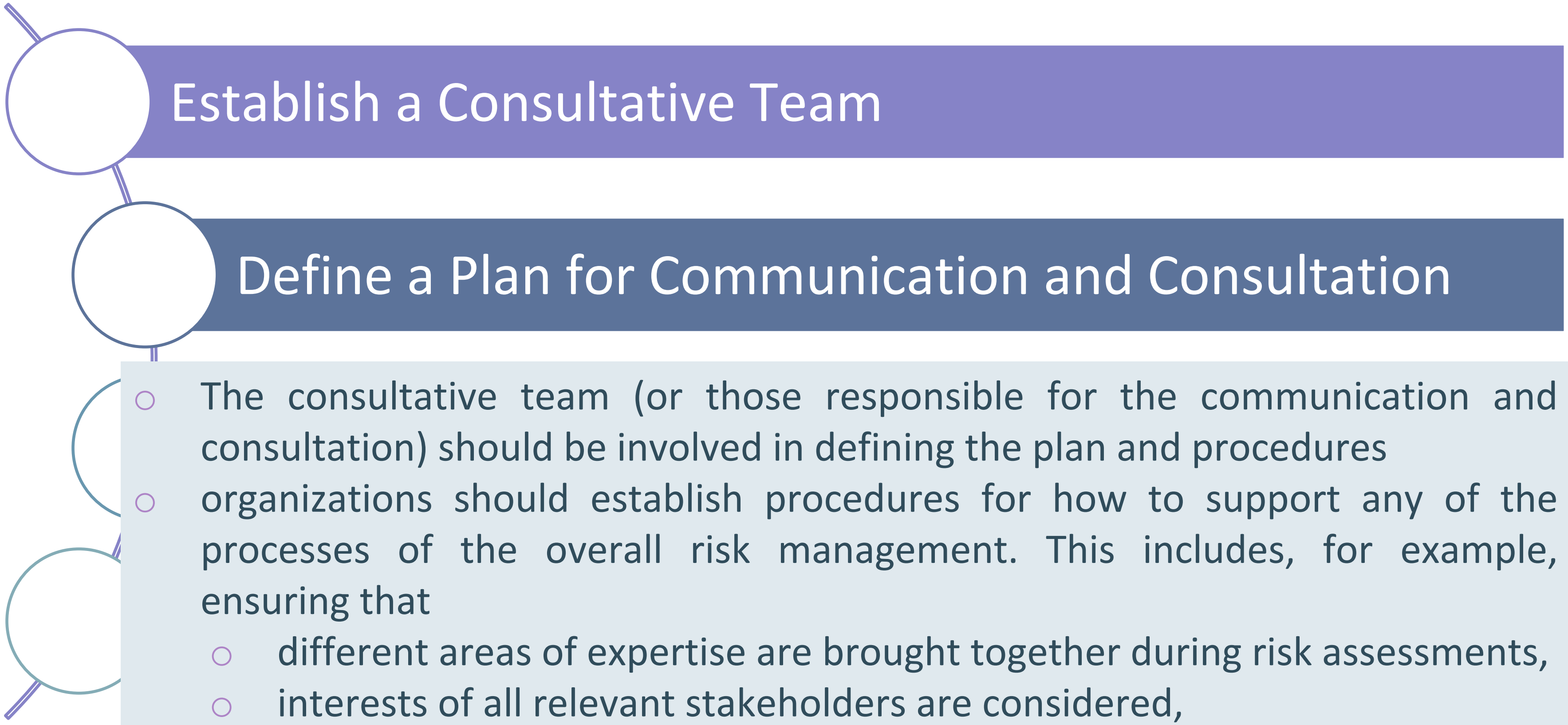
Communication and Consultation



Establish a Consultative Team

- This process may concern any part or activity of the overall risk management process.
- Efficient and adequate communication and consultation support awareness
- it is useful to establish a consultative team (or a single responsible in small companies) with defined responsibilities for the communication and consultation.
- Consultative team typically includes internal stakeholders (e.g., decision makers, risk managers, employees with insight into the organization, board members, customers).
- Roles and responsibilities of the team members must be clearly defined and specified.

Communication and Consultation



Establish a Consultative Team

Define a Plan for Communication and Consultation

- The consultative team (or those responsible for the communication and consultation) should be involved in defining the plan and procedures
- organizations should establish procedures for how to support any of the processes of the overall risk management. This includes, for example, ensuring that
  - different areas of expertise are brought together during risk assessments,
  - interests of all relevant stakeholders are considered,
  - risk evaluation criteria are appropriate, and
  - decision making is informed.

Communication and Consultation

- good procedures for communication and consultation help to ensure endorsement of and support for the risk management process
- it is important to achieve a common agreement on and mutual understanding of how risk should be managed

Ensure Endorsement of the Risk Management Process

Communicate Risk Assessment Results

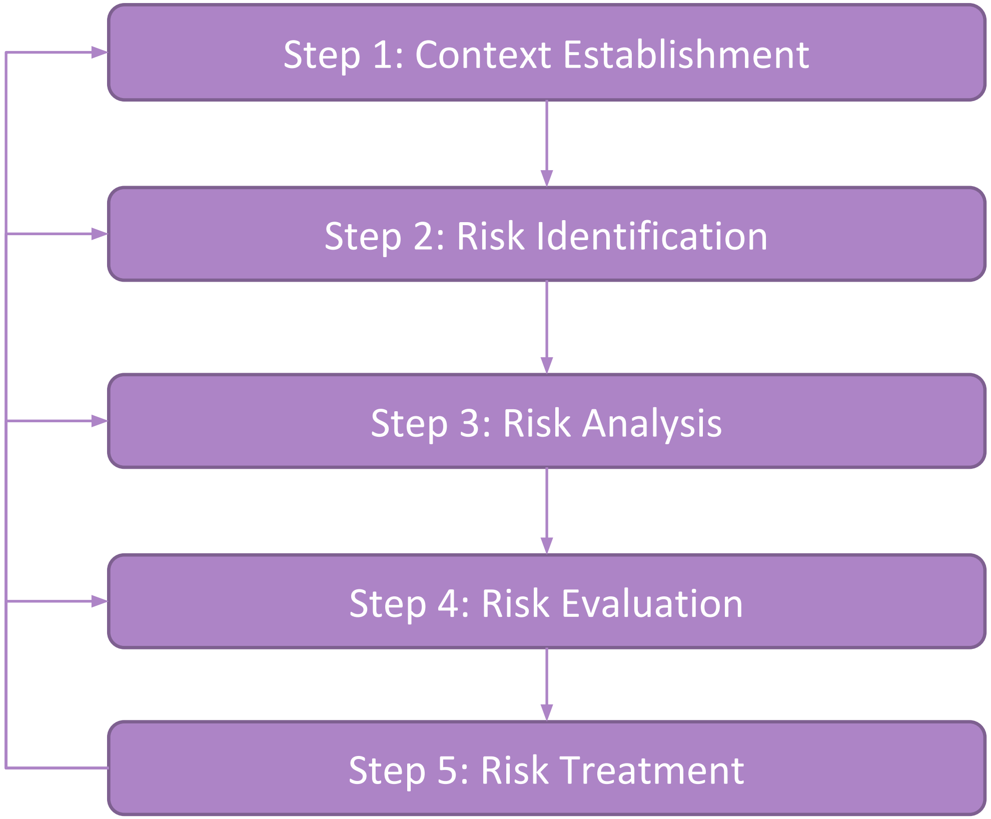
Communication and Consultation

- The risk assessment results may be important for
  - demonstrating policy adherence or compliance with directives and regulations.
  - justifying treatment plans, including the required resources for risk mitigation.
- Communicating the results helps those with a vested interest to understand the basis on which decisions are made and why particular actions are required.
- This, in turn, helps to ensure endorsement of risk treatment plans from key stakeholders.

Communicate Risk Assessment Results

Risk Assessment

The risk assessment process is divided in 5 steps



Context Establishment

GOAL

Identify and Describe the Context of the Risk Assessment process

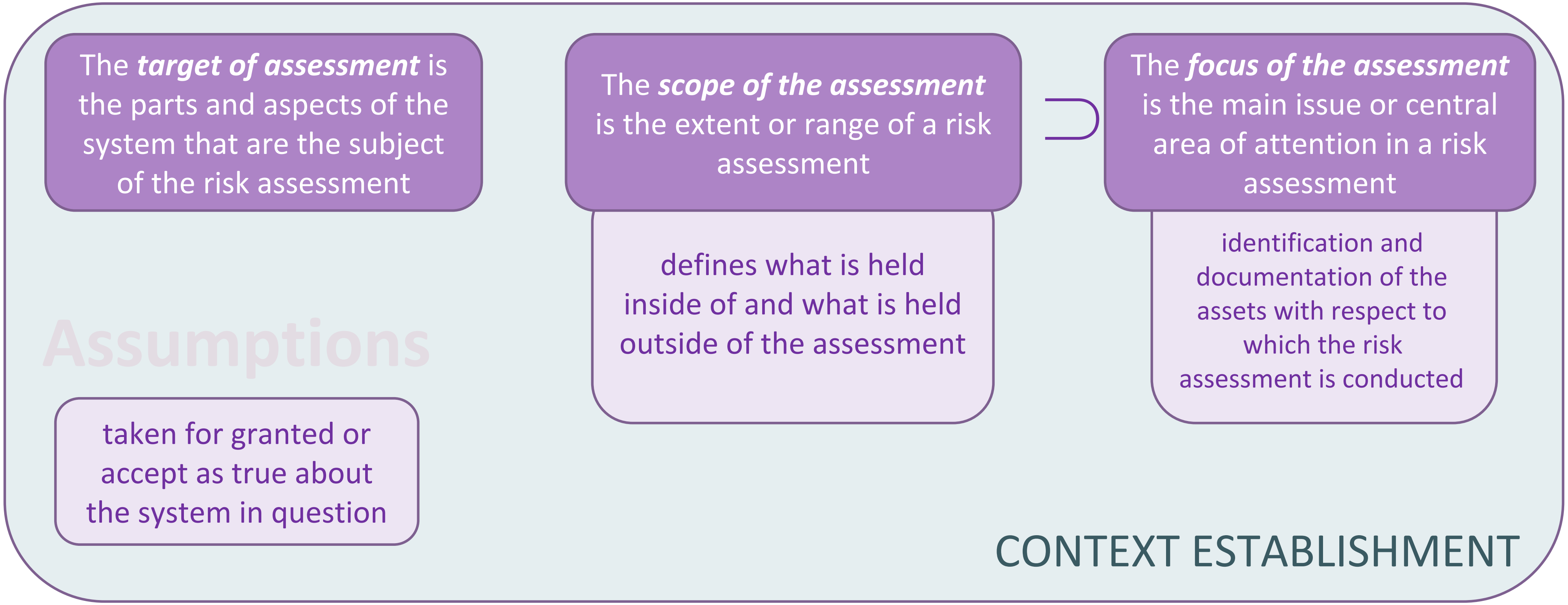
The first task to perform is the identification (and documentation) of the context relevant for the assessment

- *External Context*: description of societal, legal, regulatory, and financial environment and of the relationships with external stakeholders
- *Internal Context*: description of relevant goals, objectives, policies, and capabilities that may determine how risk should be assessed

Then, goals and objectives of the risk assessment must be defined

- participation of decision makers is needed

Context Establishment



The ***target of assessment*** is the parts and aspects of the system that are the subject of the risk assessment

The ***scope of the assessment*** is the extent or range of a risk assessment

⊃

The ***focus of the assessment*** is the main issue or central area of attention in a risk assessment

defines what is held inside of and what is held outside of the assessment

identification and documentation of the assets with respect to which the risk assessment is conducted

Assumptions

taken for granted or accept as true about the system in question

CONTEXT ESTABLISHMENT

Context Description

The context description is the input for the risk assessment process and must contain:

1. Identification of the party involved in the Assessment
2. Assumption declaration
3. Relevant Assets identification for the Risk Assessment (focus of the assessment)
4. Risk scales Definition
    1. for consequences and likelihoods
    2. they can be quantitative or qualitative, continuous, discrete, or given as intervals.
5. risk evaluation criteria (terms of reference by which the significance of risk is assessed)

Risk Identification

The risk identification is the set of activities aiming to identify, describe, and document risks and possible causes of risk

Observation 1: a risk is always associated with an incident

Observation 2: there are three elements without which there can be no risk

Without assets there is nothing to harm

Without vulnerabilities there is no way to cause harm

Without threats there are no causes of harm

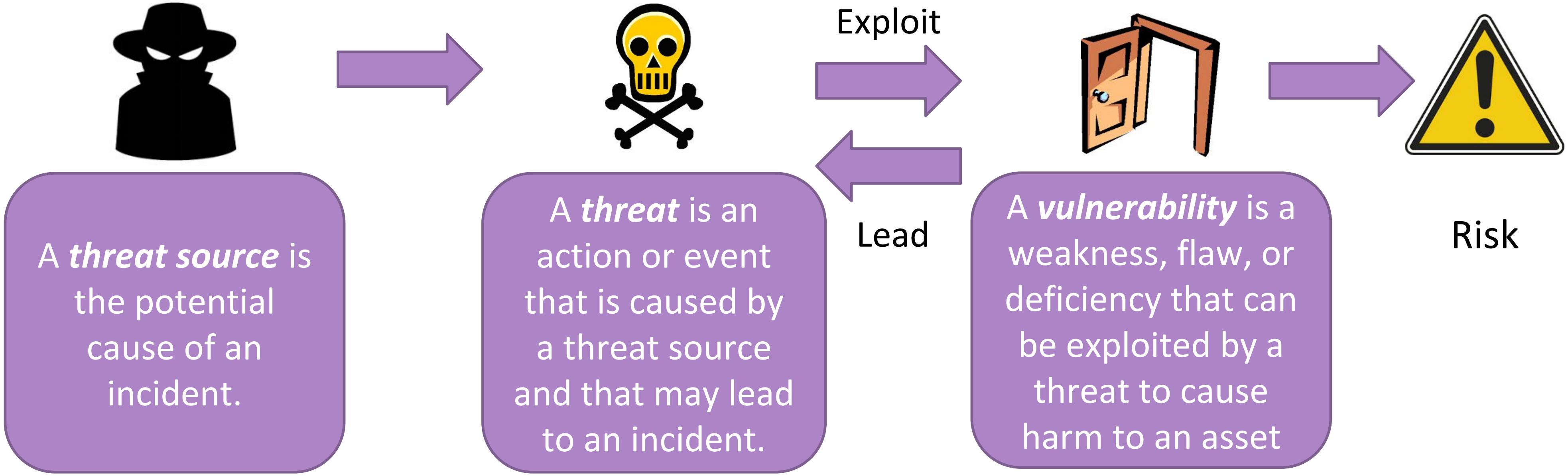
Risk Identification

Our Scope

Conduct the risk identification with respect to the identified assets by

1. identifying threats and
2. understanding how the threats may lead to incidents (and thereby risks) by exploiting vulnerabilities

A bit of Terminology



A ***threat source*** is the potential cause of an incident.

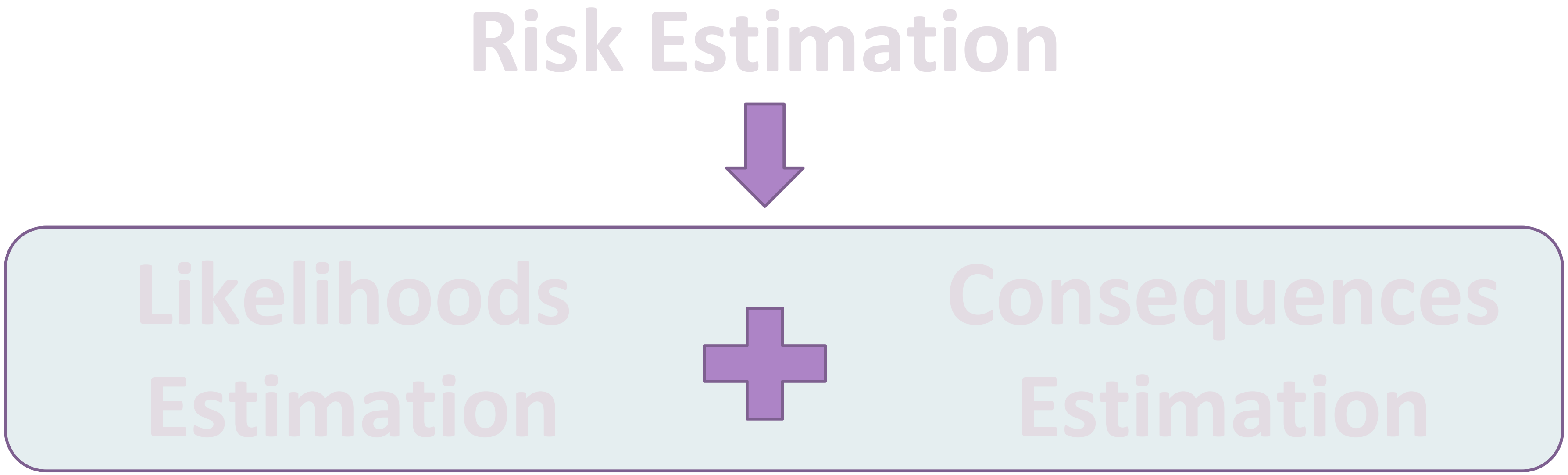
A ***threat*** is an action or event that is caused by a threat source and that may lead to an incident.

A ***vulnerability*** is a weakness, flaw, or deficiency that can be exploited by a threat to cause harm to an asset

Risk Analysis

The risk analysis is the activity aiming to estimate and determine the level of the identified risks

Observation 1: the risk level is derived from the combination of the likelihood and consequence



Risk Estimation

Likelihoods Estimation

Consequences Estimation

Likelihoods Estimation

Likelihood estimation is to determine the frequency or probability of incidents to occur using the defined likelihood scale.

It requires the use of techniques for gathering empirical data.

Many of the risk-modelling techniques (i.e., Bayesian networks, attack trees, and CORAS diagrams) support the likelihood estimation and documentation

Very often, we need to understand how risks are most likely to arise, and which threat sources are most important.

- try to estimate the likelihood that threat sources initiate threats,
- try to estimate the likelihood that such threats may lead to incidents.

Consequences Estimation

RECALL: An incident represents one risk for each of the assets it harms

Thus, it is necessary to estimate the consequence for each of these assets.

The consequence estimation should be conducted by a walk-through of all identified incidents and assigning the estimates with the involvement of personnel representing the party or someone who can judge consequences on behalf of the party.

Risk Evaluation

○*The **risk evaluation** is the set of activities involving the comparison of the risk analysis results with the risk evaluation criteria to determine which risks should be considered for treatment*

This step is quite straightforward given the risk estimates and evaluation criteria

However, some steps have to be done

1. Consolidation of risk analysis results: focus on the risk estimates that we are uncertain about and where this uncertainty implies doubt about the actual risk level
2. Evaluation of risk level
3. Risk aggregation: investigate the identified risks to see whether certain sets of risks should be aggregated and evaluated as a single risk
   - avoid to accept a set of risks that individually are non-critical, yet unacceptable in combination
   - Investigate situation where a number of separate incidents harm the same asset or where the incidents may be caused by the same threat.
4. Risk grouping: group risks that have elements in common

Risk Treatment

The ***risk treatment*** is the set of activities aiming to identify and select means for risk mitigation and reduction

In principle, we should seek to treat all risks that are unacceptable, but in the end this is a question of cost and benefit, no matter the risk level

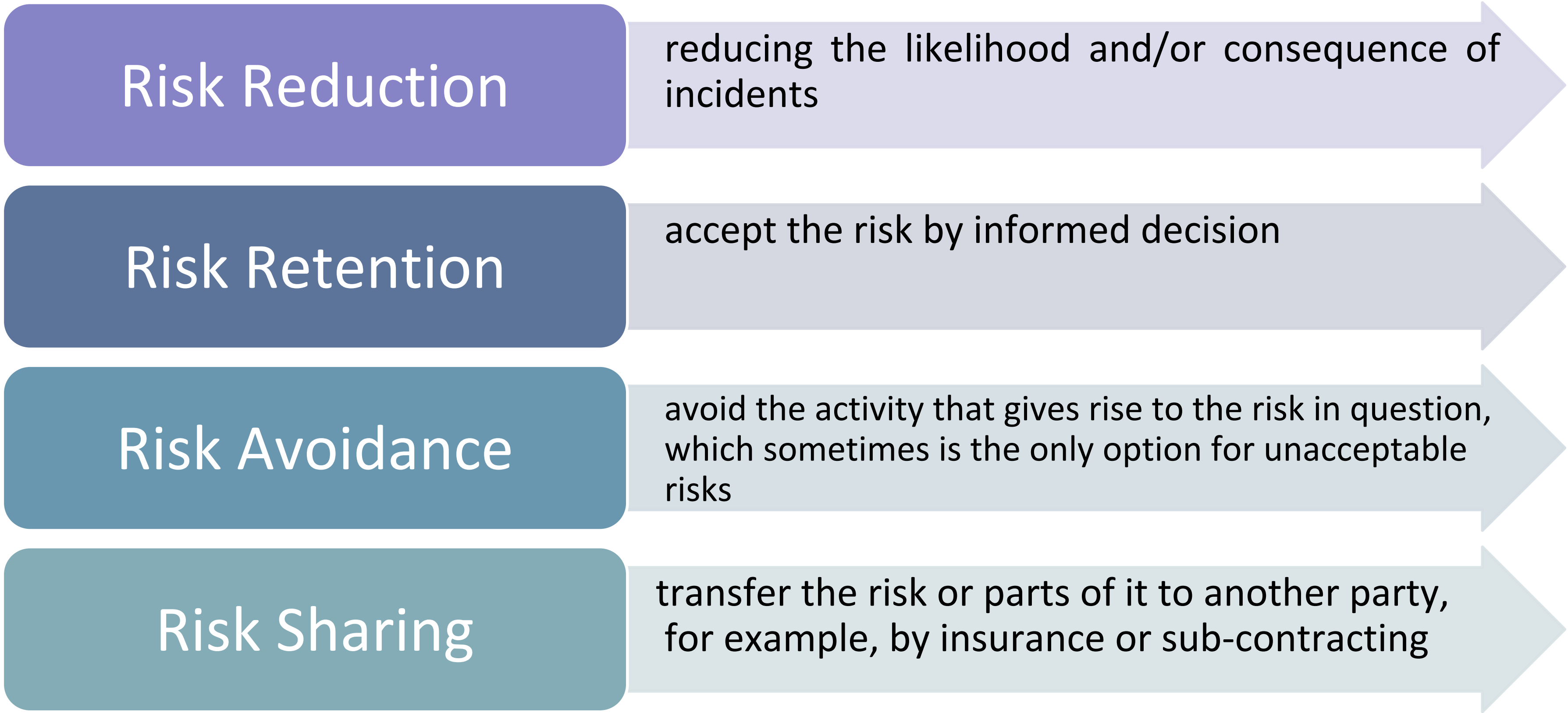
- if a low risk is very cheap to eliminate, we might do so even if the risk in principle is acceptable.
- if the cost of treating a very high risk is unbearable there may be no other option than to accept it.

The risk treatment activity, therefore, should involve both the identification and the analysis of treatments

The analysis should take into account that some treatments can create new risks, and that some groups of treatments can reduce the isolated effect of each other.

Risk Treatment

There are four main options for risk treatment



Risk Reduction

reducing the likelihood and/or consequence of incidents

Risk Retention

accept the risk by informed decision

Risk Avoidance

avoid the activity that gives rise to the risk in question, which sometimes is the only option for unacceptable risks

Risk Sharing

transfer the risk or parts of it to another party, for example, by insurance or sub-contracting

Monitoring and Review

Monitoring is the continual checking, supervising, critically observing, or determining the current status in order to identify deviations from the expected or required status.

The ***review*** activity is to determine the suitability, adequacy, and effectiveness of the risk management process and framework, as well as risks and treatments.

Monitoring and review apply to

- the underlying risk management framework
- the risk management process
- to the identified risks
- to the measures that the organization implements in order to treat risks

Monitoring and Review

The main purposes of Monitor and Review process are:

- Ensure that controls are effective and efficient
- Obtain further information to improve risk assessment
- Analyse and learn lessons from incidents, changes, trends, successes, and failures
- Detect changes
- Identify emerging risks

Monitoring and Review of Risks

Risks are not static and must therefore be monitored and reviewed

The monitoring and review of risk serves as a basis for taking actions, such as modifying the risk picture or conducting new risk assessments

Asset

Check changes in

- asset value or priority over time
- internal or external context

Vulnerability

- Check vulnerability that potentially could be exposed to new threats
- Check vulnerability parameters (e.g., exploitability, diffusion, etc.)

Threat

Check changes in

- Internal or external changes

Sometimes new threats can be observed directly, sometimes a new risk assessment is needed

Monitoring and Review of Risk Management

WHY MONITORING AND REVIEW OF THE RISK MANAGEMENT PROCESS?

To ensure that the framework and process, as well as all related activities, procedures, roles, and responsibilities, remain relevant, appropriate, and adequate for the organization

WHAT SHOULD BE MONITORED?

Changes in the internal or external context that may affect the adequacy of the risk management. This may include the following:

- Legal and environmental context
- Competition context
- Assets and asset values
- Risk evaluation criteria
- Resources required for adhering to the risk management framework