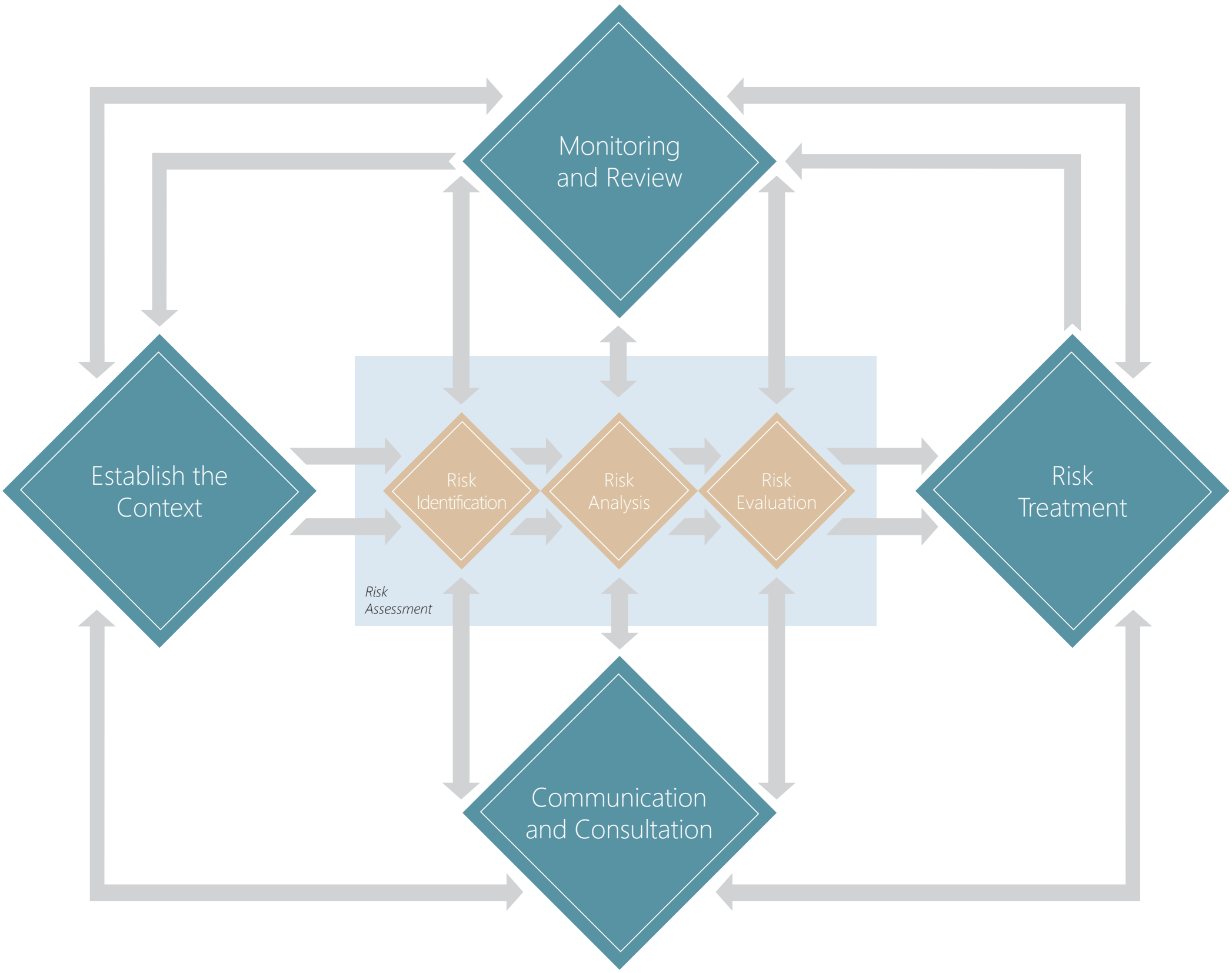
ISO 31000

Risk Management Process

ISO 31000 provides a set of process-orientated guidelines for Risk Management, used globally across the public and private sectors.

It is also used as the benchmark for Risk Management within ITIL, where it is an important part of many of the processes in the service lifecycle.



Risk assessment consists of three steps:

- Risk Identification
- Creation of a list of risks based on events impacting the organization's objectives
- Risk Analysis
- Understanding the risks as an input to evaluation and plan for treating the risks
- Risk Evaluation
- Make decisions about which risks require treatment and relative prioritization

ISO 31000 was published in November 2009 and is the first set of international guidelines for risk management, intended to be applicable and adaptable for 'any public, private or community enterprise, association, group or individual.'

ISO 31000 is a process-oriented rather than a control-oriented approach to risk management, and provides guidance on a broader, more conceptual basis, rather than specifying all aspects of an organization's risk assessment and management approach. ISO 31000 was published as a standard without certification.

ISO 31000 defines risk as 'the effect of uncertainty on objectives' and identifies the necessary components of a risk framework as:

- Mandate and commitment
- Design of framework for managing risk
- Understanding the organization and its context
- Establishing risk management policy
- Accountability
- Integration into organizational processes
- Resources
- Establishing internal communication and reporting mechanisms
- Establishing external communication and reporting mechanisms
- Implementing risk management
- Monitoring and review of the framework
- Continual improvement of the framework.

Risk treatment involves the modification of risks using one or more approaches including:

- Avoiding the risk by not carrying out the actions creating the risk
- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties
- Retaining the risk by informed decision