INTRODUCTION TO RISK MANAGEMENT

WHAT IS RISK

As you may have noticed, in the literature there are a lot of different definitions of risk. At BELRIM, we like to pose risk as any potential event - positive or negative - or uncertainty on the achievement of any organisation's strategic and operational objectives. Risk is measured in terms of consequences (impact) and likelihood. Lost opportunities should also be considered as risks.

OUR DEFINITION OF RISK MANAGEMENT

Again, a variety of different risk management definitions exists in the literature. We define risk management as a continuous, proactive and systematic process of identifying, assessing, and managing risks in line with the organisation's risk appetite, to provide reasonable assurance with regards to the achievement of the objectives.

The aim of risk management is not to avoid risks at all costs, but as a minimum to identify the risk that an organisation is exposed to and whether mitigating factors are or should be in place. Risk management offers an integrated approach to the identification, evaluation, mitigation and monitoring of risks. It should be applied to the entire organisation across all its levels: areas, functions and activities. It will strengthen the linkages between the different activities of the organisation and its overall objectives.

Risk management needs to be:

- Proportionate to the level of risk within the organisation and the amount of risk an organisation is ready to accept.
- Aligned and embedded within business activities.
- Comprehensive, systematic, structured, dynamic, iterative and responsive to change.

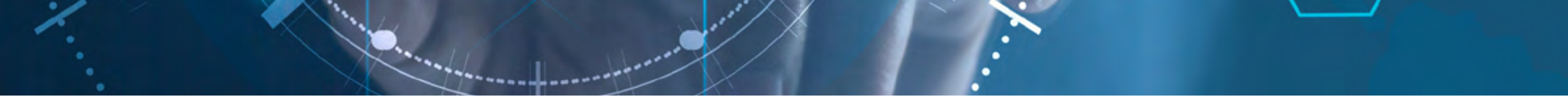
FROM COSO TO ISO

A variety of risk management frameworks/standards were developed by recognised organisations. Those frameworks can be used in establishing risk management. They provide the foundations and organisational arrangements that will be embedded within the organisation and assist the organisation in managing its risks effectively through the risk management process. A risk management framework also ensures that risk information derived from the risk management process is adequately reported and used as a basis for decision making and accountability at relevant levels of the organisation. While all these frameworks are suitable for risk management, do note that it is important to adapt the framework to the size and environment of your organisation.

OVERVIEW OF WIDELY RECOGNISED RISK MANAGEMENT FRAMEWORKS (NON-EXHAUSTIVE)

1992	1995	2002	2004	2008	2009	2017	2018
COSO Internal Control	Criteria of Control (CoCo)	ISO Guide 73:2002 SOx 2002 Institute of Risk Management	COSO ERM 2004 Orange Book AS/NZ 4360:2004	BS 31100	ISO Guide 73:2009 ISO 31000:2009	COSO ERM 2017	ISO 31000:2018

BELRIM
Belgian Risk Management Association



ADDED VALUE

The added value of risk management translates to different domains: compliance, assurance, efficiency of operations and decision making. Generally, effective risk management can strengthen the communication process, support strategic and operational management decisions, trigger new ideas and solutions, and provide useful information for establishing appropriate control strategies (less control in certain areas, more/better control in others). A structured and consistent management approach facilitates the coordination, analysis and management of risks at organisational level.

SUCCESSFUL RISK MANAGEMENT GOVERNANCE

The success of risk management depends on the effectiveness of the governance implemented. Therefore, clear roles and responsibilities towards risk management need to be defined. Risk owners are key, as they are responsible for defining concrete action plans for the risk mitigation.

RISK MANAGEMENT PROCESS STEP BY STEP

Preparation	Risk identification	Risk documentation	Risk evaluation	Risk response	Risk monitoring (Recurring exercise)
Establish risk appetite, define risk typology and impact and likelihood scales	Identify risks through document analysis (internal and external) and interviews/ workshops with stakeholders	Develop a risk register and document risks with analysis of possible causes and effects	Evaluate and prioritise top risks	Develop risk responses and action plans to mitigate priority risks	Develop a risk register and document risks with analysis of possible causes and effect

RISK TREATMENT

Risk treatment involves selecting one or more options for modifying risks and implementing those options. It is a cyclical process of assessing a risk treatment:

- Deciding whether residual risk levels are tolerable or not.
- If not tolerable, generating a new risk treatment.
- And assessing the effect of that treatment until the residual risk reaches an acceptable level for the organisation.

TRANSFER, TERMINATE, TOLERATE OR TREAT?

In principle, there are four possible options when treating risks (also known as '4Ts'). However, the categorisation of risk treatment is not an end in itself; it should merely be seen as guidance.

- **Terminate** or avoid the risk by changing or modifying the objectives.
- **Transfer** or share the risk with a third party (insurance company, outsourcing, clients and suppliers agreement).
- **Treat** or reduce the risk by implementing effective controls and other measures such as training, information, etc.
- **Tolerate** or accept the risk because of cost/benefit aspects or for other reasons (for example a non-controllable internal or external risk associated with an activity that cannot be discontinued).

Impact ↑		
	Transfer the risk to another party	**Terminate** activity generating risk
	Tolerate the risk and its likely impact	**Treat** the risk to reduce likely impact or exposure
		Likelihood →

Note that organisations are not always able to terminate all risks with high impact and high likelihood as some risks are inherent to their activities and / or not under their control. In those cases, risk management involves selecting other options for modifying the risk and bring it to an acceptable level for the organisation, within management's risk appetite.

CONCRETE ACTIONS TO BE TAKEN

Establishing clear and comprehensive treatment plans is essential for an effective risk management. They are needed to make sure that risks are addressed in line with management's instructions and constitute the benchmark for progress monitoring. In order to establish effective treatment plans, the root causes of risks must be fully analysed and understood - what is the underlying problem? As a minimum, the treatment plans should include a description of the risks and the actions to be taken, the accountable persons of these actions, a determination of costs and benefits, and target dates/milestones.