



RISK APPETITE,
THE CORNERSTONE OF
ENTERPRISE RISK
MANAGEMENT



Enterprise risk management has become a crucial component of contemporary corporate governance and is an evolving discipline that has been supported and promoted throughout years.

While an expanding list of companies has become identified with failure to anticipate and manage risks within their organizations, the changing competitive environments push companies to take risk in order to optimize their profit. It is impossible making profit without taking any risk. And yet, taking such risks without being able to manage them can guide towards collapse. While conducting proper oversight, top management along with the board must tackle the challenge to define how much risk is acceptable in following their objectives. The key enabler is to understand the level of risk they are willing to accept.

Risk appetite is an essential business concept that makes a significant distinction to how organizations are governed. Risk appetite is the amount of risk which the company is willing to accept. It is a key enabling structure and active relation among risk management, strategy and target setting. Every organization follows different aims to add value, and should generally recognize the acceptable level of risk in doing so.

External stakeholders and different divisions of the organization usually have different perceptions. Lot of organizations consider risk appetite as the focus of appealing theoretical discussions regarding risk, but do not successfully incorporate the theory into their daily activities or day-to-day decision making process. Once a board identifies a strategy, it should decide whether it supports the level of risk appetite.

Consequently, an organization must recognize risk appetite along with operational strategies or objectives. Thus, management must pursue three main steps:

1. Develop risk appetite
2. Communicate risk appetite
3. Monitor and update risk appetite

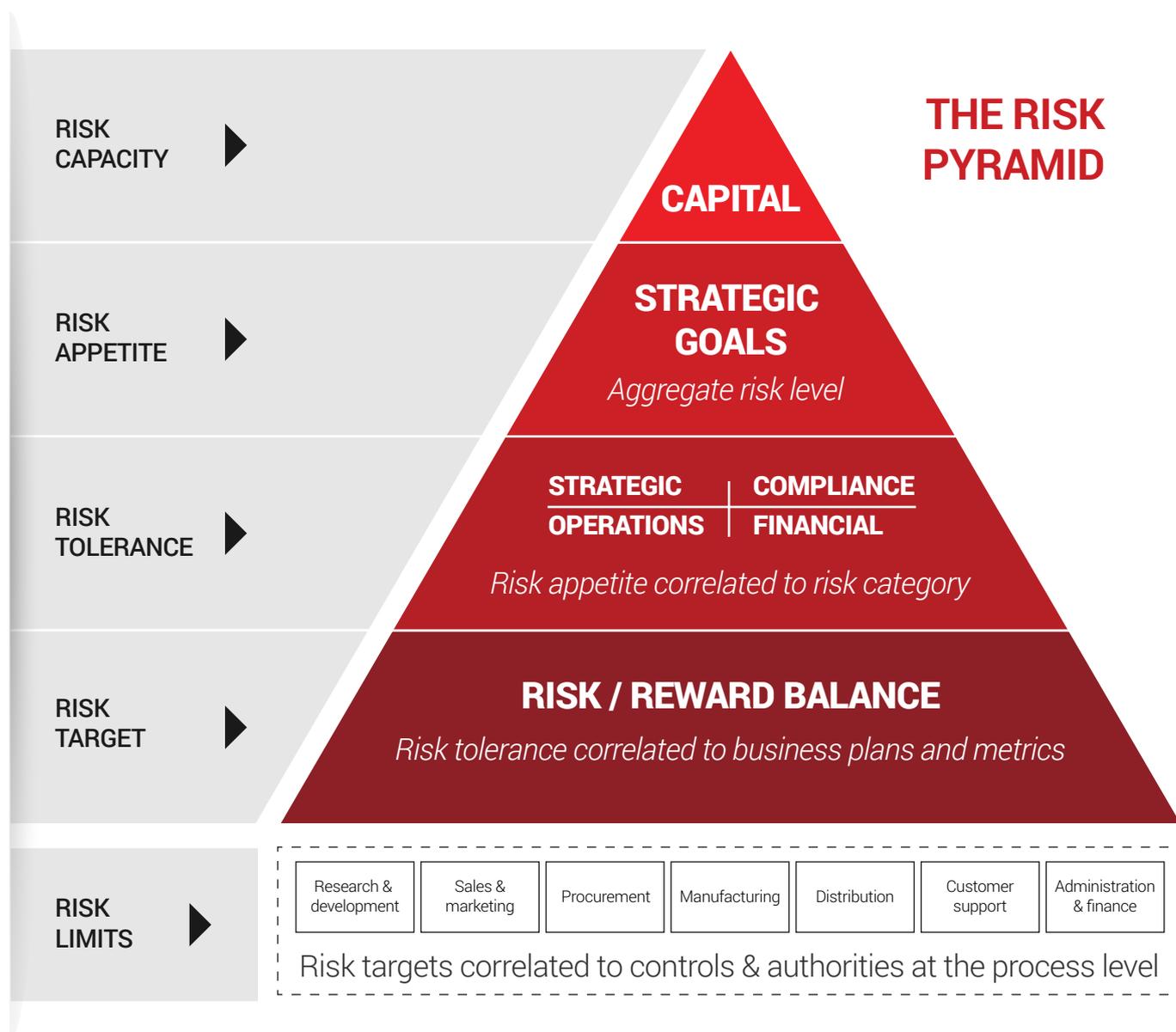
Most importantly, communicating risk appetite correctly leads the organization towards considerable benefits. Those benefits encompass:

1. Transparency over the risks
2. Fundamentals for reliable communication to different stakeholders
3. Reduces cost of capital
4. Competitive advantage

Other benefits include more precise financial reporting, superior marketplace presence, enhancement of both perception of the organization and political and community support.

The best approach to initiate risk appetite definition is the top-down approach.

THE RISK PYRAMID



The maximum amount of risk in an organization is known as **risk capacity**. The amount of risk must be taken by the company in order to achieve its financial goals. Unlike risk capacity, **risk tolerance** is the specific amount of risk an organization is willing to take in regards with a specific category of risks. Categories of risk include strategic, operational, financial, compliance and reputational risks.

Furthermore, a **risk target** is the most advantageous level of risk that an organization wants to acquire to achieve defined business objectives. And finally, **risk limits** are used to guarantee the real levels of risk that will settle within the agreed-upon risk tolerances. Breaking risk limits will usually act as a trigger for remedial action at the process level.

Enterprise risk management allows management to successfully deal with related risk and uncertainty, boosting the ability to build value. Additionally, ERM can provide practical assurance that management is informed of the degree to which the body is moving toward accomplishment of the goals.

Enterprise risk management consists of eight interconnected elements: Internal and External Environment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Information, Communication and Monitoring. ERM is not firmly a consecutive process, it is a multidirectional process in which nearly any element can and does influence another.



With all above in place, a useful and proven scheme for effectively managing many risks may be applied to streamline risk management and align it to best practices. Such a solution involves adopting an internationally recognized standard such as ISO 31000, which drives the most relevant best-practice from organizations worldwide and tailored to reduce or eliminate bias. ISO 31000 explains the mechanism of risk management implementation. It provides principles; a framework and a process to implement a risk management suite. Moreover, with due cognizance of its own internal and external contexts, an organization must recognize the applicable and relevant obligations and should put into practice a system of controls to attain compliance. Additionally, ISO 31000 distinguishes the significance of feedback by means of two mechanisms: “communicating and consulting” and the “monitoring and reviewing” of performance. Communicating and consulting ensure the engagement of relevant internal and external stakeholders while monitoring and reviewing guarantee that the organization observes risk performance, thereby gaining knowledge from experience and practices.

PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including ISO 31000 Lead Risk Manager Course.

ABOUT AUTHOR:

Alba Keqa is a Portfolio Marketing Manager for Risk & Management at PECB. She is in charge of conducting market research while developing and providing information related to Risk and Management standards. If you have any questions, please do not hesitate to contact: marketing.rm@pecb.com.

CONTRIBUTOR:

David Lannoy is a Senior Enterprise Risk Manager in a global telecommunication company and has vast experience in Risk Management gained over 15 years working in various sectors including transport and finance. He is a regular guest lecturer and master thesis supervisor in well ranked Business Schools. Due to this valuable experience and academic track record, he has been able to join The Institute of Risk Management in London as a Specialist Member and has also become Certified ISO 31000 Risk Professional and Certified PECB Trainer.