Balancing Risk Appetite and Strategy Execution

The national and international market structures keep diverting from their relatively less complex predecessors into more intricate interlacements that often subdue our judgment in discerning opportunities and threats that can profoundly impact not merely the performance of an organization, but its very existence as well. This has led to a greater focus in enterprise governance, an aspect of which is to properly define risk appetite. The COSO ERM Framework defines risk appetite as “the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value.” Simply put, risk appetite is the willingness of an organization to take risk.

ISO 31000 defines risk as the effect of uncertainty, whether negative or positive, on organizational objectives. For this article, risks will be connoted with the possibility of adverse outcomes, whereas situations from which advantages and benefits can be elicited will be labeled as opportunities.

The concept of risk is abstract, and as such the meanings of its derived terms are evasive to the grip of a common comprehension and perception. Risk expectation and the organization’s capacity to deal with risk depend on many factors to whose actual properties we remain oblivious until we ponder on risk in retrospect. Hence, risk appetite will vary depending on the perception of stakeholders. If articulated meticulously, a risk appetite statement converts risk metrics and techniques into strategic decisions, which can:

- Aid an organization in better understanding, and hence managing, its exposure to risk
- Provide a clear and explicit assertion of the top management’s standing towards risk
- Aid top management in making well-informed risk-related decisions
- Aid top management in appropriately and efficiently allocating resources following a risk-benefit trade-off scheme
- Meliorate the transparency of the organization for stakeholders, regulators, and investors

An organization must be decisive and assiduous about the degree of risk it is willing to be subjected to and how it will embed threats and opportunities in its strategy execution. In the pursuit of establishing a risk appetite statement impervious to any shortcomings, the management must firstly apprehend the company’s goals, strategies, risk taking experience, organizational culture pertaining risk, and the organization’s stakeholder perception. Nevertheless, of particular importance is the organization’s ability to manage risk. Risk on its own represents the possibility of adverse outcomes, but when an organization is able to better manage a certain kind of risk as compared to its competitors, it can be considered that that organization has a competitive advantage (in such circumstances, it is advisable for the organization to become more audacious and leverage from this head-start). Once understanding has been gained regarding the company’s values, these values will convolute to the risk appetite’s foundation upon which we analyze the following:

- Risk profile – What are the identified risks and how can they be mitigated or eliminated
- Risk capacity – The kind and amount or risk that an organization can withstand
- Risk tolerance – To what extent an organization can accept deviation in the pursuit of achieving its goals
- Qualitative risk analysis – Classification and ranking of identified risks in an interval scale, including controls
- Quantitative risk analysis – Objectifying risks as much as possible through the means of assigning numeric values to the likelihood of occurrence and impact of possible outcomes, and identifying controls

The outcome of this approach will be a sound framework that can yield a well-defined risk appetite. After the analysis has been carried out, the risk appetite can be articulated and formalized, delineating the organization’s openness towards risk, beginning from a high level and then narrowing it down throughout all the organizational levels.
Once the risk appetite has been articulated and approved by the board of directors, it is the responsibility of the top management to communicate it. By communicating risk appetite, light is shed on other important facets of the organization’s nature as well, such as:

- Corporate values – The risks an organization is willing to take or avoid
- Strategy – How risk is embedded in the organizational strategy
- Stakeholders – How they perceive risk and how much risk they are willing to take on
- Capacity – The amount of risk that the organization can handle

The explicit and formalized enunciation of a risk appetite statement is a relatively recent revelation, and keeping in sight the ever-growing complexities that abound in our environment as a result of expanding global economies and industrial advancements, its role in organization management is ascending in importance. Articulating risk appetite bears the benefit of properly balancing the organization’s capacities to handle risk with the actual risk at hand, by which means the organization’s pursuit in benefiting from opportunities and dissipating unfeasible risk exposure is facilitated. Companies that commit to a risk appetite statement intend either to become more assertive in a more daring market strategy, especially when opportunities where the company has a competitive advantage arise, or to lower its vulnerability from risks whenever it deems that the risk-benefit ratio doesn’t fall in an encouraging domain for challenging risk, which is the case when global crisis surface.

Prior to determining risk appetite, a diligent and attentive analysis must be executed regarding the external and internal organizational context, stakeholder needs and expectations, potential risks, risk occurrence likelihood, risk impact, and risk addressing options. By defining the above, a company can better fathom its position in the market, how it stands in relation to risk, and how well it is able to deal with risks that are in the front-line. ISO has drafted different standards with the aim of addressing the aforementioned points. The most renowned and used standard for this purpose is ISO 31000:2009, which is also the standard upon which ISO relied the drafting of other field-specific risk management standards.
PECB International is a certification body for persons on a wide range of international standards. It offers training on ISO 31000 and certification services for professionals wanting to gain a comprehensive knowledge on risk management, its principles, core subjects, and risk management related issues. This training suits risk and quality professionals, project managers, and consultants wanting to prepare and support an organization in the integration of risk management throughout the organization. In addition, ISO 31000 certification demonstrates you are knowledgeable in identifying, analyzing, controlling, financing, and administrating risks in accordance with ISO 31000.

Risk Management Trainings offered by PECB:

- Certified ISO 31000 Risk Management (3 days)
- Certified ISO 27005 Risk Management (3 days)
- Certified EBIOS Risk Management (1 and 2 days)
- Certified MEHARI Risk Management (1 and 2 days)
- Certified OCTAVE Risk Management (1 and 2 days)

ISO 31000 Risk Manager, ISO 27005 Risk Manager and OCTAVE, MEHARI, and EBIOS Risk Manager are certification schemes accredited by ANSI ISO/IEC 17024.

Besart Grabanica is the Governance, Risk and Compliance (GRC) Course Development Manager at PECB International. He is in charge of developing and maintaining training courses related to GRC. If you have any questions, please do not hesitate to contact him at: grc@pecb.com.

For further information, please visit www.pecb.org