1.3 Establishing risk management policy

TAGS: Risk appetite; Risk Profile; Top management; Commitment; Stakeholder.

To achieve consistency in risk management activities across the organization, the risk management policy should contain a high level overview and description of the risk management process.

The main features of the policy are:

- Definition of corporate risk appetite: the board and senior managers set the risk tolerance level by identifying general boundaries against unacceptable exposure to risk. The corporate risk appetite is then used to shape tolerance levels down the organization (see below);
- Implementation of a risk management standardized process at all levels, to ensure that risk management is an inherent part of how core-business is run (see Ch. 4);
- Top management involvement in risk management framework design (see below);
- Stakeholders' empowerment (see below and see also Section 2, Ch. 1);
- Definition of risk criteria (see Section 2, Ch. 3);
- Definition of a hierarchy of risks (see Section 2, Ch. 3);
- Implementation of a risk management unit/office (see Ch. 2);
- Definition of human resource training policy to support risk management process (see Ch. 2);
- Establishing a communication system (see Section 2, Ch. 1);
- Establishing a reporting system (see Ch. 4).

I. Risk Appetite and Risk Profile

Any organization intending to implement a congruous risk management system should define a Risk Appetite Framework (RAF), which is a framework connecting risks to the mission and strategic objectives, and so translating strategy into quali-quantitative variables. With reference to the risk profile (the “set of risks that may affect all or part of the organization”) and consistently with the overall strategic plan, such a framework defines the leaning toward risk (risk tendency), tolerance thresholds, risk limits, risk governance, as well as any processes needed to outline and implement them.

An organization cannot consider risk as simply resulting from likelihood-per-impact in order to treat it: its management depends on the component variables involved in determining risk appetite, or “the amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time”. Risk Appetite level mostly depends on the kind of activity performed, the products and services offered, and the regulatory and environmental contexts in which the organization operates.

The variables expressing risk profile-risk appetite ratio are as follows:

- Risk perception, which describes how people perceive risks according to their values and interests;
- Risk attitude (existing risk profile): If an organization is particularly effective in managing certain types of risks, it may be willing to take on more risk in that category, or conversely, it may not have any appetite in that area;
- Risk acceptance, which refers to the maximum potential impact of a risk event that an organization could withstand. Often appetite will be well below acceptance;
- Risk capacity, which is the maximum level of risk that an organization can assume without violating the regulatory burden;
- Risk retention, which considers stakeholders’ conservative return expectations and a very low appetite for risk-taking;
- Risk tolerance, which is the level of variation that an organization is willing to accept around specific objectives.

While risk appetite is linked to strategic objectives, risk tolerance is mainly connected to the operational ones since through the latter the governing body sets up the maximum deviation allowed by risk appetite.

Figure 1: From the risk profile to the risk appetite definition

Figure 1: From the risk profile to the risk appetite definition
The Risk Appetite Framework (RAF) is a methodological scheme aimed at determining the organization’s risk appetite level, through an evolving, iterative process, that helps the organization outline the amount of risk it is willing to take, in order to achieve its objectives according to the business strategy.

When outlining risk appetite, all strategic activities (planning, detection of financial and human resources, portfolio project selection, etc.) are determined according to risk-based thinking and criteria. It’s up to the governing body to draw up the RAF through a statement (RAS – Risk Appetite Statement), comprising an official document that sets out risk objectives, as well as the ways to monitor their achievement and cascading them through the organization’s operational processes.

In particular, the RAF should state:
Ø The types of risks an organization intends to take;
Ø For each kind of risk, any possible tolerance threshold and operational limit, under both normal and critical (at organizational/financial level) circumstances;
Ø Any procedures and/or actions to start if it becomes necessary to lead risk level back to either the objective or the limits established, especially if risk level reaches the tolerance threshold;
Ø The role of actors involved in defining and implementing the RAF (board, managers, auditors, operational units);
Ø Timing and procedures to monitor and update the RAF;
Ø Rules for sharing the RAF contents with all actors, both internal and external, involved in its definition and implementation.

Those organizations who effectively adopt a risk Appetite Framework are able to integrate it within their own decision-making processes, and strive to internally communicate and disseminate its contents, starting from the top management.

In defining its own risk appetite level, an organization should set up a template to identify tolerance thresholds for any activity area; for example, the template will show whether a particular activity within each area has a low, medium or high risk level and then, respectively, a high, medium or low tolerance level.

The RAF should contain any elements to be taken into consideration in order to determine the tendency to risk, for example, through designing a matrix in order to assess the risk tendency level for each activity, to be made by the respective risk owners.

A different level of risk appetite can therefore be outlined for the top strategic risks, as well as specific behaviours consistent with a pre-determined level of risk tendency; for this a matrix to support the decision-making processes can be laid down, in order to align the individual approach with the risk policies established by the top management: risk adverse; risk minimising; cautious; open to risk; or risk-taking.
II. Risk management commitment

Risk management design should be mostly contributed to by top management with the assistance of middle/low management and technical staff (for example, through mixed working groups). Particularly during the start-up phase, every organizational level should be involved in order to collect inputs and needs (for example, through *ad hoc* interviews). Employees know best the most typical and recurring risks in their area, and should be both encouraged and engaged to regularly give information about them.

Risk management goals should not only be clearly defined and communicated by top management, but also discussed within each of NSO’s units. Each unit should have a contact person who is entitled to coordinate all the risk management activities, in cooperation with his/her colleagues, including the head of unit.

III. Stakeholders’ empowerment

It is very important to establish and maintain proper risk frameworks, that ensure cooperation with stakeholders in achieving common objectives (e.g. the public’s trust in the quality of official statistics; protection of confidentiality related to respondent data, etc.). An organization should regularly circulate information, as well as continuing dialogue about risk management with internal and external stakeholders, in order to ensure that everybody understands the basis upon which decisions are made and the reasons why particular actions are required.

For this purpose, the organization needs to:

- Periodically review interfaces;
- Check whether communication is correctly understood, and all communication channels are effective;
- Set up clear communication protocols in order to ensure there is a common understanding of the respective responsibilities;
- Implement a consultative team approach, to help properly define the internal and external context, and ensure risks are identified effectively; to put different areas of expertise together when analysing risks; to ensure different views are properly considered in evaluating risks; and to assure appropriate change management during risk treatment;
- Develop a communication plan for both internal and external stakeholders, at the earliest stage of the risk management process;
- Encourage, acknowledge and appreciate unsolicited views;
- Provide periodic feedback to show how well what was promised or projected has been actually performed.

For further information see Section 2, Ch. 1.