Q How can organizations define risk appetite? Is there any standard method or technique?

A The objective of risk management is to reduce the organization's risk below an acceptable level. This acceptable level is decided based on the organization's risk appetite and risk tolerance for particular risk.

Risk appetite is the amount that an organization is willing to lose in case risk materializes or a project fails to meet objectives. Risk appetite is different for different organizations depending on industry sector, culture, spread, size and objectives. The risk appetite of an organization changes over time.

A benefit of risk appetite is that while considering investments in new projects, management may consider different risk scenarios for the project and try to get an answer to the question, "If the project fails, the organization may lose the entire investment. Can the organization afford it?" This affordability is decided by the risk appetite of the organization.

The main challenge organizations face today is defining risk appetite. A study by the US National Association of Corporate Directors identified that only 26 percent organizations have a defined risk appetite statement and approximately 70 percent of organizations have not defined risk appetite.[1]

A risk appetite statement of an organization is an important part of an enterprise risk management (ERM) framework and must be aligned with business strategy. The risk appetite should be expressed in quantitative measures; however, it can also include qualitative statements. The risk appetite of the organization depends upon the risk culture of organization.

Defining risk appetite is the responsibility of the board of directors and, while defining risk appetite, the following aspects should be considered by the board:

- Board and management judgment about risk materializing
- Total earnings of the organization and the equity capital that will decide the upper limit
- Compliance requirements, particularly legal and regulatory
- Level of achievement of business objectives and the impact of risk on them
- Stakeholder expectations from the organization
- Historical data and experience on risk materialization
- Risk scenario analysis

In addition, certain aspects must be part of the enterprise risk management (ERM) framework, which will ensure the effectiveness of risk appetite and, hence, the risk management process:

- Developing a common understanding and taxonomy for risk at the board, management and business levels
- Conducting risk awareness and building a desired risk culture
- Aligning business strategy with risk management, which will provide mapping between financial aspects and risk response action plans
- Assessing and reporting the risk profile to ensure that residual risk is within acceptable limits
- Developing key risk indicators (KRIs), key performance indicators (KPIs) and a monitoring process
- Understanding stakeholder expectations about value creation, risk optimization, security and economic sustainability

Endnotes

1 National Association of Corporate Directors (NACD), *2013-2014 Public Company Governance Survey*, USA, 2014, *https://www.nacdonline.org/analytics/survey.cfm?ItemNumber=66753*

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, CDPSE, AMIIB, BS
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.