An Overview of ISO 31000: 2018 Risk Management and Role of Chartered Accountants

In the last decade, there has been a major surge in the interest towards Risk Management. This is due to the change in management's attitude towards Risk Management. Risk Management which earlier limited itself to the middle and lower-level management has now risen to the strategic level management with an emphasis on the Tone at the Top. This momentum has initiated the need for the change in the Standards and Frameworks related to Risk Management. Most of the standard-setting organisations have updated their standards with the changing needs. Read on to know more...

CA. Chethan Jayantha

(The author is a member of the Institute. He can be reached at chethan2525@gmail.com and eboard@icai.in)

ISO 31000: 2018 Risk Management, is a prominent standard that was updated in February 2018 and Enterprise Risk Management – Integrated Framework was released in September 2017. The article is intended to provide an understanding of ISO 31000: 2018 Risk management.

Introduction

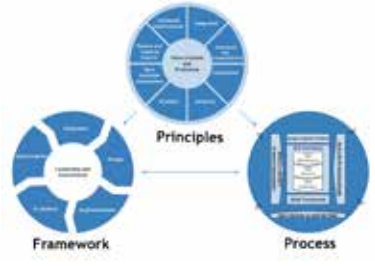
The International Organisation for Standardisation (ISO) is an international standard-setting body composed of representatives from various national standards organisations. This organisation promotes worldwide proprietary, industrial, and commercial standards. The technical management board of ISO is responsible for more than 250 technical committees and these technical committees develop the ISO standards considering the industry's needs.

In November 2009, ISO released the standard on Risk Management titled ISO 31000:2009 Risk Management. It provided the principles and generic guidelines on Risk Management. The objective of this standard was to replace the many differing standards, which stretch across industries, regions, and subjects. Hence this standard was not specific

to any particular industry or sector, but it could be used by any public, private or community enterprise, association, group, or individual. It could be applied to any type of risk and any nature of Risk. Further, it could be used during any life cycle of the organisation. Over a period, the ISO identified few drawbacks in the erstwhile standard. Which include,

- A very minimal integration with the corporate control systems, including strategic planning and management control
- The Non-integrated approach of Risk Management with other functions of the organisation
- No risk taxonomies
- Did not offer practical implementation tools for Risk Managers
- Owing to this limitation and the changing business environment, the ISO has issued 31000:2018 Risk Management, with following key improvement areas
- The importance and leadership of top management are highlighted. Managing risk is part of governance and leadership and is fundamental to how the organisation is managed at all levels.
- Integration of risk management with other functions, starting with the governance of the organisation.
- review of the principles of Risk Management.
- Greater emphasis is given on the iterative nature of Risk Management, i.e. documenting the new experiences, knowledge, and analysis which can lead to a revision of process elements, actions, and controls at each stage of the process.
- Streamlining of the content with a greater focus on sustaining an open systems model to fit multiple needs and contexts.

The ISO 31000:2018 Risk Management is divided into 3 major segments namely Principles, Framework, and the Process. (*Image: © 2018 ISO - All rights reserved*) The same is discussed in detail in the upcoming paragraph.



Principles

As mentioned in the standard, the Principles are the foundation for managing risk. These principles should be considered with the utmost importance when establishing the organisation's risk management framework and processes. All the principles of Risk Management are enumerated in the above image. These are the guiding factors that enable the organisation to achieve its objectives.

The core principle around which the Risk Management standard is established is "Value creation and Protection". All other principle is bounded together with this core principle. It can be evidenced in the above image in which the "value creation and protection" is kept at the center. According to the principle, Risk Management not only creates value to the internal stakeholders namely management and shareholders who want to see their stake appreciate but also to all external stakeholders including the customers purchasing its products and services.

Effective Risk Management requires all the 8 elements portrayed in the image above. Let us have a detailed understanding of the same.

a. Integrated

This principle mentions that Risk Management cannot work in silos. Risk Management is not just the responsibility of the Risk Management team. In contrary to the traditional Risk Management, this standard mention that Risk Management is an integral part of all organisational activities. All the functions in the organisation and all the levels of management should be part of Risk Management. Only when Risk management is done holistically, the objective of Risk Management is achieved.

b. Structured and Comprehensive

Risk Management should be a structured approach and not an ad-hoc activity. Further, it should be comprehensive enough to cover all the activities of the organisation. Creating and following a comprehensive, structured Risk Management approach leads to the most consistent and desirable Risk Management outcomes.

c. Customised

The Risk Management Framework should not take an approach of one size fits all. It should consider the nature, size, and objective of the organisation. The Risk Management approach should be customized to the organisation's needs including the external and internal context in which the organisation operates.

d. Inclusive

In Risk Management, all the stakeholders in the organisation should participate and get involved. The knowledge, views, and the perception of all the stakeholders should be collated. This facilitates the increased awareness of the risk and leads to informed Risk Management.

e. Dynamic

Risk Management is not a stagnant activity and it is not once prepared and used lifetime. Risk exposed to the organisation changes with time. New risk can emerge, and existing risk may diminish. Risk Management process should be adaptable to the changing environment. Risk Management needs to anticipate, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.

f. Best available information

Information is the core of all the decision making and Risk Management is no exception. Accurate and timely information is the success factor in Risk Management. The input for Risk Management can be historical information, current information, and future expectation. The best available information must be considered after taking into account the limitation of information namely cost-benefit analysis with regard to the accuracy and timeliness of the information.

g. Human and cultural factors

Human factors and culture play crucial roles in Risk Management. An organisation's culture will influence human behavior and attitude towards risk. At the end of the day, it is the humans who deal with the Risk. This Principle suggests the Risk Management should be driven by the Tone at the Top and the same should percolate down to all levels of management.

h. Continual improvement

Risk Management is not a one-time activity. It is a continuous process that needs to be followed during all stages of the life cycle of the organisation. Based on the experience and the knowledge gained during the continued process of Risk Management, an ongoing effort to improve the process must be initiated. These efforts will lead to "incremental" improvement over time.

Framework

The Framework needs to be designed to assist the organisation to integrate Risk Management with all the activities and functions of the organisation. Framework development encompasses integrating, designing, implementing, evaluating, and improving Risk Management across the organisation as articulated in the above image. The framework should be customized as per the needs and demands of the organisation.

a. Leadership and commitment

The critical success factor for any implementation is the commitment of the leadership and Risk Management is no exception. Top Management is required to demonstrate leadership and commitment toward Risk Management. They are responsible for implementing and following the Risk Management practices and integrating the same across all the functions in the organisation. They should create a positive tone at the top and show their commitment by implementing Risk Management policies, plan and course of actions, assigning necessary resources, assigning authority, and responsibility to Oversight bodies.

b. Integration

Risk Management needs to be integrated at all levels of the management and across all functions of the organisation. Risk Management practice should not be restricted to the oversight team but everyone in the organisation should be responsible for managing the Risk. Necessary care needs to be taken while integration and it needs to be done after understanding the organisation structure. It should also consider the objective, purpose, and goals of the organisation. It is a dynamic process and it needs to be customized based on the organisation's culture and needs.

c. Design

Designing the Framework is a significant activity in Risk Management. While designing the framework for Risk Management, the following activities must be performed.

- Understanding the organisation and its context
- The organisation must examine and understand its external and internal context while designing the Risk Management Framework. The external context includes the social, cultural, political, legal, regulatory, financial, technological, economic, and environmental factors, whether international, national, regional, or local, external stakeholders' relationships, perceptions, values, needs, and expectations. Internal context includes but not limited to vision, mission, and values, the organisation's culture; strategy, objectives and policies, standards, guidelines and models adopted by the organisation, contractual relationships, and commitments
- Articulating Risk Management commitment
- The oversight bodies and the Top Management must create the Risk Management Tone at the top and show their commitment towards the same. Commitment can be articulated by creating the necessary policies which indicate the objective and commitment towards Risk Management. Further, this tone at the top needs to percolate down to all the levels of management and stakeholders through appropriate communication.
- Assigning organisational roles, authorities, responsibilities, and accountabilities
- The commitment of the Top Management and the policies towards Risk Management would not be enough to achieve the objective of Risk Management. The management must assign the roles and responsibilities to the relevant personnel across the organisation and make them accountable for their responsibilities. Further, the same need to be communicated to all the levels of management.
- Allocating resources

  While designing the Framework, the management must ensure that adequate resources are deployed for the Risk Management process. It shows the commitment of the top management towards the Risk Management process. The resources required for Risk management includes people, skills, experience and competence, methods, and tools to be used for managing risk, professional development, and training needs.
- Establishing communication and consultation

The top management and the oversight bodies need to ensure that proper communication channels are established to ensure that timely, accurate, and relevant information is collected, collated, synthesized, and shared with the relevant stakeholder. Similarly, management must establish consulting channels for providing and receiving feedback that will contribute to and shape decisions.

d. Implementation

The framework suggests that the Risk Management process needs to be implemented after proper design. The implementation needs to be initiated only after having the appropriate plan regarding the time and resources. The successful implementation of the framework requires the

engagement, commitment, and awareness of stakeholders. The implementation needs to be monitored at each stage concerning the time and resources and necessary course correction needs to be initiated for the timely and proper implementation.

e. Evaluation

The Risk Management Framework needs to be evaluated periodically as against the objective for which the process was initiated, its effectiveness and efficiency. Necessary modification if any required needs to be done to ensure that the objective of the organisation is achieved.

f. Improvement

The management should constantly monitor the Risk Management Framework and make the necessary changes to adapt and address external and internal changes. The organisation should continually improve the suitability, adequacy, and effectiveness of the Risk Management Framework and the way the Risk Management process is integrated.

Process

According to this ISO, the Risk Management process involves the following activities namely Communicating and Consulting, defining Scope Context and Criteria, Risk Assessment, Risk Treatment, Monitoring, Reviewing, Recording, and Reporting. Even though this process is presented as sequential, in practice it is iterative.

a. Communication and Consultation

Communication and Consultation should take place across the organisation which includes the internal and external stakeholders. Further, it should also take place throughout all the stages of Risk Management. This will facilitate the stakeholder to understand the risk and make informed decisions. Communication and Consultation aim to bring different areas of expertise together at each stage of the Risk Management process and provide sufficient information to facilitate risk oversight and decision-making.

b. Scope, Context, and Criteria

- *Scope*

  The organisation needs to define the scope of Risk Management activities. Risk Management can be applied across all the levels and functions of management namely strategic, operational, project activity among others. To have a clear understanding as to what is covered and what is not, it is required to define the scope. This will also support in aligning the organisation's objective.

- *External and Internal Context*

  The external and internal context of the Risk Management process should be established by understanding both the external and internal environment in which the organisation operates. Further, this should also reflect the specific environment of the activity for which the Risk Management process is applied.

- *Defining Risk Criteria*

  The organisation should specify and document the amount and type of risk that it may or may not want to contemplate for Risk Management considering the objective of the organisation and its stakeholders. It should also be aligned with the Risk Management Framework and the scope of the Risk Management process. The Risk Criteria need to be defined after considering the positive and negative consequences of the inclusions and exclusions. The Risk Criteria need to be fixed along with the scope of the Risk Management process; however, it needs to be dynamic. In other words, it needs to be reviewed and monitored periodically and amended on a need basis.

c. Risk Assessment

The Risk Assessment process consists of the following process namely Risk Identification, Risk Analysis, and Risk Evaluation.

- *Risk Identification*

  The organisation identifies new, emerging, and changing risks which will have a negative impact on the achievement of its strategy and

business objectives. Risk Identification should occur at all levels of management and across all functions. Relevant, appropriate, and up-to-date information is important for identifying risks. The following factors need to be considered during Risk Identification namely tangible and intangible sources of risk, causes and events, threats and opportunities, vulnerabilities and capabilities, changes in the external and internal context.

- *Risk Analysis*

  The risks identified needs to be analyzed to understand the severity of each risk. The purpose of the Risk Analysis is to comprehend the nature of risk, its characteristics, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness. The event can have multiple causes and consequences and can affect multiple objectives and at multiple levels of the organisation. Hence the Risk Analysis needs to be undertaken at a varying degree at all levels of the organisation. Further, depending on the complexities and circumstances, the quantitative techniques, qualitative techniques, or a combination of both can be used to assess/analyze the risk. Risk Analysis will be the basis for Risk Evaluation and Risk Treatment.

- *Risk Evaluation*

  Risk Evaluation refers to comparing the results of the Risk Analysis and determining the actions to be initiated considering the Risk Criteria defined in the scope. In other words, the purpose of the Risk Evaluation is to support the decision related to Risk Treatment. The outcome of Risk Evaluation should be recorded, communicated, and then validated at appropriate levels of Management.

d. Risk Treatment

Risk Treatment should be deployed for all identified risks. Risk Treatment refers to the process of addressing the risk i.e. the process of the selection and implementation of the Risk Treatment options. Hence the Risk Treatment has the two subprocesses namely selection of Risk Treatment options and preparing and implementing Risk Treatment plans.

- Selection of Risk Treatment Options

While selecting Risk Treatment options, the organisation has to perform the cost-benefit analysis. The organisation has to consider potential socio-economic benefits derived from the implementation of the Risk Treatment option and assess the same against all the direct and indirect costs that would be incurred during and after the implementation.

There are various options for Risk Treatment which can be considered based on the Risk Analysis.

- Avoiding the risk
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing or Transfer the risk (like Insurance)
- Retaining the risk by informed decision

The selection of Risk Treatment options should be made in accordance with the organisation's objectives, risk criteria, and available resources.

- Preparing and Implementing Risk Treatment Plans

Post selection of the Risk Treatment option, the next stage is to draft the plan which specifies how the chosen treatment options would be implemented. This plan should clearly identify the order in which Risk Treatment should be implemented. The Treatment plans should be communicated to the appropriate stakeholder and it should be integrated into the management plans and processes of the organisation. It should also contain when actions are expected to be undertaken and completed.

e. Monitoring and Review

Risk Treatment options, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Hence, we need to have a monitoring and review process to assure and improve the quality and

effectiveness of process design, implementation, and outcomes. Ongoing Monitoring and review should be an integral part to give assurance that the different forms of treatment become and remain effective. Monitoring and Review include planning, gathering and analyzing information, recording results, and providing feedback.

f. Recording and Reporting

The Risk Management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and Reporting aim to communicate Risk Management activities and outcomes across the organisation to all stakeholders and to support decision making.

The need for reports / information is different for a different level of management. Reporting is an integral part of the organisation's governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Each report user will require different levels of detail of risk and performance information to fulfill their responsibilities in the organisation. Reporting supports personnel at all levels to understand the relationships between risk and performance and to improve decision-making. The Factor like frequency, timeliness, and cost associated with the same should be considered while determining the appropriate reporting structure.

Role Of Chartered Accountant and ICAI

Chartered Accountants are trusted advisors and provide services to businesses either as a consultant or as a practicing partner. Chartered Accountants work as managers, steering businesses in the right strategic direction, solving problems, and implementing change. Historically, Chartered Accountants has provided professional services related to Auditing, Taxation, Accounting, and Financial analysis. In recent decades, the Chartered Accountants have quickly developed strong commercial and decision-making skills and are supporting the organisations in the new area namely advisory services. One of the prominent among them is the advisory and consulting services on Risk Management. Chartered Accountants are risk experts who are outward-looking and providers of valuable insights to manage risk.

Unlike in other developed countries, in India, there was no legislation which promoting Risk Management practice, until the introduction of Companies Act, 2013. The first attempt to introduce Risk Management was done by SEBI. Based on the recommendation of the Committee chaired by Shri Kumar Mangalam Birla and The Murthy Committee's Recommendations on Risk Management, SEBI introduced Clause 49 of Listing Agreement. Clause 49 of the Listing Agreement was implemented with force from 31st December 2005. It was articulated for the enhancement of corporate governance in Indian listed companies. The key provisions which were relevant to Risk Management are:

- Responsibility of Independent Directors to periodically review risk and compliance reports arranged by the company along with those steps initiated by the company to improve its performance in those areas.
- Disclosure of Risk Management procedures and, specifically, of certain risks of fraud including those related to third-party transactions and contingent liabilities.
- Reports concerning legal compliance and Risk Management are subject to mandatory review by the Audit Committee.
- Management shall put in place procedures to inform corporate directors about risk assessment and minimisation initiatives. These procedures need to be periodically monitored to guarantee that management controls and reviews risk through a predefined framework.
- Management shall deliver to the Board of Directors a quarterly report certified by the compliance officer of the company. The report shall articulate the risks faced by the business; measures initiated to

mitigate the risks. The Board of Directors shall review this and attest the said document

With the introduction of Companies Act, 2013, Risk Management gained its momentum in the companies having business in India. The prominent sections which changed the game are

Section 134 (3) There shall be attached to *(Financial)* statements laid before a company in general meeting, a report by its Board of Directors, which shall include—

(*n*) a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.

Section 177 (4) Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, *inter alia,* include, —

(*vii*) evaluation of internal financial controls and risk management systems.

Companies Act, 2013 has made it mandatory for the companies to develop and implement Risk Management Policies and Systems. Further, the same must be evaluated periodically by the Audit Committee. The Act is silent on the standard or the framework which can be used, and it is left to the discretion of the company's management.

This has given a tremendous opportunity for the Chartered Accountants both in practice as well as in employment. Depending on the organisation's needs, Chartered Accountants can involve in the implementation of Risk Management and during the Life cycle of Risk Management. In case the organisation outsources this Risk Management activity, the Chartered Accountants can portray their expertise in performing the end to end activities of Risk Management. In case the Company intends to have an inhouse Risk Management team, the Chartered Accountants can be the part of the management in setting up the Risk Management function by identifying the suitable framework and tailoring them to the need of the organisation. They can also support the management in all the processes of Risk Management activities namely Communicating and Consulting, defining Scope Context and Criteria, Risk Assessment, Risk Treatment, Monitoring, Reviewing, Recording, and Reporting.

Our visionary institute ICAI had already envisaged the changing industry needs. This can be evidenced by the fact that the Institute changes in the curriculum long back to include Risk Management as one of the subjects. This would equip the Chartered Accountants with the required knowledge and enable them to enhance their contribution to Risk Management.

Conclusion

Business requires taking risks and seizing opportunities to achieve success. The organisation should not solely rely on mitigating the risk, but it should promote and facilitate effective risk and opportunity management to facilitate value creation and preservation over time. This involves being focused on the benefits of intelligent risk-taking in addition to the need to mitigate and control risk. There are various standard and framework which supports organisations in Risk Management. Organisations must choose the best framework which suits their objective and tailor them to their needs.

Further, Risk Management is a statutory requirement as per the Companies Act, hence giving an avenue for the Chartered Accountants for providing risk expertise which is outward-looking and providing value addition to the organisations. ■■■