RISK FRAMEWORK

1. SCOPE

ISO 31000:2018 Risk Management Standards specifies a common but customisable approach your board or management can use throughout the life of the organization small or big, profit or not-for-profit, mining or manufacturing or trading or service. The common approach applies to any activity and at all levels.

2. PRINCIPLES

The Board should remember these principles while designing a risk framework.

a) Integrated: Integral part of any organisational or management or governance activity and is not away from it. Planning, staffing, control, machining, packing, or any activity has risk inherent in it.

b) Structured: The board and employees should apply risk practices consistently to compare results and learn from them. You should have a risk manual to foster uniformity and consistency, for example.

c) Customized: The simpler the organization's external and internal context (See Context - Appendix A1) and objectives, the simpler is the framework and vice versa. You can appoint an internal auditor or outsource or ask your quality assurer to carry out internal audit, depending on internal or external context or objectives.

d) Inclusive: Involve stakeholders in time to benefit from their knowledge, views and perceptions for improved awareness.

e) Dynamic: Risks can emerge, change, or disappear as an organization's external and internal context changes. If Government bans imports, risks from imported products will not exist.

The Board should also remember the following principles because they are used during risk process:

f) Best available information: Historical or current information or future expectations are enough for considering risk as for any decision making. Recent financial statements and estimates may be enough to assess or respond to the risk of loss for the year to end.

g) Human and cultural factors: Human behaviour and culture significantly influence risk management at each level and stage in these days of international labour migration.

h) Continual improvement: For learning and experience. Risk management is ever changing or evolving to cover risks get complex day by day in this information technology world.

3. BOARD RESPONSIBILITIES

Board must understand that the organisation faces risks while setting and pursuing the objectives. So, the board should customise the risk management system by integrating it with the organisational structure and activities. This will assist the top management to implement and operate the system where all identify, analyse, evaluate, and treat appropriate risks. Further the board is responsible for communication of risk information throughout the risk process. In short, the Board should:

- Issue a policy that establishes a risk management approach, plan, or course of action. For example, HR policy may change to incorporate pertinent risk process as part of employment contract.
- Ensure that necessary resources (men, management, materials, money, machines, hardware, and software) are allocated to managing risk (See Resource Allocation - Appendix A2). For example, internal auditor or risk officer may have to be appointed or investment in a risk management software should be budgeted.
- Assign authority, responsibility, and accountability at appropriate levels within the organization. For example, the manager should accept responsibility to keep a risk register for his department or team or project or division.

- Oversee senior management's performance during the risk management process. For example, the board should ask for top 5 risks to be reported regularly or at board meetings with management plans to respond to the risk.

4. SENIOR MANAGEMENT RESPONSIBILITIES

Based on the board's policy, using the allocated resources which perform their roles and responsibilities, senior management should be accountable for:

- Aligning risk management with its objectives, strategy, and culture. Risk is everywhere but people should relate it to organisational goals.
- Recognizing and addressing all obligations, and voluntary commitments. An unsettled obligation creates avoidable risks like litigation or loss of reputation or stoppage of supplies.
- Establishing the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated to the organization and its stakeholders. For example, higher production should be achieved but not by not maintaining the machines.
- Communicating the value of risk management to the organization and its stakeholders. For example, risk process is simply a way of making decisions.
- Promoting systematic monitoring of risks. Because monitoring ensures that all in the organisation are alert about achieving goals all the time.
- Ensuring that the risk management framework remains appropriate to the context of the organization. For example, a certain branch may be closed but manuals may still be not amended which could lead to loss.

5. RISK MANAGEMENT POLICY AND MANUAL

The Policy or Manual should articulate organization's purpose for managing risk and its links to its objectives and other policies. It should promote risk culture as part of the overall culture of the organization. It should integrate risk management into core business activities and decision-making. It should explain authorities, responsibilities and accountabilities relating to risk management. It should specify resources made available. It should explain the way in which conflicting objectives are dealt with. For example, the manual should explain why very urgent actions will still need to wait for approval. Manual should specify how risks should be measured, assessed, treated, and reported as part of performance indicators. The manual should deal with review and improvement – who will review and how frequently, for example.

6. IMPLEMENTATION GUIDELINES

- Develop an appropriate plan with time targets and resources to be assigned.
- Identify where, when, and how different types of decisions are made across the organization, and by whom – For example, how materials are bought, or production is scheduled, or delivery is made, or debts are collected and who makes decisions and when.
- Modify the applicable decision-making processes where necessary. For example, purchase manager buying for a specific sales order may discuss with the sales manager before placing the order.
- Ensuring that the organization's arrangements for managing risk are clearly understood and practised. For example, weekly or monthly meetings to populate risk register at the instance of a risk champion who reports to the Risk Officer.

(See Implementation – Appendix A4)

7. EVALUATION GUIDELINES

- Periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour; For example, irrelevant risks may be reported.
- Determine whether it remains suitable to support achieving the objectives of the organization. The company may be bought out by another company which may set a different objective.

8. IMPROVEMENT GUIDELINES

The organization should continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

[ISO 31000: 2018 gratefully acknowledged]

9. APPENDIX A1

External & Internal Context

External context may include, but is not limited to:

- The social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- Key drivers and trends affecting the objectives of the organization;
- External stakeholders' relationships, perceptions, values, needs and expectations;
- Contractual relationships and commitments;
- The complexity of networks and dependencies.

Internal context may include, but is not limited to:

- Vision, mission and values;
- Governance, organizational structure, roles and accountabilities;
- Strategy, objectives and policies;
- Organization's culture;
- Standards, guidelines and models adopted by the organization;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- Data, information systems and information flows;
- Relationships with internal stakeholders, taking into account their perceptions and values;
- Contractual relationships and commitments;
- Interdependencies and interconnections.

[ISO 31000: 2018 gratefully acknowledged]

10. APPENDIX A2

Allocating resources

- People, skills, experience and competence;
- The organization's processes, methods and tools to be used for managing risk;
- Documented processes and procedures;
- Information and knowledge management systems;
- Professional development and training needs.

[ISO 31000: 2018 gratefully acknowledged]

11. APPENDIX A3

Implementation Plan

Risk management architecture

- Committee structure and terms of reference
- Roles and responsibilities
- Internal reporting requirements
- External reporting controls
- Risk management assurance arrangements

Risk management strategy

- Risk management philosophy
- Arrangements for embedding risk management
- Risk appetite and attitude to risk
- Benchmark tests for significance
- Specific risk statements/policies
- Risk assessment techniques
- Risk priorities for the present year

Risk management protocols

- Tools and techniques
- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Audit procedures and protocols
- Reporting/disclosures/certification

[Extracted from Page 11 of Standard Deviations (2018) by the Institute of Risk Management (UK). It is a guide to risk practitioners}