TOPIC FOUR
RISK MANAGEMENT PROCESS, PERSPECTIVES AND RESPONSIBILITIES

Standard Risk Management Process

The risk management process is a framework for the actions that need to be taken. There are five basic steps that are taken to manage risk; these steps are referred to as the risk management process. It begins with identifying risks, goes on to analyze risks, then the risk is prioritized, a solution is implemented, and finally, the risk is monitored. In manual systems, each step involves a lot of documentation and administration.

Step 1: Identify the Risk

The initial step in the risk management process is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks: Legal risks, Environmental risks, Market risks, Regulatory risks etc.
It is important to identify as many of these risk factors as possible.

Step 2: Analyze the Risk

Once a risk has been identified it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the organization. To determine the severity and seriousness of the risk it is necessary to see how many business functions the risk affects. There are risks that can bring the whole business to a standstill if actualized, while there are risks that will only be minor inconveniences in the analysis.

Step 3: Evaluate the Risk or Risk Assessment

Risks need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on the severity of the risk. A risk that may cause some inconvenience is rated lowly, risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization to gain a holistic view of the risk exposure of the whole organization.
There are two types of risk assessments: Qualitative Risk Assessment and Quantitative Risk Assessment.
Qualitative Risk Assessment: Risk assessments are inherently qualitative – while we can derive metrics from the risks, most risks are not quantifiable. For instance, the risk of climate change that many businesses are now focusing on cannot be quantified as a whole, only different aspects of it can be quantified. There needs to be a way to perform qualitative risk assessments while still ensuring objectivity and standardization in the assessments throughout the enterprise.

Quantitative Risk Assessment: Finance-related risks are best assessed through quantitative risk assessments. Such risk assessments are so common in the financial sector because the sector primarily deals in numbers. Quantitative risk assessments are easier to automate than qualitative risk assessments and are generally considered more objective.

Step 4: Treat the Risk

This involves coming up with strategies to minimize the likelihood and impact of risk. Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs. In a risk management solution, all the relevant stakeholders can be sent notifications from within the system.

Step 5: Monitor and Review the Risk

Not all risks can be eliminated – some risks are always present. Market risks and environmental risks are just two examples of risks that always need to be monitored. Under manual systems monitoring happens through diligent employees. These professionals must make sure that they keep a close watch on all risk factors. Under a digital environment, the risk management system monitors the entire risk framework of the organization. If any factor or risk changes, it is immediately visible to everyone. Computers are also much better at continuously monitoring risks than people. Monitoring risks also allows your business to ensure continuity.

Enterprise Risk Management (ERM) Framework

An enterprise risk management (ERM) framework is a systematic approach used by organizations to identify, assess, manage, and monitor risks. It includes the strategies and processes by which organizations effectively manage risks across the entire organization.

Elements of an Enterprise Risk Management Framework

An enterprise risk management framework should include the following:

1. Risk Governance and Culture; An organization's internal environment is the most important ERM as it's the ultimate source of its risk management strategy. The board of directors and senior management must establish a culture of risk oversight and compliance. Promote a risk-aware culture where employees at all levels understand the importance of risk management and their role in it.

The values, actions, and attitudes espoused by a company's senior management will reverberate throughout the operations of each department. An organization with a risk-aware culture will provide the support and resources to protect all parties from

unnecessary risk exposure, whereas establishments with less structure could have consistent problems meeting their objectives and avoiding legal trouble.
There are several practices you can implement to create a positive risk management culture such as:

- Creating an independent risk committee that provides risk oversight for the entire organization. Their authoritative powers and place within the organizational structure should be outlined in the risk committee charter.
- Aligning risk management activities with overall company goals,
- Encouraging employees to communicate and share any concerns regarding potential risks. This can be done through regular meetings or anonymous reporting channels.
- Developing training programs to educate employees on how to identify and address potential risks.
- Rewarding employees who display high-level risk awareness. Doing this actively rewards workers for thinking deeply about risk management.

2. Risk Appetite and Tolerance; Risk appetite describes the amount and types of risk an organization is willing to accept when attempting to achieve its strategic objectives. Risk tolerance refers to the level of risk an organization can withstand before its ability to meet its objectives becomes negatively impacted. The combination of these two elements helps define an organization's boundaries and provides a greater context for the decision-making process of executive leadership. Find the right balance between risk appetite and risk tolerance to allocate resources wisely and enact strategies that strive for growth without leaving the organization vulnerable to potential risks.

3. Risk Identification; Risk identification is an ongoing process of identifying potential internal and external risks that could negatively impact the organization's ability to accomplish its goals. When undergoing risk identification, the organization studies its culture, business processes, and enforce policies to take note of any risky events that could pose a threat to the company's operations. Possible risks should be documented with risk statements kept in the company's risk register. These documents should aptly describe the situation and the consequences if these incidents take place.

4. Risk Assessment and Measurement; After identifying potential risks, the next aspect of an enterprise risk management framework is to assess the likelihood, potential impact, and your organization's ability to respond to these risks. Risk assessments (sometimes referred to as risk analysis) help management categorize and quantify the level of risks by measuring the chance of each risk occurring and giving them an overall risk score on a risk assessment matrix.

5. Risk Monitoring and Reporting; Periodically monitoring your risk management policies and operations is another crucial element of any effective ERM process. It's inevitable that an organization's goals, stakeholders, and risk profile will change as circumstances change and the wider industry evolves. This fact means that the benchmarks for risks will also shift as a result. Companies need to be prepared to pivot when necessary.

Roles of Risk Function and Risk Manager

The primary person working in an organization as a risk management team leader is known as a Risk Manager. Some of the duties they perform include:

- *Risk Identification;* The first step involves looking for risks that might threaten the achievement of the organization's goals and objectives or the smooth running of its operations. These can include financial, operational, strategic and compliance risks.
- *Assess and Analyze Risk;* Analyze risks determined based on their probability and effect to gain an adequate measure of the risks involved.
- *Risk Assessment;* Make balanced risk identification through risk analysis of risks according to the likelihood rating of the impact.
- *Risk Mitigation;* There are strategies and action plans that must be used to reduce or even remove identified risks so that risk management measures that are in place are comprehensive and sustainable.
- *Employee Training and Awareness;* Another important aspect of risk management duties is employing training sessions and awareness programs to help employees understand the organizational culture of risk management and how to observe and report risks.
- *Management;* One of the key risk manager responsibilities is to supervise the execution of the risk management policies in the organization to ensure that all activities related to risk management form a part of the whole management setup.
- *Maintaining Insurance Record;* Check and coordinate the organization's insurance policies and insurance claims to ensure sufficient coverage and timely updates to minimize risk.
- *Regulatory Compliance;* Follow laws and regulations and set standards by familiarizing yourself with changes and making the necessary changes for the organization.
- *Audit Processes and Procedures;* Performing regular checks on risk management procedures and practices to enhance their efficacy and compliance.
- *Communication;* Establish and maintain good relations with the organization's various stakeholders and external partners, customers and service providers.

- ❖ *Monitoring and Review;* There is always a need to assess the risk environment and the efficiency of risk management activities when identifying and managing risks to make modifications due to the dynamic nature of risks.
- ❖ *Preparing Reports;* Present such risk management reports to the upper management and the Board of directors in summarized formats with recommendations made after conducting risk assessments and risk analysis.

Compliance Function Responsibilities

Compliance function responsibilities vary a great deal, depending on the industry and nature of corporation. Yet there are numerous directives, guidelines or recommendations, which outline the core of suggested compliance functions for businesses.

• *Guidance and education:* The compliance function should assist senior management in educating staff on compliance issues and acting as a contact point within the bank for compliance queries from staff members.

- *Advice:* The compliance function should advise senior management on compliance laws, rules and standards, including keeping them informed on developments in the area.

• *Identification, measurement and assessment of compliance risk:* The compliance function should, on a proactive basis, identify, document and assess the compliance risks associated with the bank's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships.

• *Monitoring, testing and reporting:* The compliance function should monitor and test compliance by performing sufficient and representative compliance testing.

• *Statutory responsibilities and liaison:* The compliance function may have specific statutory responsibilities (e.g. fulfilling the role of anti-money laundering officer).

• *Compliance program:* The responsibilities of the compliance function should be carried out under a compliance program that sets out its planned activities (e.g. review of specific policies and procedures, compliance risk assessment, compliance testing)

Internal audit and Risk management

Internal auditing is an independent, objective assurance and consulting activity. Its core role regarding ERM is to provide objective assurance to the board on the effectiveness of risk management. Internal audit provides independent checks on the effectiveness of internal controls and risk management processes, while risk management focuses on finding, assessing, and handling risks to meet organizational goals.

In today's world, processes and operations have become more complex and new risks have emerged. The best approach is to have a separate internal audit and risk management function, but operationally this is difficult to implement, time-consuming and is costly. Most organizations have internal audit functions but do not have a risk management function. Therefore, the internal audit function undertakes risk function in organizations without an effective risk management function.

There are three levels of defense in an effective Risk Management Control Framework is **Operational Management** as the first line of defense, **Risk management and compliance** as the second level defense function and **internal audit** as the third level of defense responsible for entity wide assurance. The main role of the internal audit in risk management is providing an assurance on the effectiveness of the risk management process.

If Internal Audit and Risk Management is performed as one role, these are some of the recommended actions internal auditors can take to help their organization adopt a more strategic risk management focus:

- ✓ Ensuring that the risk assessment identifies those risks presenting the most significant risks to shareholder value.
- ✓ Facilitating risk management discussions across the organization.
- ✓ Viewing risk management as a core competency and ensuring that auditors receive appropriate training on risk and risk management practices.
- ✓ Reviewing business plans to determine whether they assess the risks embedded in their strategies and have risk monitoring and trigger points.
- ✓ Reviewing the annual report to determine whether risks are addressed appropriately.
- ✓ Continuously monitoring and assessing stakeholder expectations relative to risk and risk management, as well as assisting in the education of these stakeholders.
- ✓ Building a stronger relationship with other risk and control business functions to drive an enhanced process to identify emerging risks.
- ✓ Identifying and sharing best practices in risk management.