AN ANALYSIS OF RISK MANAGEMENT FRAMEWORK FOR EFFECTIVE RISK MANAGEMENT IN IT SECTOR

Agnes Amala Anitha T, Hindustan Institute of Technology and Science, Padur, Chennai

ABSTRACT

IT sectors are very important in India and play a crucial role in developing he country's economy and also contribute significantly to the GDP growth of the country, creating employment in the current generation, and also creating technological advancement which makes human life at ease. In recent days the IT sector has faced various newly evolving risks. Risk can have substantial impacts on the it sector. The risk would affect the various aspects of working in the IT sector. In this study, we examine effective risk management practices. We shall discuss various risk management structures followed in Indian IT sectors. Incorporating risk management committees, how do they identify risk? How do they assess the identified risk? Their monitoring strategies. Key components of this paper include risk management structure, risk management committee, risk identification, risk assessment, risk mitigation strategies, monitoring and control practices, and challenges faced in monitoring and controlling activities. In this research work, I intend to have a robust framework for effective risk management in the IT sector.

Keywords: Risk Management, Risk Management Strategies, Risk Management Committee, Effective Risk Management, Risk Management structure

Introduction

The risk management framework in the Indian IT sector involves a systematic approach. The study of the systemic approach involves identifying risks, assessing risks, prioritizing risks, and mitigating risks. Risk could impact the Indian IT Sector in various ways affecting its operations, and also have high risks in their assets, and reputation. To obtain an effective risk management framework in the Indian IT sector, we must have a special focus on understanding the IT sector, enquiring about the Key Risks evolved in the Indian IT Sector, and analysing the Components of the Risk Management Framework followed by the Indian IT Sectors.

Risks in the Indian IT Sector:

1. Supply chain disruptions and commodity inflation:

It may involve or occur in several ways like Delayed delivery of hardware components from global suppliers which would impact the project timelines and also customer satisfaction. Commodity inflation occurs when there is an increase in hardware cost. Inflationary pressures can result in higher licensing fees and higher costs for cloud services, which are the main reasons to affect the company's profit.

2. Global economic and geographical environment

The complete health of the global economy sways demand for IT services and solutions. so, during this period, the IT sectors invest a way lot than usual circumstances. Accordingly neglecting the global factors results in risk in the sectors. In addition, Fluctuations in exchange rates can affect the Indian IT sector's competitiveness. Changes in global interest rates and monetary policy decisions made by central banks, specifically major economies like the US Federal Reserve, can alter capital flows, change investment decisions, and also impact the borrowing costs for Indian IT companies. The geopolitical environment includes Political instability and regional conflicts which can create uncertainty to the business confidence and investment decisions.

3. IT systems and security:

IT Sectors must address the integrity, confidentiality, and availability of their data and systems. Indian IT companies face a wide range of cybersecurity threats, including phishing attacks,

malware, insider threats, ransomware, and distributed denial-of-service (DDoS) attacks. This potential harm can negotiate sensitive data, disrupt business operations, and damage the company's reputation. Besides Failure to effectively protect customer data can result in legal penalties and reputational damage.

4. **Growth strategy and competitive business efficiency**

Striving determined growth strategies without proper planning and risk assessment can lead to over-development. Which leads to providing inadequate services to customers. Intense competition and market saturation can be a risk to sectors aiming for growth. Without skilled talent, it would cause vigorous risk in sustaining growth and maintaining competitive advantage.

5. **Brand positioning, innovation and rapid technology change:**

Brand positioning can become a risk if the brand fails to strike a responsive chord with consumers or fails to differentiate itself sufficiently. Moreover, Poor brand positioning can lead to market confusion, loss of brand and destroy customer loyalty. All these factors ultimately impact sales and profitability. While innovation is crucial for driving growth and staying ahead of competitors, it also carries inherent risks. Rapid advancements in technology bring both opportunities and risks for businesses. Adapting to the technological changes also requires huge investment and expertise. Failure to keep pace with it can render businesses disrupted by more tech-savvy competitors.

6. **Manufacturing operations and pandemic**

In manufacturing operations, during the pandemic situations like COVID-19, the risks related to supply chain disruptions, workforce shortages, and operational continuity have been vulnerably increased. Companies have had to face challenges regarding sourcing raw materials, maintaining production levels, and ensuring employee safety.

7. **Distribution channels, retailer network and customer service delivery**

Variations in demand for IT products and services can influence distribution channels and retailer networks. Severe competition within the IT sector can pressure retailers to offer

competitive pricing and value-added services which will lead to affecting profit margins and customer retention.

8. Environmental regulations and compliance

environmental regulations and compliance risks are considered due to the sector's reliance on various resources in the state. The government may impose regulations regarding the protection of environmental resources. While sectors find it difficult to comply with the regulations imposed. Some of the regulations may include Regulations governing the disposal and recycling of e-waste. Governments may impose energy efficiency standards. Restrictions on the use of hazardous materials in manufacturing IT products, such as lead, mercury, and brominated flame retardants, necessitate compliance with regulations like the Restriction of Hazardous Substances (RoHS) directive. Regulations may also govern the cooling systems and water usage in data centres to minimize water consumption. These regulations require IT sectors to invest in efficient cooling technologies and water management practices. Which again involves a huge investment in the sectors.

9. Climate change

Climate change would cause several risks in the IT sector. Some of the risks due to climatic changes like Floods, cyclones and storms can Damage Extreme weather IT infrastructure such as data centres, networks and communication systems, leading to service disruptions and financial losses.

10. Human capital

Human capital risks in the IT sector encompass managing and retaining skilled talent. Gradual reduction in employees can lead to disruption of project continuity and increase recruitment costs which will affect client satisfaction. A shortage of skilled professionals in newly evolving technologies like AI, cyber security, machine learning etc. will hinder the execution of projects because the projects need expertise and innovation.

What is risk management?

Risk management is the process of identifying, assessing, prioritizing, and mitigating risks which could effectively impact the sectors. It is a proactive process which requires functions

at different stages. Risk management is needed to protect the sector's assets. minimize the occurring losses. Risk management helps sectors adapt to evolving environments and recover quickly from adverse events. Presenting a strong risk management framework boosts stakeholder confidence and trust in the IT sector. Risk management highly contributes to the long-term sustainability of sectors by assuring their continued feasibility and success. Generally, risk management is essential for the IT sector to steer uncertainty, protect shareholder's interests, and achieve their goals in a vibrant and unpredictable business environment.

Steps involved in effective risk management

1. **Risk identification**

This is the foremost step involved in effective risk management. The sector must identify the possibly occurring risk. That is the identification of the above-stated risks in IT sectors. Identification of risks involves a systematic approach to recognizing potential threats which could influence the sector's goals, operations, or stakeholders. Risks may be identified in several ways which may include Maintaining risk registers or databases to capture and categorize potential risks across various aspects of the sectors. Conducting workshops and brainstorming sessions which involve key stakeholders, including senior management, project teams, and subject matter experts, to identify and discuss potential risks and their potential impacts. Conducting SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to identify both internal and external factors that may induce risks or opportunities to the sector's strategic objectives. Monitoring industry trends, market developments, technological advancements, and regulatory changes to anticipate emerging risks and opportunities that could affect the sector's objectives. Learning from past incidents near misses, or failures by analysing root causes and identifying underlying risks that contributed to the outcome and Using this information to improve risk identification processes which will help in implementing preventive measures. Respecting and accepting the input and feedback from various stakeholders, including employees, clients, suppliers, regulators, and industry associations, to identify risks from different perspectives could be a great source in identifying risk. Utilizing established risk taxonomies or frameworks, such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) or ISO 31000. This will help to systematically categorize and classify risks based on common criteria and definitions.

2. Assessing the identified risks.

Risk assessment is the process of evaluating the risks which have more and faster impact in the sector. There are many significant methods to assess risks. Such as Qualitative Risk Assessment Method Risks are typically categorized into higher, medium, or lower based on qualitative criteria. The qualitative criteria may include such as severity, frequency, and strategic importance. The quantitative method uses numerical data and statistical techniques to assess risks often using tools such as Monte Carlo simulation or decision trees. Risk matrices are also graphical tools that help visualize and prioritize risks based on their likelihood, occurrence and impact. Scenario analysis is also a method of risk assessment in Indian IT sectors which involves considering numerous hypothetical scenarios or events and assessing their potential impact on the sector. Key risk Indicators are specific indicators used to monitor changes in risk levels over time. Benchmarking is also a process of assessing risk which helps in comparing the sector's risk profile and management practices against its peers or best practices. Risk assessment in IT Sector I done to focus on high-priority risks.

3. Mitigation of prioritized risks.

Mitigation is the process of implementing effective strategies according to the nature of the risk and it helps in reducing the impact of that risk in the sector. Avoiding high-risk activities, technologies, or markets that create threats to the sector. This stage takes place after the evaluation or risk assessment which involves discontinuing certain projects which create harm to the sectors, exiting risky markets, or refraining from adopting unproven technologies which may make the situation worse. This may include strengthening cybersecurity protocols, implementing controls and safeguards, enhancing employee training and creating awareness, and improving operational processes to minimize risks. Risks can also be mitigated through Transferring the financial consequences of risks to third parties through the process of insurance, contracts, or outsourcing arrangements. This method may be implemented by purchasing insurance policies to cover specific risks, negotiating contractual agreements that allocate risk to vendors or partners, or outsourcing certain functions to specialized service providers. Another important part of mitigation is Sharing risks with other stakeholders, partners, or industry peers to spread the impact and increase resilience. This may include efforts like forming strategic alliances, partnerships, or consortiums to jointly address common risks or pooling resources to manage shared risks collaboratively. Proper Planning must be executed

in Developing contingency plans and response strategies to mitigate the impact of adverse events or emergencies. This may happen when there is a need for establishing business continuity plans, disaster recovery plans, and crisis management protocols to ensure rapid response and recovery in the event of disruptions. Continuous Monitoring is also a part of the mitigation process. Continuously monitoring and reassessing risks to changes in risk levels. This allows organizations to adapt and adjust mitigation strategies proactively in response to evolving risk landscapes. Stakeholder plays a crucial role in sectors, stakeholders Engagement are Engagement is needed to foster a culture of risk awareness, collaboration, and shared responsibility. This helps ensure risks are identified, assessed, and managed effectively across the sector.

4. Risk communication

For an effective risk management framework stakeholders should be aware of the potential risks and their implications. For that effective risks communication to the stakeholders is required. Which would include preparing reports and documentation or memos summarizing key risks and distributing them to all the stakeholders. Conducting presentations, workshops, or meetings to communicate risks effectively to key stakeholders. And the sector can also provide training sessions to educate the employee about the potential risks. Maintaining proper risk registers and dashboards which are easily accessible to relevant stakeholders, providing real-time visibility into the sector's risk profile, mitigation activities, and performance against risk management objectives. These details must be established in the annual report of the company so the risks can be transparent to the shareholders and investors. Illustrating key risks and their implications through case studies, examples, or scenarios relevant to the sector's context helps stakeholders understand the practical implications of risks and strengthen the importance of proactive risk management.

5. Monitoring and control

Risk monitoring and control are one of the key components of effective risk management in the IT sector. Regular Reviewing or Continuously monitoring identified risks and their associated factors. The purpose of Monitoring and controlling involves the ongoing observation, tracking of the risks and assessment of identified risks. This is done to understand effective changes in risk levels or trends over time to time. The main focus of monitoring is on

identifying and understanding risks, assessing them and providing early warning signs of potential risk events or trends. The primary outcome of monitoring is to provide stakeholders with timely and accurate information about the sector's risk profile, enabling informed decision-making and proactive risk management.

Risk management governance:

1. **Board**

The board of directors of the sector constitutes a committee called the risk management committee. The board may define the role and responsibilities of the Risk Management Committee. The board may delegate duties to the Risk Management Committee such as monitoring and reviewing the risk management plan.

2. **Risk management committee**

A minimum of 3 members must be there on this committee where the majority of members should be from the board and the chairperson also must be the member of the board. At least one independent director must be a member of the committee or two-thirds of the members must be independent directors. Senior executives can be a member of this committee. A meeting of this Risk Management Committee should be held at least twice a year with a quorum of two members or one - third whichever is higher in addition one board member must be present. The meeting cannot elapse for more than 180 days between two consecutive meetings. The power of the Risk Management Committee is it can seek information from any employee of the sector. The committee can also obtain legal or professional advice from the outsider, and secure the attendance of the other outside experts.

3. **Audit Committee**

The audit committee plays a crucial role in overseeing and supporting risk management in the sector. The Audit Committee oversees the audit of financial statements, which includes assessing risks related to financial reporting. The audit committee always maintains communication with senior management and the chief risk officer to stay informed about the key risk factors that are emerging in the sector. The Audit Committee reports its findings to the board and updates the risk profile of the sector. Overall, The Risk Management Committee

plays an important role in supporting effective risk management within an organization related to finance.

4. Other Sub-Committee

In addition to these committees, the sector can establish other sub-committees to focus on specified aspects of risk management. Some examples of sub-committees include the compliance committee where the committee focuses on ensuring the compliance of the sector with newly applicable laws, regulations, and industry standards. Cyber committee with the importance of cyber security risk management. The operational risk committee focuses on identifying and managing operational risks related to the sector. These committees work collaboratively with the Risk management committee and audit committee to ensure comprehensive risk management across the sector.

5. Chief Risk Officer

A Chief Risk Officer (CRO) is a senior executive responsible for identifying, assessing, and managing risks within the sector. The officer develops strategies to mitigate the risk. The Chief Risk Officer is typically appointed by the board of directors or senior management of the sector. The appointment process may vary depending on the sector's structure and governance policies. The chief risk officer may be appointed by the board of directors or sometimes even the CEO by consulting with the other senior executives. The chief risk officer is accountable directly to the board of directors. According to the structure of the organization and depending upon the governance practices of the sector it is possible to have a Chief Risk Officer in each major team or department to have a close look over possible risk. Having departmental chief risk officers allows for a more focused approach to risk management to the specific needs and challenges of each department.

Risk management policy

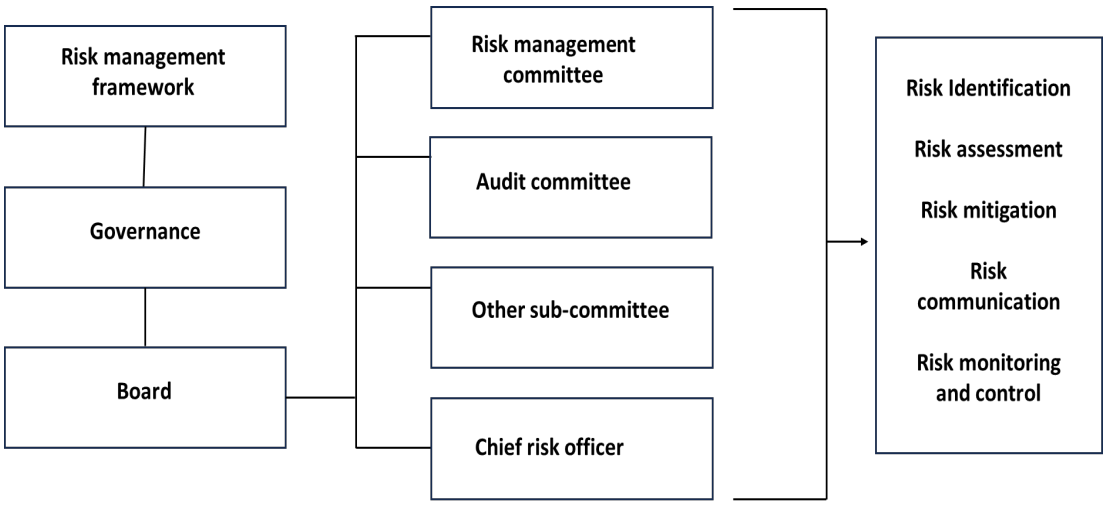
The sector should maintain policy regarding the measures taken for risk mitigation, and a framework for the identification of risk which may be internal risk or external risk. Methodology and processes of mitigation must be established in the policy. The policy must be reviewed periodically at least once in two years to obtain an effective risk management policy.

Risk Management Report

Risk management reports must be disclosed in the sector's annual report. In the Risk management report descriptions of the identified risks and their impact on the sector are denoted, evaluated risks and decisions on precautions including the implications or improvements made or to be made to the risk management system of the sector. An overview of the sector risk management framework including its goals, governance, structure, policies and procedures followed is expressed in the risk management report.

Disclosure

As we know the sector should maintain transparency to the stakeholders. Hence the information regarding the risk management governance must be disclosed in the annual report including composition, name of the members and chairperson of the committee. Meetings held and their attendance, brief description of the terms of reference, risk management framework, principal risk, its strategies. These regulations comply with 21 read with part D of schedule ll of the SEBI (listing obligation and disclosure regulations),2015. This disclosure procedure is to protect the stakeholder's interest may be an individual or group who will be affected when the sector acquires a loss.



ISO 31000 – Guidelines to build RMF

ISO 31000 is an international standard for risk management established by the International Organization for Standardization (ISO). It provides guidelines and principles for managing

risks effectively in organizations. The standard outlines a systematic and structured approach to identifying, assessing, treating, and monitoring risks, helping organizations make informed decisions to achieve their objectives, ISO 31000 provides a framework for organizations to manage risks effectively. ISO 31000 applies to all types and sizes of organizations in various sectors. It emphasizes integrating risk management into a sector's overall governance, strategy, and decision-making processes. sectors can alter the risk management framework to suit their specific needs, context, and risk appetite. Overall, ISO 31000 helps organizations proactively identify and address risks, enabling them to make informed decisions, protect their assets, and achieve their objectives. Hence sectors can adapt the guidelines to suit their risk management framework if needed.

Conclusion

In conclusion, implementing a robust risk management framework is essential for the Indian IT sector to mitigate various threats and uncertainties which have been a great fear in the industry. By adopting pre-emptive measures such as identifying risk, assessing risk, and mitigating risks, risk communication and also have a continuous process of controlling and monitoring the risks. So that Sectors can safeguard their operations, reputation, and stakeholders' interests. This framework should be dynamic, adaptable, and aligned with sector best practices to address emerging challenges in cybersecurity, data privacy, regulatory compliance, and business continuity. Furthermore, fostering a culture of risk awareness and accountability among employees is crucial for ensuring the effectiveness of the risk management framework across the organization. Ultimately, integrating risk management into their strategic planning processes, and proper governance in risk management is required in managing risk framework. So that, Indian IT sectors can enhance resilience, sustain competitiveness, and drive long-term success in an increasingly complex and volatile business environment.

References

Global standard ISO 31000

21 read with part D of schedule ll of the SEBI (listing obligation and disclosure regulations),2015

Tata Motors Annual Report 2022 -2023

Infosys Annual Report 2022-2023

Wipro Annual Report 2022-2023

Section 134 of the Companies Act 2013- report by the board of directors

The risk management policy of NSIC -2012

Section 177(3) of the Companies Act 2013 – terms of references to the audit committee

Clause 49 of the listing agreement – SEBI guidelines for listed companies says under the board disclosures

HCL Techs Annual Report 2022-2023