RISK MANAGEMENT REPORT

Risk Management Report

At Nucleus Software (The Company), Enterprise Risk Management is an extremely important discipline, managed by a robust governance and supported by Executive sponsorship, to keep identifying the possible risks related to our business strategy, business model, the ever evolving risks, the qualitative assessment exposures from these risks, effective prioritization of the risks and lay down the Mitigation processes and procedures to manage the emerging risks and ensure minimal impact to the company.

Your Company strive to achieve an appropriate balance between business growth and risk management, and continue to build, enhance, and evolve the risk management framework which enables us to achieve our business strategies with minimal risk exposures and impact.

Risk Management Objectives

The three main objectives of Risk Management at Nucleus are:

1. **Enable the Company to reduce the impact of risk events if they occur**
2. **Empower the Management to take informed decisions, under the guidance of our Board of Directors, to maximize value, reduce costs and balance risk with returns.**
3. **Promote confidence amongst the Company's stakeholders in the effectiveness of the Company's business management process and our ability to plan and meet strategic objectives.**

Your Company adopt a comprehensive approach to risk management that is conducted across the organisation at various levels.

A. Risk Management Framework at Nucleus:

B. Risk Management Group Structure at Nucleus:

1. The Board
2. The Audit Committee
3. The Risk Management Committee
4. Chief Risk Officer/Manager
5. The Risk Task Forces
6. Nucleites

At strategic level, the Risk Management committee:

1. Provides executive oversight to Company's Enterprise Risk Management Framework (ERMF), process, procedures, and controls.
2. Formulates a detailed risk management policy including the framework for identification of risks with a special focus to compliance, regulatory, cyber and info security, financial, operational, business continuity, and reputational risk; measures for risk mitigation; systems of internal control and business contingency plans.
3. Oversee Company's process and policies for determining risk threshold / tolerance and review management's measurement and comparison of overall risk tolerance to established levels.
4. Reviews the Risk Management at the required frequency, considering the changing dynamics.
5. Coordinate its activities with the Audit Committee in the instances of overlap with audit activities (e.g., internal, or external audit issue relating to risk management policy or practice)
6. Keep the Board informed about nature and content of discussions, recommendations, and actions to be taken.
7. Assist in selecting, appointing, removing, and finalizing the remuneration of the Chief Risk Officer (CRO), if any, subject to joint review with the Nomination and Remuneration/ Compensation Committee.
8. Nurture the culture of Proactive Risk Identification and Management as well environment of learnings and referred learnings.
9. Reward the professionals and teams, which are proactive in risk identification and exhibit creativity and innovation in managing the risks and related risk exposures effectively.
10. Develops creative thoughts and plans to shape the organizational maturity and behaviour towards the risk management.

C. Risk Categorization

The Company believes that all Risks can be categorized as follows:

1. Business environment related Risk
2. Regulatory and Compliance Risk
3. Technology related Risk
4. Operational Risk

The Risk Management Committee continuously monitors, and reviews various risks as identified for categorizing them under the above categories and finalize their mitigation plans.

While company keeps monitoring multiple risks in the ongoing basis along with their associated mitigation plans, few of the risks are mentioned below:

Risk Management Report

a. Cyber Security Risks

The risks of cyber-attacks are emerging as complex, high impact and high probability risks due to fast-evolving nature of the threat. This risk has potential to bring multi-dimensional impacts, including but not limited to Business continuity and growth, Reputational, and Legal Impact.

Nucleus was hit by a cyber breach attack in May 2021. The company has moved at a tremendous pace to take required steps to strengthen our security posture. Nucleus has become more resilient and continuous strengthening of our cyber security posture has become among the top focus avenues.

Comprehensive actions have been taken which includes the below but not limited to

i) Enhanced security for VPN
ii) World class Next Generation Firewall
iii) Focus on Network Security
iv) Multi Factor Authentication across all internet facing services
v) Comprehensive AV Guard
vi) End Point Detection and Response (EDR) solution
vii) Setting up of 24X7 Security Operations Center
viii) Enterprise mobility and Microsoft 365 Security
ix) Implemented Advance Email Security
x) Engaged Retainer Services of Cyber Security Expert Organization
xi) Availability of the right size and right skilled teams and continuous upskilling of the team

With 100% of your Company's workforce working from home during the COVID-19 lockdowns, we have taken additional steps to ensure that there are enough safeguards to maintain security and confidentiality of our data.

Connectivity to the employees to enable work from home has been allowed via highly secured Virtual Private Network (VPN)

Comprehensive background verification is carried out for our associates. Continuous awareness sessions are arranged for our associates advising them about the fast-evolving challenges and risks related to Cyber and Info Security. This is also backed by comprehensive and continuously enhanced processes and practices, tools, and platforms.

b. Risks related to Legal Compliance worldwide / Less than adequate protection of our Intellectual Property (IP) rights.

As an incorporated legal entity, the Company can be impacted by changes in various laws, rules, and regulations such as Companies Act, Accounting Standards, Labor laws, SEBI Regulations, etc. Our operations world-wide may be affected by changes in the political scenario, trade protection laws, policies and measures, and other regulatory requirements affecting trade and investment

The Company has an IP-led business model and globally licenses IP in the form of products for the Banking and Financial Services Industry. We rely on patent, copyright, trade secret and trademark laws, trade secret protection, and confidentiality or license agreements with our employees, customers, partners, and others to protect our intellectual property rights. Protecting our global intellectual property rights and combating unlicensed copying and use of software and other intellectual property is challenging.

Any inaction to prevent violation of any regulations or misuse of intellectual property could cause significant damage to our reputation and adversely affect our revenue and results of operations.

Various departments within the Company, are taking care of compliances of applicable laws/rules etc., are manned by qualified personnel. The Company has systems and processes in place to ensure the protection of our intellectual property rights.

As a policy, the Company develops own IP at its own cost using its own resources and is actively engaged in seeking maximum legal protection for the Intellectual Property through a combination of trademarks, confidentiality procedures and contractual provisions. There are also restrictions and controls put in our network to detect and report misuse of source code.

c. Risks related to attracting the right talent and retain the talent and ensuring no impact to business continuity and growth.

Nucleus being a product/IP-Led company, our knowledgeable associates are our most important assets, the talent domain knowledge and technical skills of our associates play a critical role in shaping our world class products and solutions. Great Resignation wave, Increased focus on Digitalization across the Globe, has put tremendous stress on talent availability across Industries and has impacted Nucleus as well and continues to be a business risk for the company.

High Attrition can happen due to many factors including continuously increasing compensation expectations, growth aspirations of the associates, peer pressure and emergence of new IT/FinTech Players in the industry bringing unprecedented career opportunities.

Right since the inception, Nucleus has been investing significantly in our assets, our associates, in terms of providing excellent career opportunities, knowledge upskilling, great employee engagement and great work life balance and compensation and benefits.

We are sticking to our basics and strengthening above mentioned measures. We have taken C&B of our associates to very high levels, launching intense employee engagements, enhancing the career opportunities available for the associates so associates can have crystalized career progression.

Executive leadership of Nucleus have been continuously connecting with all the associates to ensure the perfect alignment between our vision and our associates

Succession planning for the top leadership positions in each business unit is planned / driven and reviewed by senior management. Extending the same, heads of business units carry out succession planning for key functions within their business units, so Nucleus has strong teams and right talent across all the levels from top to junior most levels.