INMACS LIMITED

Corporate office:-909, Chiranjiv Tower , 43 , Nehru Place , New Delhi 110019

RISK MANAGEMENT POLICY

Our organization follows following process to manage risk:

Risk is an event which can prevent, hinder or fail to further or otherwise obstruct the enterprise in achieving its objective. Risk can cause financial disadvantage.

There may be different types of risks; some of them are as follows:

1. **Strategic Risk**: Risk associated with primary long term objectives and direction for business, revenue models, etc.
2. **Credit /financial Risks**:
    - Relating to clients: clients exposure policies and credit policies.
    - Relating to enterprises: process, techniques, instruments, used to manage the finance of an enterprise.
3. **Process/operation risk**: Risk associated with ongoing day to day operations of an enterprise.
4. **Information technology risk**: Risk associated with weak information technology environment and weak controls in it.
5. **Regulation risk**: Risk associated with non compliances of directions, rules and regulations of SEBI, and exchanges.

STRATEGIC RISK:

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

AGGREGATE LEVEL OF STRATEGIC RISK INDICATORS:

The following indicators should be used when accessing the aggregate level of strategic risk:

Low

Risk management practices are an integral part of strategic planning.Strategic goals, objectives, corporate culture, and behavior are effectively communicated and consistently applied throughout the institution. Strategic direction and organizational efficiency are enhanced by the depth and technical expertise of Management. Management has been successful in accomplishing past goals and is appropriately disciplined. Management information systems effectively support strategic direction and initiatives. Exposure reflects strategic goals that are not overly aggressive and are compatible with developed business strategies. Initiatives are well conceived and supported by appropriate communication channels, operating systems, and service delivery networks. The initiatives are supported by capital for the foreseeable future and pose only nominal possible effects on earnings volatility. Strategic initiatives are supported by sound due diligence and strong risk management systems. The decisions can be reversed with little difficulty and manageable costs.

Moderate

The quality of risk management is consistent with the strategic issues confronting the organization. Management has demonstrated the ability and technical expertise to implement goals and objectives, and successful implementation of strategic initiatives is likely. Management has a reasonable record in decision making and controls. Management information systems reasonably support the company's short-term direction and initiatives. Exposure reflects strategic goals that are aggressive but compatible with business strategies. The corporate culture has only minor inconsistencies with planned initiatives. The initiatives are reasonable considering the capital, communication channels, operating systems, and service delivery networks. Decisions are not likely to have a significant adverse impact on earnings or capital. If necessary, the decisions or actions can be reversed without significant cost or difficulty. Strategic initiatives will not materially alter business direction, can be implemented efficiently and cost effectively, and are within Management's abilities.

High

Risk management practices are inconsistent with strategic initiatives. A lack of strategic direction is evident. Strategic initiatives are inadequately supported by the operating policies and programs that direct behavior. The structure and managerial and/or technical talent of the organization do not support long-term strategies. Deficiencies in management decision-making and risk recognition do not allow the institution to effectively evaluate new products, services, or acquisitions. Management information systems supporting strategic initiatives are seriously flawed or do no exist. Strategic goals emphasize significant growth or expansion that is likely to result in earnings volatility or capital pressures.

The impact of strategic decisions is expected to significantly affect franchise value. Strategic initiatives may be aggressive or incompatible with developed business strategies, communication channels, operating systems, and service delivery networks. Decisions are either difficult or costly to reverse.

CREDIT /FINANCIAL RISKS IN RELATION TO CLIENT AND ENTERPRISES:

The company follows prudent risk Management policies by collecting requisite margin money from clients in selective cases which is decided based on track records of clients, trading pattern etc and the decisions are taken on case to case basis. The company has a dedicated team which monitors the debits balances on a daily basis. the company does not have any long outstanding debts.

The company follows the system of quarterly reconciliation with the client. Company maintains proper accounts of all its clients so that no mistake will occur while effecting securities pay-in and pay out and pay-out.

1. Company never indulges in client funding as a measure of prudent risk management.
2. While effecting trades on behalf of institutional clients, company follows the time schedule as prescribed by the Securities Regulations.
3. Company also takes care that it is not violating any of the provisions of applicable laws , rules or regulations.

MARGIN TRADING:

Company does not indulge in to Margin trading.

EXPOSURE AND TURNOVER:

Exposures are decided by the management for every client only after considering their previous trading habits, track record and financial status. These limits are reviewed periodically.

MARGIN COLLECTION:

The company follows the policy of collecting the margin money from the clients based on their nature of trading and payment in form of cash / securities.

PAY-IN OF FUND AND SECURITIES:

There is a system in place to ensure that there are no third party-in of funds and securities The Risk Management Team follows an adequate system to ensure that the company does not accept third party funds or securities.

REAL TIME BASIS:

There is adequate system in place through which risk management team can check and keep track of client position limits and mark to market on real time basis.

OPERATION RISK:

Operational risks are risks that every organization confronts. Generally, an operational risk is a risk that comes about from a company's execution of its business functions. The term operational risk is typically a broad term and includes some of the following; fraud risks, legal risks, physical or environmental risks. More specifically, operational risk can be defined as the risk of loss or incident resulting from insufficient or unsuccessful internal processes, people and systems, or from external events.

Operational Risks under control:

It can be difficult to manage the various risks across an organization's departments, and in some cases the various regions it operates in. The operational solution can track, trace and manage all of the various risks an organization must manage under perational risk, leading to a reduction in the associated costs of those risks. Risks can be entered into the operational solution by each department, and Internal Auditors can request risk assessments and surveys from individuals throughout the organization about those risks in the same solution. In fact, the departments throughout the enterprise will use the same system to manage and mitigate those risks, leading to less overhead, and time and cost efficiencies. Lastly, reports on risks, for example heat maps, can also be generated in the operational solution for executives and managers. Operational risk information can even be used automatically to generate dashboard views for risk managers.

INFORMATION TECHNOLOGY RISK MANAGEMENT PROGRAM:

An effective information technology risk management program is one that is designed to execute, manage, measure, control, and report on risk matters within information technology. If successful, an information technology risk management program provides the board of directors, senior management, regulators, and other stakeholders with the confidence that information technology can deliver business value efficiently and securely while providing high-quality assurance around data integrity, availability, and confidentiality.

Our Risk Management Framework Components :

Business Drivers— These conditions help determine why having an information technology risk management program is important or required from a business perspective. They reflect the purpose, mission, and vision of the program from the perspectives of business objectives, regulatory requirements, and board and executive management directives.

Risk Strategy—The risk strategy is a concise, high level plan that articulates the vision and direction for risk management within the organization. The plan should encompass risk tolerance guidance, risk processes, expectations for the risk management function, and the integration of risk processes with information technology operations.

Governance—Ownership, accountability, and oversight are the cornerstones of an effective information technology risk management program. Risk governance includes the organizational approach and operating model of the broader program, which supports the risk management

Policies and Standards—The information technology risk management program office define information technology policies, standards, and procedures with the participation of business and information technology functions. The decision-making process should be designed to be fair to all stakeholders, while ensuring that the execution of policies and standards is managed effectively, and that they appropriately reflect the organization's risk appetite.

Risk Identification and Profiling— The organization needs to define a consistent process for identifying and classifying risk. This includes defining a taxonomy for risk and internal controls, risk ratings and prioritization, and parameters for the frequency and rigor of information technology risk and internal control assessments. Risk ratings and risk prioritization are critical to management's efforts in aligning risk management resources effectively across the enterprise.

The data obtained through the risk identification process make it possible to profile and then prioritize the various risks and profile categories. As the organization prioritizes its risks, management utilizes the established risk categories or profiles to group risks across information technology systems and processes. An example of a potential grouping might be change management for distributed computing environments, where an organization may have identified several discrete issues for this information technology process. After the information technology process areas are defined, the organization should identify key indicators (KIs), including Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and Key Control Indicators (KCIs). The KIs must be articulated for each information technology process area. Ideally, KIs are simple and measurable. KIs may be linked to risks and controls contained in a

risk and control library. The library, which presents definitions for all risks and controls, helps ensure that risks and controls are classified and assessed consistently throughout the enterprise.

Processes and Operational Procedures—Processes and operational procedures represent the heart of the execution phase of the program and should be directly linked to the appropriate risk management standards. Core risk processes should include:

- Risk assessments, risk control assessments (RCA), and risk control self-assessments (RCSA)
- Detailed risk analyses, including scenario or threat vulnerability analyses
- Risk reporting
- Issues risk management
- Event capture and loss estimates
- Risk mitigation planning
- Risk acceptance and exception processes

Risk management processes should be aligned with legal and regulatory requirements and should include or link to relevant activities such as privacy initiatives, information security, and continuity of business. For large organizations to implement risk processes consistently, they must utilize strong communications, focused change management processes, process guidance, and training.

Tools and Technology—Risk management tools and technology vary in maturity and capability. Many large organizations tend to build their own risk management systems or use multiple commercially available risk management applications. They may process their business requirements with a reporting tool that can aggregate various risk elements and information. Organizations should reassess the vulnerability and compliance technology tools already in place to ensure they have the relevant risk management measurements and reporting capabilities in areas such as threat and vulnerability protection, availability monitoring, and entitlements.

People and Organizational Management— An appropriate management structure at the functional and line levels enables the organization to make the transition from a risk management initiative to a full program with enterprise-wide operational capabilities for information technology risk management. Most organizations underestimate the time frame required for this maturation process. In most cases, it takes two to three years from program start-up to engineer risk processes successfully into operational procedures that are fully integrated throughout a large global organization. Therefore, it is important to understand the risk management target environment, end state, and interim solutions. design, implementation,

and measurements right can be difficult and time-consuming. Building an framework and processes. The structure enables organizations to make the appropriate risk decisions and supports the ability to exercise guidance over all risk activities. A key element of governance is the need for effective policies and standards.

Policies and Standards— The information technology risk management program office should help define information technology policies, standards, and procedures with the participation of business and information technology functions. The decision-making process should be designed to be fair to all stakeholders, while ensuring that the execution of policies and standards is managed effectively, and that they appropriately reflect the organization's risk appetite.

Risk Identification and Profiling—The organization needs to define a consistent process for identifying and classifying risk. This includes defining a taxonomy for risk and internal controls, risk ratings and prioritization, and parameters for the frequency and rigor of information technology risk and internal control assessments. Risk ratingsand risk prioritization are critical to management's efforts in aligning risk management resources effectively across the enterprise.The data obtained through the risk identification process make it possible to profile and then prioritize various risks and profile categories. As the organization prioritizes its risks, management utilizes the established risk categories or profiles to group risks across information technology systems and processes. An example of a potential grouping might be change management for distributed computing environments, where an organization may have identified several discrete issues for this information technology process. After the information technology process areas are defined, the organization should identify key indicators (KIs), including Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and Key Control Indicators (KCIs). The KIs must be articulated for each information technology process area. Ideally, KIs are simple and measurable. KIs may be linked to risks and controls contained in a risk and control library. The library, which presents definitions for all risks and controls, helps ensure that risks and controls are classified and assessed consistently throughout the enterprise.

Compliance, Monitoring, and Reporting—This is the critical juncture for information technology risk management. The organization puts in place its processes to assess risks and compliance with policies, standards, procedures, and regulatory requirements. Monitoring and reporting capabilities are designed to provide management with organizational views and trend analyses for risks, control issues, and vulnerabilities. When designing metrics for monitoring and reporting, many organizations start with the end product (information technology risk management dashboards) to ensure that their metrics will be aligned with executive management's vision and requirements. Obtaining and reporting on KIs are critical for

organizations to demonstrate the value of the program and verify that risk management processes have been implemented. Getting the KI design, implementation, and measurements right can be difficult and time-consuming. Building an information technology risk management program is a challenge. But an appropriately designed program helps break down silos and allows the organization to look across functional areas to address risk objectives most effectively.

REGULATION RISK:

We have proper training system for updating the rule and regulation of SEBI and NATIONAL STOCK EXCHANGES for employee of organization.
Our compliance officer has active involvement regarding dissemination of rule and regulation issued by said authority on day to day basis.

For & on behalf of INMACS LIMITED

Sd/-
Vinod Jain (Director)