Risk Management Policy

Version 1.0

MOSCHIP

RISK MANAGEMENT POLICY

1. Introduction:

MosChip Established in 1999, which is a publicly traded semiconductor and system design services company headquartered in Hyderabad, India. MosChip has over a 20+ year track record in designing semiconductor products and SoCs for computing, networking, and consumer applications.

Moschip operates across multiple geographies and serving multiple international clients across the industry and most of the companies are blue chip companies working in tight regulatory norms. MosChip risk management policy is tailored to address the unique challenges and opportunities inherent in business.

From the business perspective, it is pertinent to note that:

- the risks that the business faces are identified, tracked, monitored, mitigated and managed;
- a proper framework is evolved for understanding, managing, reporting and reviewing the risks at periodic intervals.

Risk literally means the effect of uncertainty on the objectives. It is the chance of something happening which will have an impact on the objectives of a company. Risk is measured in terms of consequences and likelihood.

Risk Management is a systematic and formal approach in mitigating and managing risks. It is process which is towards achievement of potential opportunities while managing adverse effects.

An effective risk management promotes operating efficiency by better understanding of the risks associated with accomplishment of business goals, enhancing capital efficiency through improved profitability besides reducing volatility. The requisites for an effective risk management are:

- strategic focus
- forward looking approach;
- striking a balance between risk management and anticipated benefits thereof
- business continuity plan in event of critical threats
- translation of risk management strategy into operational aspects

The risk management framework of the Company comprises the risk management policy which lays down the structure of the process at the Company and business levels as well as the risk management structure which facilitates the enterprise wide risk management process.

Statutory and Regulatory Requirement

- Section 134(3) of the Companies Act, 2013 requires a statement to be included in the report of the board of directors ("Board") of the Company, indicating development and implementation of a risk management policy for the Company, including identification therein of elements of risk, if any, which, in the opinion of the Board, may threaten the existence of the Company.

- Regulation 17 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended ("Listing Regulations"), requires that the Company set out procedures to inform the Board of risk assessment and minimization procedures and makes the Board responsible for framing, implementing and monitoring the risk management plan of the Company

2. Policy Overview:

The Company's risk management policy relates to identification, assessment, monitoring and mitigation of various risks to our business. The policy seeks to minimize adverse impact on our business objectives and enhance stakeholder value. Further, our risk management practices seek to sustain and enhance long–term competitive advantage of the Company.

Objectives and Principles of the policy

The prime objective of this Risk Management Policy and Procedure is to ensure sustainable business growth with stability and establish a structured and intelligent approach to Risk Management at MosChip Technologies Limited. This would include the process for development and periodic review of the unit-wise Risk Registers and Databases in order to guide decisions on business risk issues. This would promote a proactive approach in analysis, reporting and mitigation of key risks associated with the business in order to ensure a sustainable business growth.

The specific objectives of the Risk Management Policy are:

1. To establish a risk intelligence framework for the organization;

2. To establish ownership throughout the Organization and embed risk management as in integral part of the business rather than a stand-alone system

3. To help the decision makers of the organization explicitly take account of uncertainty, the nature of that uncertainty, and work towards a solution to address it

4. To ensure that all the current and expected risk exposures of the organization are identified, qualitatively and quantitatively evaluated, analysed and appropriately managed

5. To enable compliance with the relevant legal and regulatory requirements and international norms

6. To assure demonstrable achievement of objectives and improvement of financial stability of the organization.

Risk Management Principles

The basic principles on which the risk management framework of the Company is developed are:

- Identification of risks within the ambit of available financial resources to manage and improve the profitability of the business exposed to risks.
- Alignment with overall corporate objectives to protect the Company's reputation.
- Evaluation of Company's strategic business panning
- Dynamic approach in risk identification and mitigation which is preventive in nature
- Identification of risk impacts including, financial risk, regulatory risks, reputational risks, etc.
- Detailed internal control procedures which are aligned with risk management perspective
- Balanced approach in mitigating risks and managing opportunities
- Awareness of risks and its mitigation plans amongst the employees

- Responsibility of individual employees have responsibility for maintaining appropriate internal controls and risk mitigation in their sphere of activities.
- Senior Management have primary responsibility for managing business risks.
- Periodic review of the risks and the mitigation procedures thereof.

3. Risk Management Framework:

Risk management will protect and add value to the organization and its stakeholders through supporting the organization's objectives by improving decision making, planning and prioritization by comprehensive and structured understanding of business activity, volatility and project opportunity/threat.

It will provide a framework that enables future activity to take place in a consistent and controlled manner. The framework will help in creating an environment in which risk management is consistently practiced across the Company and where Management can take informed decisions to reduce the possibility of surprises.

The components of risk management are defined by the company's business model and strategies, organizational structure, culture, risk category and dedicated resources. An effective risk management framework requires consistent processes for assessment, mitigation, monitoring and communication of risk issues across the organization. Essential to this process is its alignment with corporate direction and objectives, specifically strategic planning and annual business planning processes. Risk management is a continuous and evolving process, which integrates with the culture of the Company.

3.1 Risk Management Structure:

The Risk Management Committee of Directors shall review the risk management policy of the Company and evaluate the risk management systems so that management controls the risk through a properly defined network.

Head of Departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning.

3.2 Risk Management Process:

The risk management process adopted by the Company has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:

- ✓ Establishing the Context
- ✓ Risk Assessment (identification, analysis & evaluation)
- ✓ Risk Treatment (mitigation plan)
- ✓ Monitoring, review and reporting
- ✓ Communication and consultation

Detailed flow of the risk management process

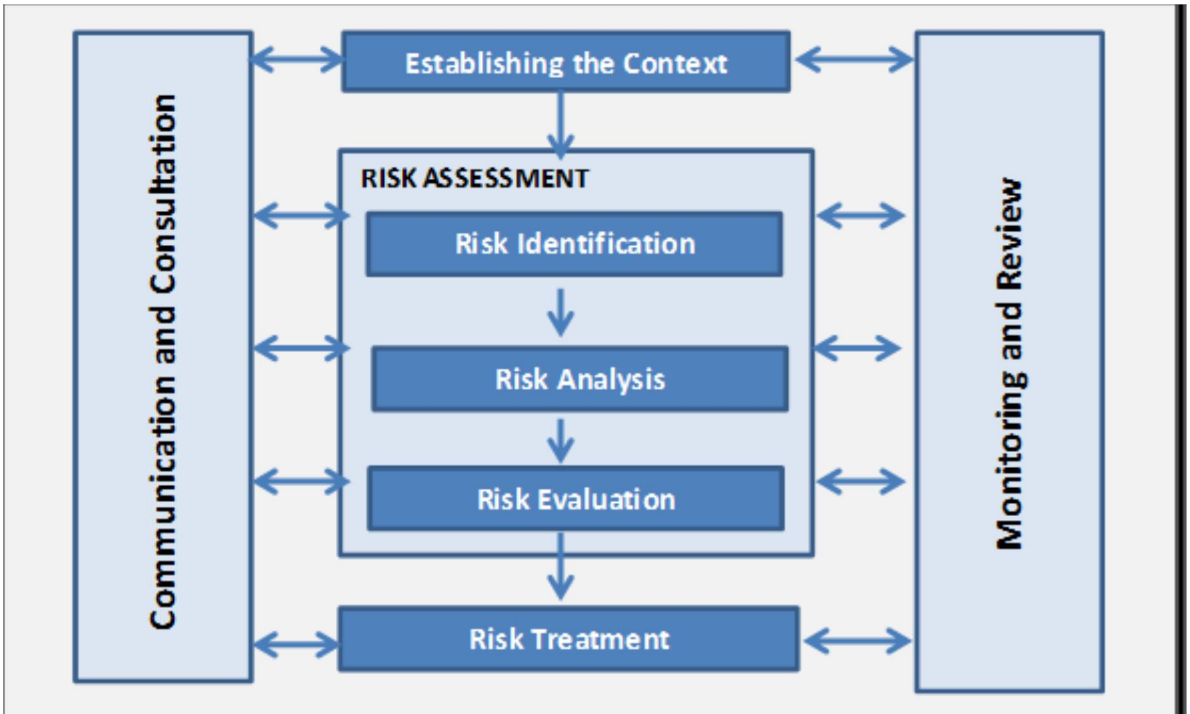


Figure 1: Risk Management Process

3.2.1 Establishing the Context

Articulate the objectives and define the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

Establishing the External Context

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.
The external context can include, but is not limited to:

- ✓ The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- ✓ Key drivers and trends having impact on the objectives of the organization; and
- ✓ Relationships with, perceptions and values of external stakeholders

Establishing the Internal Context

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way risks will be managed

It is necessary to understand the internal context. This can include, but is not limited to:

- ✓ Governance, organizational structure, roles and accountabilities;
- ✓ Policies, objectives, and the strategies that are in place to achieve them;
- ✓ Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- ✓ The relationships with and perceptions and values of internal stakeholders; the organization's culture;
- ✓ Information systems, information flows and decision making processes (both formal and informal);
- ✓ Standards, guidelines and models adopted by the organization

3.2.2. Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

a) Risk Identification

Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself. This stage involves identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

b) **Risk Analysis**

Risk analysis involves:

- ✓ consideration of the causes and sources of risk
- ✓ the trigger events that would lead to the occurrence of the risks
- ✓ the positive and negative consequences of the risk the likelihood that those consequences can occur

Factors that affect consequences and likelihood should be identified. Risk is analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

c) **Risk Evaluation**

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

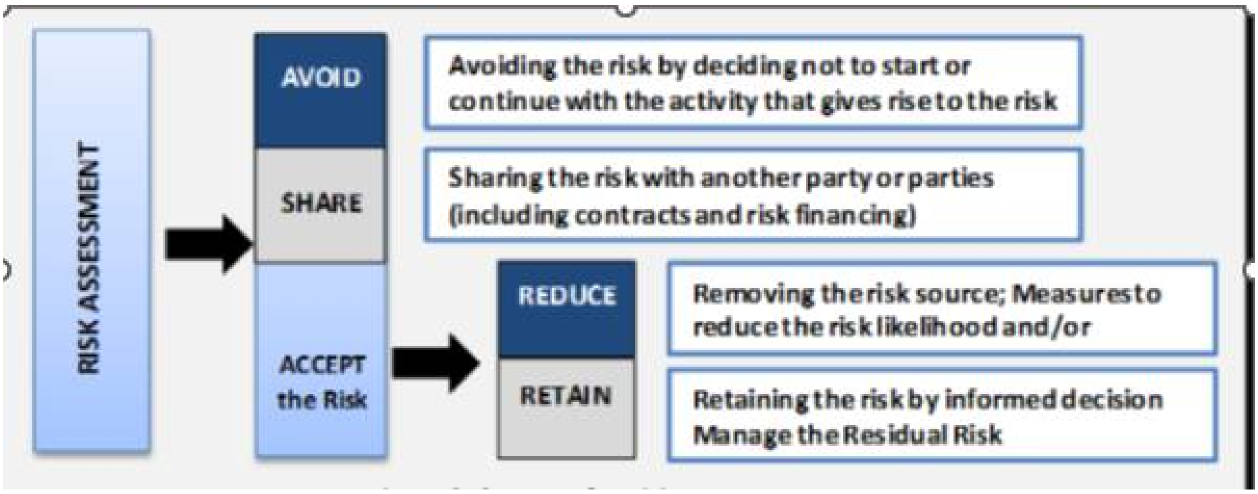
Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties, other than the organization, that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

d) Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.
Risk treatment involves a cyclical process of:

- ✓ Assessing a risk treatment;
- ✓ Deciding whether residual risk levels are tolerable;
- ✓ If not tolerable, generating a new risk treatment; and
- ✓ Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:



i. Avoidance (eliminate, withdraw from or not become involved)

As the name suggests, risk avoidance implies not to start or continue with the activity that gives rise to the risk.

ii. Reduction (optimize - mitigate)
Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

iii. Sharing (transfer - outsource or insure)

Sharing, with another party, the burden of loss or the benefit of gain, from a risk

iv. Retention (accept and budget)

Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

v. Monitoring and review

In order to ensure that risk management is effective and continues to support organizational performance, processes shall be established to:

- ✓ Measure risk management performance against the key risk indicators, which are periodically reviewed for appropriateness
- ✓ Periodically measure progress against, and deviation from, the risk management plan
- ✓ Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context
- ✓ Report on risk, progress with the risk management plan and how well the risk management policy is being followed
- ✓ Periodically review the effectiveness of the risk management framework.

F. Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

4. Risk Categories & Mitigation Measures:

Please referrer enclosed spread sheet

5) Creation of Risk Register

Risk Register shall be the key document used to communicate the current status of all known risks. Risks identified shall be documented in the risk register by the Risk Manager. The Risk Register shall inter alia include the following:

- ✓ List of risks
- ✓ Root causes for each risk
- ✓ Impact- high, medium and low
- ✓ Mitigation plan

6) Review and Reporting

- The status of implementation of the approved Mitigation plans shall be reviewed by the Risk Managers (Business unit head) and reported to Chief Risk Manager as frequently as required. This report to Chief Risk Manager shall also indicate any Policy deviations, failure of existing mitigation plans and other major issues, if any, faced during the period.

- The Chief Risk Manager shall review the Report of the Risk Managers and shall identify the high impact risks (along with the mitigation plan), for the purpose of reporting to Risk Management Committee ("RMC") on a Half yearly basis. This report to RMC shall also indicate any Policy deviations, failure of existing control measures and other major issues, if any, faced during the period.

- RMC shall review the Report of the Chief Risk Manager and suggest measures, if required. Further, it shall also escalate High Impact Risks as it deems necessary to the Board twice a year or at such other intervals as RMC deems necessary.

- Board shall review the RMC's Report and provide strategic direction for effective risk management.

7). Roles and Accountabilities in Risk Management

Every employee of the Organisation is responsible for the effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies. Risk management processes should be integrated with other planning processes and management activities**.** Training and facilitation will, in the first instance, be the responsibility of the Office of Internal Audit/Risk Manager in conjunction with the Office of Human Resources.

The Board of Directors

The Directors shall ensure that a risk management system is established, implemented and maintained in accord with this policy. Assignment of responsibilities in relation to risk management is the prerogative of the Managing Director of the Company.

Risk Management Committee

The day to day oversight and management of the Company's risk management program has been conferred upon the Committee. The Committee is responsible for ensuring that the Company maintains effective risk management and internal control systems and processes, and provides regular reports to the Board of Directors on the effectiveness of the risk management program in identifying and addressing material business risks. To achieve this, the Committee is responsible for:

- ✓ managing and monitoring the implementation of action plans developed to address material business risks within the Company and its business units, and regularly reviewing the progress of action plans;
- ✓ setting up internal processes and systems to control the implementation of action plans;
- ✓ regularly monitoring and evaluating the performance of management in managing risk;
- ✓ providing management and employees with the necessary tools and resources to identify and manage risks;
- ✓ regularly reviewing and updating the current list of material business risks;
- ✓ regularly reporting to the Board on the status of material business risks;
- ✓ review and monitor cyber security; and
- ✓ ensuring compliance with regulatory requirements and best practices with respect to risk management.

Business Unit Head

Business Unit Heads shall have the prime responsibility for the management of risk in their business unit. They shall ensure all the contractual obligation, deviation from them may result in serious risk on the respective project and overall profitability of the Organisation. This includes the identification of risks and actions that mitigate these risks while supporting the business to achieve its objectives. The Business Unit Heads shall act as Risk Managers for their respective business unit.

Chief Financial Officer

The CFO of the Company shall ensure the financial stability along with a risk management plan. Advice will be sought from the Internal Auditor/statuary Auditor on risk management issues in relation to these matters. The CFO will also act as Chief Risk Manager for the administration of Risk Management Policy.

Human Resources - Head

The head of HR shall ensure for the occupational health and safety and workers compensation portfolio, procedures and administration, hiring process, employee benefits & Supervision.

General

The Board of Directors of the Company and the Risk Management Committee shall periodically review the risk management policy of the Company so that management controls the risk through properly defined network. Risk Managers shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning and report to the Chief Risk Manager/RMC/Board.

The decision of the Board of Directors of the Company with regard to any or all matters relating to this policy shall be final and binding on all concerned. The Board of Directors of the Company shall have the power to modify, amend or replace this policy in part or full as may be thought fit from time to time in their absolute discretion.

8) Risk Management Reporting Structure: