Solar Energy Corporation of India Ltd.

Risk Management Policy

July, 2018

VISION

To build ‘Green India’ through harnessing abundant solar radiation and to achieve energy security for the country.

MISSION

- To become the leader in development of large scale solar installations, solar plants and solar parks and to promote and commercialize the use of solar energy to reach remotest corner of India.

- To become leader in exploring new technologies and their deployment to harness solar energy.

CONTENTS

1. INTRODUCTION

Risk Management is a mechanism for dealing with various aspects of associated risks in managing any business activity. It is a structured approach to manage risk resulting from all kinds of threats and involves treatment of risk, embracing both the analysis and handling of risks, using appropriate forms of risk control. Therefore, in the broadest terms, Risk Management is concerned with the planning, organizing and controlling of activities and resources in order to minimize the impact of risks.

The objective of the risk management is to reduce risks related to a pre-selected domain to an acceptable level. It may refer to numerous types of threats caused by environment, technology, humans, organization and politics. On the other hand it involves all means available to humans or to a risk management entity (employees, other stakeholders and organization). The Risk Management strategies include avoiding the risk, reducing the negative effect of the risk, transferring the risk to another party and accepting some or all of the consequences of a particular risk.

Risk Management makes an effective contribution to the achievement of the corporate objective and is an integral part of various functional management areas.

SECI, being active in many segments of the Renewable Energy domain, such as scheme implementation, project development, consultancy and power trading, faces significant sector-specific and location-specific risks in its business activities. Risk Management for projects assumes greater significance in the wake of inherent risks associated with Social, Environment, Geo-technical conditions etc. In addition there are uncertainties, often linked to political pressures, environmental and social aspects etc. that may have adverse impact on project delivery and cause time and cost overrun. Similarly, for Plants under operation there are threats of accidents, machine break down, generation loss etc. For sustainable development all these risks need to be effectively handled.

SECI's business areas encompass pan-India. Further, SECI is working on expanding and diversifying its business segments in terms of technologies, geographies, delivery mechanisms etc. All these activities carry a certain level of risk. The major risk categories can be defined as:

- Change in Government Policies
- Exposure to international events due to globalization
- Sector dynamics
- Technology changes
- Volatility in Financial markets
- Interest rate and Foreign exchange fluctuations

- Lack of expertise in new areas

Hence, in today's uncertain and volatile business world, the need to manage risk more coherently, comprehensively and economically through effective Risk Management System is more critical than ever. This Risk Management Policy is an effort to give directions to adopt suitable mitigation measures in subsequent chapters.

1.1 Scope and Objectives

Risk Management Policy has been developed to assist in establishing and maintaining an effective risk management framework for SECI. SECI operates in a business environment that is characterized by intensifying competition and a greater number of government regulations. Further, increasing speed of business activity and opportunities for expansion and diversification are rapidly changing and expanding the quantum and importance of risks faced by the company. Risk management framework assists the management in effectively dealing with uncertainty and associated risks & opportunities, thereby enhancing the organization's capacity to build value.

Key objectives of the 'Policy" is to:

1. To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed;
2. To establish a framework for the company's risk management process and to ensure companywide implementation;
3. To ensure proactive rather than reactive management;
4. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices;
5. To provide assistance to and improve the quality of decision making throughout the organization;
6. To assure business growth with financial stability.

Further, it applies to all employees of SECI and to every part of SECI's business and functions.

1.2 Principles of Risk Management

To achieve these objectives, SECI shall adhere to the following core principles:

Effective Risk Management Process: The Risk Management Committee constituted by the Board shall have the overall responsibility to ensure effective risk management process within the company.

Everyone's commitment: Every function/ department/ office in the organization shall work in coordination to ensure effective implementation of this risk management policy.

Proactive Leadership: Risk identification (including identification of the risk of lost opportunities), risk assessment, risk response and risk monitoring are ongoing activities and shall form an integral part of the company's operations, management and decision Making process. All the identified risks shall be updated in the central repository.

Risk Culture: Informed and consistent risk related decisions shall be taken, noncompliant behaviours shall not be tolerated and risk management shall be dealt professionally.

Transparency and Compliance: The risk management activities along with the most Significant risks shall be reported and the material failures in mitigation measures shall be escalated through reporting line to the relevant levels of organization structure.

Result Evaluation: To assess the effectiveness of the Risk Management Policy and its implementation and need for improvement if any.

1.3 Extent of Application

The policy guidelines are devised in the context of the present business areas, future growth objectives, business profiles envisaged and new business endeavours. This policy is meant to ensure continuity of business and protection of interests of the investors and thus covers all the activities within the organization and events outside which have a bearing on the organization's business.

The policy shall operate in conjunction with other business and operating / administrative policies. The Risk management process shall become part of, and not separate from other organizational processes and in particular should be embedded into the policy development, business and strategic planning and review and change management processes.

There shall be an organization-wide risk management plan comprising activity/project-wise operation plans to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes.

The policy will be a guiding document for risk management with an endeavour to facilitate the decisions at SECI.

1.4 Terms and Definitions

Risk - Risk is often described by an event, a change in circumstances or a consequence that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. Thus, risk is the effect of uncertainty on objectives.

Risk Management - Risk Management is the coordinated activities to direct and control an organization with regard to risk. It is the process whereby organizations methodically address the risks attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

Risk Management Policy - Risk Management Policy is a statement of the overall intentions and direction of an organization related to Risk Management.

Risk Management Framework - Risk Management Framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving Risk Management throughout the organization.

Risk Strategy - The Risk Strategy of an organization defines its readiness towards dealing with various risks associated with the business. It describes the organization's risk appetite or tolerance levels and decision to transfer, reduce or retain the risks associated with the business.

Risk Assessment - Risk Assessment is defined as the overall process of risk identification, risk analysis and risk evaluation.

Risk Estimation - Risk Estimation is the process of carrying out quantitative, semi-quantitative or qualitative assessment of risk in terms of the probability of occurrence and the possible consequence.

Risk Identification - Risk Identification is a process of finding, recognizing and describing risks.

Risk Tolerance / Risk Appetite – Risk Tolerance or Risk Appetite is a driver of Risk Strategy of an organization. It defines the maximum quantum of risk which the company is willing to take as determined from time to time in consonance with the Risk Strategy of the company.

Risk Description - A Risk Description is a comprehensive template covering a range of information about a particular risk that may need to be recorded in a structured manner. It is an input to the Risk Register.

Risk Register - A 'Risk Register' is a tool for recording the risks encountered at various locations and levels in a standardized format of Risk Description. It becomes a major input in formulating subsequent Risk Strategy.

Risk Treatment - Risk Treatment is a process to modify a Risk. It that deals with negative consequences is also referred to as 'Risk Mitigation', 'Risk Elimination', 'Risk Prevention' and 'Risk Reduction'. It can create new risks or modify existing Risks.

Residual Risk - Residual Risk is a risk remaining after Risk Treatment. It can contain unidentified risk and also be known as 'Retained Risk'.

2. RISK MANAGEMENT FRAMEWORK

Key elements of Risk Management Framework include (a) Risk Assessment, (b) Risk Organization Structure, (c) Risk Measuring & Monitoring, and (d) Risk Optimization & Treatment.

The implementation of the framework is supported through criteria for risk assessment and categorization, risk matrix, risk forms & MIS. The overall objective of risk management process is to optimize the risk-return relationship.

2.1 Risk Assessment

Risk assessment enables objective quantification of risks and their outcomes, through a system of Risk identification, Risk analysis and Risk evaluation. The Process entails the following key steps:

a) Risk Identification and Categorization – the process of identifying the company's exposure to uncertainties, generally classified as Business Environment / Strategic Business / Operational.

b) Risk Description – the method of systematically capturing and recording the company's identified risks in a structured template covering a range of information about the risk.

c) Risk Estimation – the process for estimating the cost of likely impact either by quantitative, semi-quantitative or qualitative approach in terms of the probability or occurrence and the possible consequences.

Risk Assessment is done through various techniques, such as questionnaires, checklists, workshops, inspections & audits etc. and is documented in a systematic manner in a Risk Matrix.

The purpose of the assessment is to assist in making decisions about which risks need treatment and priority of treatment implementation.

2.2 Risk Organization Structure

A formal risk organization structure with defined roles and responsibilities for risk management activities is an essential prerequisite for an effective risk management framework. Board of Directors (BOD) is overall responsible for overseeing and approving the risk management strategy and policies. BOD may delegate the responsibility and authority of assessing effectiveness of the risk management procedures to the Audit Committee and Risk Management Committee (RMC).

RMC is the owner of the Risk Management Process and reviews risk management activities including Risk Register, on periodic basis for which it receives periodic updates on identified risks from the Risk Assessment Committee. Chief Risk Officer (CRO) provides updates to the Audit Committee and the Board, based on decisions of RMC, through the Managing Director.

2.3 Risk Mitigation Strategy

There are four common strategies for treating risk. There is no single "best" response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

- **Risk avoidance/ termination:** This involves doing things differently and thus removing the risk. This is particularly important in terms of project risk, market risk or customer risk but often wishful thinking in terms of the strategic risks.
- **Risk reduction/ mitigation:** Reduce or Treat the risk. This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either:
    - **Containment actions** (lessen the likelihood or consequences and applied before the risk materializes) or;
    - **Contingent actions** (put into action after the risk has happened, i.e. reducing the impact. Must be pre-planned)
- **Risk acceptance/ retention:** Accept and tolerate the risk. Risk Management doesn't necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The organization shall tolerate such risks that are considered to be acceptable, for example:
    - a risk that cannot be mitigated cost effectively;
    - a risk that opens up greater benefits than loss
    - uncontrollable risks

The Risk Assessment Committee shall take a decision to tolerate a risk as a mitigation measure, and when such a decision is taken, the rationale behind it shall be fully documented. In addition, the risk shall continue to be monitored and contingency plans shall be in place in the event of the risk occurring.

- **Risk transfer:** Transfer some aspects of the risk to a third party. Examples of risk transfer include insurance and hedging. This option is particularly good for mitigating financial risks or risks to assets.
    - The following aspects shall be considered for the transfer of identified risks to the transferring party:
        - Internal processes of the organization for managing and mitigating the identified risks.
        - Cost benefits analysis of transferring the risk to the third party.
    - Insurance can be used as one of the instrument for transferring risk.

Risk Mitigation Process

The risks are identified and if the risk treatment mechanism selected is risk mitigation or risk transfer, the next step shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also to identify new and improved controls.

Risk Mitigation Process

Identify controls

New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite.

Control activities are categorized into Preventive or Detective on the basis of their nature and timing:

- Preventive controls – focus on preventing an error or irregularity.
- Detective controls – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

Implement Controls

It is the responsibility of the Risk Assessment Committee to ensure that the risk mitigation plan for each function/department is in place and is reviewed regularly.

2.4 Risk Monitoring & Review

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the risks with their mitigation measures shall be updated on a regular basis.

The following process shall be followed:

Quarterly

1 The departments/projects shall review and report the status of risks and treatment actions to the CRO on quarterly basis. In addition, CRO shall identify any new or changed risk on quarterly basis.

2 The Risk Assessment Committee shall monitor and supervise the development and implementation of the Risk Management Policy and maintain wide view of the key risks and their mitigation measures faced by the organization on quarterly basis.

3 The CRO along with the other members of the Risk Assessment Committee shall identify the key risks and suggest mitigation measures to the departments/projects on quarterly basis.

Half yearly

The Risk Assessment Committee shall report the key risks and their mitigation plans to the Risk Management Committee on bi-annual basis.

Annually

The Risk Management Committee shall apprise the Audit Committee and the Board, through the Managing Director, on the key risks faced by the organization and the mitigation measures taken on annual basis.

Risk Review

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.

Audits of policy and standards compliance shall be carried out periodically and standards performance reviewed to identify opportunities for improvement. It shall be remembered that organization is dynamic and operates in dynamic environment. Changes in the organization and the environment in which it operates must be identified and appropriate modifications made to risk management practices. The monitoring process shall provide assurance that there are appropriate controls in place for the organization's activities and that the procedures are properly understood and followed.

Risk monitoring and review process shall also determine whether:

- The measures adopted resulted in what was intended.
- The procedures adopted and information gathered for undertaking the assessment was appropriate.
- The acceptability of each identified risk and their mitigation plan shall be assessed and risks shall then be ranked to identify key risks for the organization.
- Proposed actions to eliminate, reduce or manage each material risk shall be considered and agreed.

Responsibilities for the mitigation measures for key risks management of each risk shall be assigned to appropriate functional heads.

MIS may be developed by the Chief Risk Officer for gathering report of risks and early warning in respect thereof from the project managers. The anticipated risks in a project/activity should be captured during the project planning stage and after project completion by the project team.

The risks are then compiled systematically in a 'Risk Register' that acts as a central repository of key risks and is accessible to all functional heads within their span of control. Purpose of the risk register is to record identified key risks and related information in a structured manner. Reports drawn from the register are used to communicate the current status of all known risks and are vital for assessing management control, reporting and reviewing the risks faced by SECI. Sample format of Risk register is given in **Annexure B**.

The 'Risk Register' should contain the following information:

i. Identified key risk
ii. Risk description
iii. Risk category
iv. Risk owner
v. Root cause(s)
vi. Impact and probability
vii. Planned response with timelines

The Risk Register may be updated on quarterly/bi-annual basis by RMC. Chief Risk Officer is responsible for preparation and maintenance of the Risk Register.

3. RISK ASSESSMENT

3.1 Identification and categorization of risks

As defined earlier, Risks are often described by an event, a change in circumstances or a consequence that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives.

The organization should identify sources of risk, areas of impacts, events and their causes with potential consequences. The aim 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. Comprehensive identification is critical, because a risk that is not identified here will be missed from further analysis. This should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects.

The organization should apply risk identification tools and techniques compatible to its objectives and capabilities and to the nature of business. Relevant and up-to-date information including background information is important.

Key characteristics by which risks can be identified are:

• Risks are adverse consequences of events or changed circumstances

• Their occurrence may be identified by the happening of trigger events

• Their occurrence is uncertain and may have different extents of likelihood

Recognizing the kind of risks that SECI is/may be exposed to, risks can be classified broadly into the following categories:

1. **Business Environment Risk**: include the range of external events and trends (like Government policy, competition, court rulings or a change in stakeholders' requirements) that can adversely impact the organization's strategic growth trajectory and destroy shareholders' value.
2. **Strategic Business Risk**: include the risks associated specifically with the organization and having an adverse impact on the organization's capability to execute activities critical for business growth, thereby affecting its near-term performance.
3. **Operational Risk** : are those risks which are associated with operational uncertainties like unpredictable solar radiation levels, supply chain uncertainties, acts of nature like floods affecting operations, internal risks like attrition etc.

A list of potential risks for SECI, as per its business areas, is given at **Annexure C**. it may be noted that the list is non-exhaustive, and would be updated periodically as per business environment changes and experience gained.

3.2 Risk Description and Estimation

Risk Description provides an input to decisions on whether risks need to be treated and on the most appropriate risk treatment strategies and methods. It involves consideration of the causes and sources of risk, their likelihood consequences and identification of the factors that affect them.

Consequences can be expressed in terms of tangible and intangible impacts. In some cases more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

A risk description helps in understanding the nature and quantum of risk and its likely impact and possible mitigation measures. Risk descriptions for each of the risks identified in earlier sections are to be documented and recorded in a structured template in each area where the risk is identified. Suggested template is given in.

In this process, the consequences of the risk occurrences have to be quantified to the maximum extent possible, using quantitative, semi-quantitative or qualitative techniques.

Process of risk quantification for the organization has to be qualitative, supported by quantitative impact analysis. To apply this approach, the chain of adverse consequences which may occur in case the identified risk materializes, should be enlisted.

For each of the chain of adverse consequences, efforts will be made to quantify its impact for each particular risk. In such an exercise, estimated cost impact like claims by contractor, loss of equipment value etc. as well as opportunity cost like loss in realization of revenue, delay in commissioning of project etc. will be considered.

According to the adverse impact analysis for identified risks, an appropriate risk category shall be determined for each risk identified as per the criteria below:

Consequences of Risk (Cost of Impact – Stakeholder or Strategic or Financial)	
Devastating	✓ Significant stakeholder concern ✓ Significant impact on strategy or operational activities ✓ Cost of impact is likely to be or exceed ₹ 100 Crores p.a.
Major	✓ Major stakeholder concern ✓ Major impact on strategy or operational activities ✓ Cost of impact is likely to be ₹ 50 Crores or more but less than ₹ 100 Crores p.a.
Tolerable	✓ Moderate stakeholder concern ✓ Moderate impact on strategy or operational activities

	✓ Cost of impact is likely to be ₹ 10 Crores or more but less than ₹ 50 Crores p.a.
Minor	✓ Minor stakeholder concern ✓ Minor impact on strategy or operational activities ✓ Cost of impact is likely to be less than ₹ 10 Crores p.a.

A suggested template for description and estimation of risks is given in **Annexure A- Risk Reporting Template.** The template may be updated time to time, preferably on quarterly/bi-annual/annual basis.

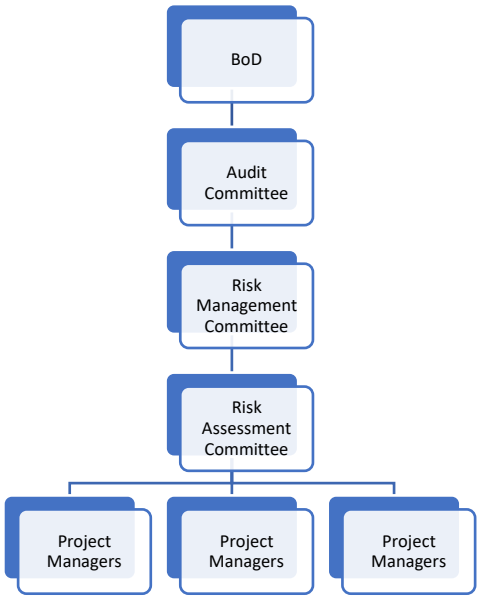
4. Risk Governance Structure

A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities for the management of risks on a day to day basis.

In order to develop and implement a Risk Management framework, a Risk Assessment Committee would be constituted. Risk Assessment Committee shall identify the key risks and report them to the Risk Management Committee which shall ensure that risk management activities are undertaken as per this policy.

The main objective of the Risk Assessment Committee shall be to provide a wide view of key risks within the organization to the Risk Management Committee.

Following is the Risk Organization Structure of SECI:



4.1 Risk Management Committee

The Risk Management Committee would normally comprise of functional heads of departments, as nominated by the concerned Directors/Managing Director.

Role and Responsibilities of the Risk Management Committee

- Assist the board in fulfilling its corporate governance in overseeing the responsibilities with regard to the identification, evaluation and mitigation of operational, strategic and external environment risks.
- Monitor, approve and review the risk policies/ plans and associated practices of the company.
- Review and approve risk disclosure statements in any public documents or disclosures.

- Ensure that appropriate systems are in place to manage the identified risks, so that the organizations assets and reputation are suitably protected.
- Ensure that responsibility and authorities are clearly defined and adequate resources are assigned to implement the Risk Management Policy.
- Review the reports from the Risk Assessment Committee and take remedial action.

4.2 Risk Assessment Committee

The Risk Assessment Committee shall comprise of Chief Risk Officer (CRO) and officers, not below Manager level, nominated from different departments.

Role and Responsibilities of Risk Assessment Committee

- The Risk Assessment Committee shall have the key role of identifying the key risks, suggest mitigation measures, monitoring and supervising the implementation of the Risk Management Policy and maintain wide view of the key risks faced by the organization.
- Identify, evaluate and assess the key risks anticipated for the organization and suggest mitigation measures to the project managers through the functional heads.
- Ensure that effective risk mitigation plans are in place and the results are evaluated and acted upon.
- Report the key risks faced by the organization and their mitigation plans to the Risk Management Committee.
- Ensure that the Risk Management Committee is informed about any new/emerging risks faced by the organization in case of exigencies/emergent conditions.
- Assist the Risk Management Committee in overseeing and monitoring the development and implementation of the Risk Management Policy.
- Prioritize the risks reported according to their risk ratings and assist the risk management committee in decision making for risk management responses for identified key risks.

Chief Risk Officer

The Chief Risk Officer (CRO) shall be nominated by Managing Director and not below the rank of Senior Manager, who works with the project managers and functional heads to ensure effective implementation of wide risk management process. The CRO shall be the convenor of the Risk Assessment Committee meeting.

Roles and Responsibilities of the CRO:

- Communicating and managing the establishment and ongoing maintenance of risk management policy pursuant to the organization’s risk management vision.
- Designing and reviewing processes for risk management.

- Communicating with the Risk Management Committee regarding the status of risk management and reporting the key risks faced by the organization.
- Coordinate with all the Risk Coordinators to compile the status of risks and mitigation measures taken.
- Convene the Risk Assessment Committee meeting and facilitate discussions among the committee to fulfill its responsibilities.

4.3 Risk Reporting Structure

The following risk reporting structure shall be followed by the organization:

First Line of Reporting

- The project managers shall send the report on status of risks to the CRO, through the functional heads, in the format as provided at **Annexure-A** on quarterly basis.
- The CRO shall send the report on status of risks and mitigation measures taken to the Risk Assessment Committee on quarterly basis.

Second Line of Reporting

- The CRO along with the other members of the Risk Assessment Committee shall review the risks with their mitigation measures and decide upon the key risks which shall be reported to the Risk Management Committee on bi-annual basis.
- Upon approval of the Risk Assessment Committee of the risks and mitigation measures, CRO shall record it in the risk register with their mitigation plans and shall inform the concerned project managers for implementation of the mitigation plans, through the functional heads, on quarterly basis.
- Upon deciding and implementing the mitigation plan the Risk Assessment Committee through the CRO shall present it to the Risk Management Committee on bi-annual basis.

Third Line of Reporting

- The Risk Management Committee shall apprise the Audit committee and the Board, through the Managing Director, on the key risks faced by the organization and the mitigation measures taken on annual basis.
- The Risk Management Committee shall also apprise the Board for decision on any new/emerging risks faced by the organization in case of exigencies/ emergent conditions.

5. OPERATION OF RISK MANAGEMENT POLICY

Risk Management in the company will look into all organizational processes involved in advance detection of risks as well as in identifying and taking suitable action to counter them.

Deployment of integrated planning, control and monitoring systems and corporate governance systems and fine tune them on an ongoing basis to ensure that risks are detected at early stage and properly assessed and appropriately managed.

Risk management, a key success factor will form an integral component of company's management system. To promote risk awareness throughout the company, risk culture at all levels shall be developed through the mechanism of review framework, progress monitoring and discussions in open forums.

All identified risks will be assigned an impact, probability, category, timescale and action to be taken. This will be complemented with focus on quantitative reporting. A key element of early warning system will be regulated through a mechanism in which project managers will inform the functional heads, who in turn will inform the Chief Risk Officer about the probable/potential risk.

Chief Risk Officer shall compile all reported risks on quarterly basis with such details about risks in tabular form. This analysis will form an integral part of reporting and will be periodically reviewed by the Audit Committee/Board.

5.1 Approval of the Policy

SECI Board shall be approving authority for the company's overall Risk Management Policy. The Risk Management Committee shall monitor the compliance of the Risk Management Policy and any amendments thereto from time to time.

5.2 Review of the Policy

The risk management policy shall be reviewed in every two years based on changes in the business environment/ regulations/ standards/ best practices in the industry. However, in case of exigency, the same may be reviewed earlier also.

5.3 Maintenance of Risk Register

Centralized Risk register with their mitigation plan shall be maintained by CRO and shall be reviewed and updated as per the policy guidelines. The key risks with their mitigation measures identified and reviewed for the organization would be defined in the Risk Register.

ANNEXURE A- RISK REPORTING TEMPLATE

Risk Reporting Template

S. No.	Risk Classification	Risk Description	Risk Rating	Risk Response, Treatment and Control Mechanisms	Timeline for Completion	Progress (Completed/ in progress/ overdue)	Revised timeline for completion (if Overdue)

Note : *To be sent by the department/project managers to the CRO on quarterly basis.*

ANNEXURE B- RISK REGISTER

Risk Register Template

S. No.	Risk Classification	Risk Sub-category	Responsible Division	Risk Description	Risk Rating	Risk Mitigation Measures	Associated Divisions

Note : *To be sent by the department/project managers to the CRO on quarterly basis.*

ANNEXURE C: SAMPLE LIST OF BUSINESS-SEGMENT RISKS

(a) Scheme Implementation

- Lack of clarity in government guidelines/scheme documents
- Inadequate time for preparation of RfS documents
- Dynamic policies/rapid changes in Government guidelines
- Inadequate implementation time results in insufficient need assessment for the scheme may result in scheme failure
- Power evacuation issues
- Lack of Discoms support
- Release of similar schemes by multiple stakeholders at a time
- Lack of responses in schemes
- Non-readiness of land and power evacuation infrastructure before issue of RfS
- Release of multiple tenders with similar scope in quick succession
- Discovery of higher than expected price/tariff
- Projects getting held up due to implementation issues
- Projects getting into litigation/ legal issues
- Projects getting held up due to owner approval
- States also publish their own tenders
- New taxes implementation
- Availability of rooftops
- Unpredictable consumer behavior
- Adverse climatic conditions
- Changing MNRE policy

(b) Own Projects Development

- Delay in finalization of land and PPA
- Design risk
- Non standardization of technical specifications / technical eligibility criteria
- Project gets on hold after release of NIT
- Projects cancellation on account of various reasons after release of NIT

- Insufficient no. of bids in response to the NIT
- Discovery of higher than expected prices leading to impact on tariffs
- Discom backing off from signing of PPA post finalization of award recommendations
- L1 bidder backing off after issuance of LoA
- Implementation issues leading to time and/or cost overrun
- Supply chain issues
- Tariff finalization by CERC/SERC at sub-optimal level, resulting in lower returns for SECI
- Change in market prices during implementation period
- Change in taxes during implementation
- Dependence on external expert for design review.

(c) Project Management Consultancy

- Changing technologies
- Lack of standards available in new technologies
- Lack of quality assurance
- Lack of quality audit
- Lack of standardization of documents such as RfS/PPA
- Lack of adequate testing facilities of high-tech solar products in India
- Delay in finalization of land and PPA
- Design risks
- Non standardization of technical specifications / technical eligibility criteria
- Project gets on hold after release of NIT
- Projects cancellation on account of various reasons after release of NIT
- Insufficient no. of bids in response to the NIT
- Delay in issuance of LoA by client after submission of award recommendations
- L1 bidder backing off after issuance of LoA
- Implementation issues leading to time and/or cost overrun
- Supply chain issues
- Tariff finalization by ERC at sub-optimal level, resulting in lower returns for SECI
- Change in market prices during implementation period
- L1 price is higher than expectation
- Change in taxes and duties/new taxes implementation

- Discovery of abnormally low price
- Vendor back-out
- Dependence on external expert for design review.

(d) Power Trading

- Change in policies/regulations pertaining to open access, transmission, RLDC / SLDC charges, QCA, Auxiliary consumption, scheduling etc.
- Opening of LC by Discoms
- Signing of TPA as payment security
- Variation of state-wise DSM regulation
- Decline nature of solar and wind power tariff restricted to 3rd party sale
- No Payment Security Mechanism (PSM) for wind power scheme
- Delay in payment realization from Buying utilities (Discoms)
- Reduction in generation from power plants
- Failure of power plant(s) to generate power
- Dishonouring of PSAs by Discoms
- Dishonouring of PPAs by developers

(e) Strategic Risks

- Major dependence on one client
- Changing Customers preferences
- Reputation Risk
- Lack of responsiveness towards change in economic conditions
- Intense competition
- Information Technology
- Quality Control and Time Management
- New Project viability
- Supplier provisioning risk
- Mgt Contracts & JVs
- Environmental Risk
- Change in technology
- Change in rules / act relating power sector guidelines
- Compatibility with state guidelines/policies
- Environmental norms
- Manufacturing risk
- Operations Failure Risk
- Construction Defect
- Weather Volatility
- Political Risk (Domestic, International)
- Reputation Risk (Company, Product/Service Defamation)
- Regulatory Risk
- Manpower Risks – Specialized manpower leaving the jobs
- Increasing competitors

- sharing confidential information with competitors
- risk being underutilization/placement in areas where they are misfit
- Change Managements Risks
- Risk of Materials and Inventory
- Land risk
- Equipment failure

(f) Financial Risks

- Credit default risk
- Foreign Exchange Risks
- Incorrect Financial Reporting Risk
- Earning Volatility Risk
- Project Financing (Debt Equity)
- Labor and Material Costs (Contract, Outsourced)
- Earnings Volatility (Revenue Recognition, EPS Growth)
- Currency Fluctuation (Foreign Exchange, Arbitrage)
- Interest Rate Changes (Credit and Interest Rate Risks)
- Commodity Price Fluctuations (Derivatives)
- Regulatory Exposures (Company's Act, Accounting Standards)
- Funding Risks (Government Contract Funding/ Allocations)
- Liquidity Risk resulting in cash flow problems, Imposition of fresh or increased taxed or levies on the industry, by the Government
- Fall in profitability on account of increased cost not matched by prices, and also falling price of products.
- Errors in release of payment to third parties
- Non-repayment of interest/principal on timely basis
- Default in compliance of taxation issues
- Misappropriation of funds
- Insolvency of any of SECI's operational banks
- Errors/fraud in processing of employees claims
- Financial reporting risk
- Financial solvency and liquidity risk
- Foreign exchange variation risk in cases of foreign currency loan exposure
- Ability of the company to arrange finance for project
- Non-realization of outstanding dues from the state Discoms on timely basis
- Human errors resulting in errors in release of payments/processing of claims
- Non-maintenance of proper records, notes and documents
- Probability of banks not honouring deposits kept with the Bank

(g) Contractual Risks & Exposures

- Contractual Liability (Breach, Third Party Actions)
- Indemnification (Hold Harmless Clauses)
- Indemnification Forms (Limited, Intermediate and Broad)
- Design Responsibility (Design Delegation, Assumption of Risk)
- Warranties (Express, Implied)
- Waivers of Subrogation
- Liquidated, Consequential and Punitive Damages Clauses
- Force Majeure Clauses (Schedule Delay)
- Subcontractor Default, Abandonment
- Security Validity, exemption, policy/ scheme implementation
- Non standardization of the Technical Specifications/Technical Eligibility criteria
- Projects gets on hold after release of NIT
- Projects cancellation on account of various reasons after release of NIT
- Less/No bids in response to the NIT/Tender
- Case of single bid tender
- LOA/Contract denial by the Contractor/MSME bidders
- SECI being pioneer in various one of its kind Projects & schemes. So, chances of regulatory/ statutory non-compliance may arise due to lack of appropriate knowledge base regarding that particular domain.
- Non vetting by the legal team for all contracts irrespective of size/nature
- Tender is floated prior to signing of PSA
- Delay in process due to due to Delegation of Power
- Delay due to non-clarity in schemes
- Delay in award of LoA to successful bidder due to owner approval
- Delay in commissioning due to FC not completed on schedule due to land issue.

(h) Commercial Risks

- Revenue loss due to non-performance of vendors

(i) Human Resource Risks

- Inadequate succession planning
- Inability to attract quality personnel
- Employees Health & Safety
- Employees' relations
- Restriction on compensation due to Govt guidelines
- High attrition rate in employees
- Fraud & Integrity
- Manpower risk (in terms of acquisition, retention and attrition)

- Ensuring confidentiality of commercial and trade secrets
- Risks involved in increasing medical costs under SECI policy
- Provisioning of gratuity, leaves and other superannuation benefits on actuarial valuation and separate deployment of fund
- Adequate employees group insurances for personal accidents and other eventualities
- Assets insurance coverage
- Directors liability under companies act
- Professional indemnity policy for unintentional loss caused to third party
- Legal and regulatory compliances
- Data security and management
- Employee compensation and employer's liability

(j) **Legal Regulatory & Compliance Risks**

- Regulatory compliances
- Taxation
- Commercial Interests not protected by Legal Agreements
- Nonconformance or inability to comply with rules, regulations
- Contractual Liability, etc.
- Legal vetting of contracts

(k) IT Risks

- ERP outage
- Threat of sabotage
- Security incident
- Cyber attack
- Network intrusion
- Insufficient IT infrastructure
- Unavailability of Backup in case of System Failure.

(l) External Risks

- Major dependence on one client
- Changing Customers preferences
- Reputation Risk
- Lack of responsiveness towards change in economic conditions
- Intense competition