Document Title	Risk Management Policy
Version number	V1.0
Document Authoriser	Board of Directors of Indian Cricketers’ Association
Authorised date	
Signature	

RISK MANAGEMENT POLICY

CONTENTS

1. <u>BACKGROUND</u>

1.1. The Board of Directors of **Indian Cricketers' Association**('ICA')/**Company** has adopted the following policy with regard to risk management and to identify the elements of risks, which may threaten the existence of the Company. The Policy is documented to create and protect the stakeholder's value by minimizing threats or losses and identifying and maximizing opportunities.

1.2. This document lays down the framework for Risk Management and shall be under the authority of the Board of Directors of the Company. The Policy seeks to identify risks inherent in the ICA's operations of the Company and provides guidelines to define, measure, report, control and mitigate the identified risks.

1.3. This Policy shall come into force with effect from 01 April 2020.

2. LEGAL FRAMEWORK

2.1. The provisions of Section 134 of the Companies Act, 2013 ("2013 Act") must include a statement indicating development and implementation of a risk management policy for the company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the company.

2.2. The provisions of the Section 134 are applicable to **Indian Cricketers' Association**.

3. DEFINITIONS

3.1. **Board of Directors" or "Board"** in relation to a Company, means the collective body of Directors of the Company as defined under Section 2(10) of the 2013 Act.

3.2. **Policy** means Risk Management Policy.

3.3. **Risks:** The threat that an event or action, the occurrence/non-occurrence of which can adversely affect the objectives/existence of the Company. These threats may be internal/ external and may arise out of routine/non-routine actions of the Company. Such risks impact upon the organization's ability to achieve its ICA's objectives and execute its strategies successfully.

3.4. **External Environment:** The current external (i.e. largely non-controllable) factors that must be taken into consideration when assessing a risk, e.g. political, economic, regulatory and competition variables.

3.5. **Internal Environment:** The specific elements of the current control environment that support people in the achievement of the ICA's objectives, e.g. structure, systems, skills, culture, processes.

3.6. **Risk Management:** A structured, consistent and continuous process that is directed towards realizing, identifying, assessing and reporting the threats that that may affect the achievement of our objectives.

4. OBJECTIVE OF THE RISK MANAGEMENT POLICY

4.1. The main objective of this Policy is to be guarded against the everchanging risks that the ICA is exposed to and for a sustainable growth and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the operations.

4.2. The objectives of Risk management at ICA are:

a) To better understand the risk profile of the ICA in connection with its operations;

b) To ensure that the ICA's strategy and plan take in account the risks that the ICA is or may be exposed to;

c) To consider and review the Risk Management Policy of the ICA as may be required from time to time based on changes in the external, transactional and internal environment with the aim to enhance the Company's ability to achieve its strategic objectives;

d) To ensure effective monitoring of the risks being managed within the levels of appetite and tolerance and ensure that risks are prioritized and assessed accordingly.

5. POLICY FRAMEWORK

5.1. Risk Management and Risk Monitoring are important in recognizing and controlling risks. Risk mitigation is also an exercise aiming to reduce the loss or injury arising out of various risk exposures.

5.2. The ICA adopts a systematic approach to mitigate risks associated with accomplishment of its objectives. The Company believes that the Policy would ensure mitigating risks proactively and help to achieve stated objectives. The Company will consider activities at all levels of the organization and its Risk Management with focus broadly on three key elements, viz.,

(i) Risk identification
(ii) Risk Management and Monitoring
(iii) Risk Mitigation

6. RISK MANAGEMENT

6.1. ***Risk Identification***

This would envisage identification of the potential list of events/ perils/ risks/ factors that could have an adverse impact on the achievement of ICA's objectives. Risks can be identified under the following broad categories –

Sr#	Risks	Potential factors
1.	Strategic Risk	Inadequate capacity, high dependence on a single/ vendor/ brand.
2.	Business Risk	Not Applicable since ICA is not for profit organisation
3.	Personnel Risk	Health & safety, high attrition rate, incompetence of personnel
4.	Operational Risk	Breakdowns in internal procedure
5.	Reputation Risk	Doping, Other Malpractices on the part of members or players
6.	Finance Risk	Liquidity, credit, bad debts, currency fluctuation
7.	Regulatory Risk	Non-compliance to statutes, change of regulations, change in government policies, legal uncertainties

8.	Technology Risk	obsolescence, performance of IT systems, audio video failure
9.	Political Risk	Changes in the political environment, regulation/ deregulation due to changes in political environment, political instability
10.	Litigation Risk	Legal proceedings against the Company

6.2. Whether risks to the Company are from an external or internal environment, or can/ cannot be directly influenced/ managed, they are addressed by a common set of processes through the Risk Management process. This process is scheduled to be performed by the Directors of the Company:

- at any point of time on account of significant changes in internal conduct or external environment.
- when the ICA seeks to undertake a non-routine transaction.

6.3. ***Risk Evaluation***

After risk analysis/ identification, a comparison of estimated risks against organization risk criteria is required to be made by the Board of Directors. Risk evaluation is to be used to make decisions about the significance of risks and whether each specific risk is be accepted or treated.

6.4. ***Risk prioritization***

This process involves assessing the relative priority of each risk to arrive at the key risks. The potential impact and likelihood of occurrence of the risk needs to be assessed by the Board of Directors.

6.5. ***Risk Mitigation***

The Board of Directors need to treat the Risk through the process of selecting and implementing measures to mitigate risks; also to prioritize risk control actions in terms of their potential to benefit the organization. The risk mitigation can be planned using the following key strategies:

a) **Risk Avoidance**: By not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.

b) **Risk Transfer**: Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging.

c) **Risk Reduction**: Employing methods/ solutions that reduce the severity of the loss.

d) **Risk Retention**: Accepting the loss when it occurs. Risk retention is a viable strategy for small 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.

6.6. ***Reporting of Risk*:** The Board of Directors need to report the Risks to the stakeholders on regular basis.

7. KEY RISKS SPECIFIC TO THE COMPANY AND MITIGATION MEASURES ADOPTED

7.1. OPERATIONAL RISKS

Operational risk is defined as the potential loss resulting from inadequate internal processes, human and technical failure, fraud and/or external events. All operational risks are reviewed, analyzed and assessed on a regular basis in order to promptly detect deficiencies in policies, procedures and processes, and to propose and implement corrective actions. Operational risks are managed and controlled by –

- Appropriate policies, processes and procedures;
- Regular measures to identify and evaluate operational risks;
- quarterly/annual monitoring and reporting;
- A sound internal controls system including separation of function, plausibility checks, avoidance of conflict of interests; and
- Appropriate testing and documentation.

In terms of Information Technology (IT) a systematic security concept is in place governing access rights and preserving data availability and integrity.

Main target is to continuously improve the Company's risk awareness and the operational risk culture. The Board of Directors are responsible for reviewing application and effectiveness of operational risk management procedures.

7.2. LEGAL AND REGULATORY COMPLIANCE RISK

The risk is defined as the risk that a change in laws and regulations will materially impact the Company's business sector or market. A change in laws or regulations made either by a government or regulatory body could possibly increase the costs of operation. Due to the continually increasing demands from the regulators, we recognize that this has an impact on our day to day operations.

The Company has stated clearly that the Company has no appetite for regulatory breaches. Therefore, we continue to expand the knowledge and awareness of regulatory and compliance requirements throughout the Company by creating a network of responsible representatives, to ensure that we stay abreast of these developments around the world.

7.3. REPUTATIONAL RISK

The risk is defined as the risk that the Company may be exposed to negative publicity about its practices or internal controls, whether accurate or not, resulting in an impact on the confidence in the integrity of the institution. This relates to stakeholders including existing and potential client relationships, donors, suppliers and supervisors.

We consider the reputational risk a byproduct of operational, regulatory or strategic risk which could manifest itself through weaknesses or failures in our internal control environment. Thus, we manage these risks through the use of policies, processes and a robust internal control environment.

8. BOARD OF DIRECTORS

8.1. Board shall approve the Risk Management (including Risk Treatment) strategy, control structure and policy guidelines.

8.2. Board shall perform the risk treatment which includes risk control/ mitigation and extends to risk avoidance, risk transfer (insurance), risk financing, risk absorption etc. for effective and efficient operations, effective Internal Controls, Compliance with laws and regulations.

8.3. Board shall have the discretion to deal with certain risks (may be called Key or Highly Sensitive Risks) in the manner it may deem fit. Mitigation of such Highly Sensitive/Key risks and effectiveness of their mitigation measures and review of the strategy may be directly discussed by the Board members with such persons as the board may deem fit.

8.4. The Board of Directors shall review the Policy as & when decided by the board to ensure it meets the requirements of legislation and the needs of organization.

9. LIMITATIONS

The Risk Management Framework does not intend to provide complete assurance against failures to achieve ICA its objectives, nor does it provide full assurance against material misstatements, losses, frauds, human errors, misjudgements in decision-making and violations of legislation and regulations.