1. PURPOSE

The purpose of this policy is to establish a comprehensive and structured framework for identifying, assessing, monitoring, and managing risks associated with trustea's operations and its engagement with business partners. This includes safeguarding the integrity, credibility, impartiality, and sustainability objectives of the trustea programme while ensuring alignment with international best practices.

This policy further aims to ensure that risks arising from operational, reputational, legal, technological, and partnership-related aspects are proactively identified and effectively mitigated.

2. SCOPE

This policy applies to all operational areas of *trustea* and to all categories of partners engaged in the implementation and delivery of the scheme. It covers risks arising from both internal systems and external associations.

The policy is applicable to:

- Certification Bodies (CBs)
- Certified Entities (tea estates, factories, smallholder groups)
- Vendors and Service Providers
- Funders
- Oversight Bodies
- Internal systems including IT and data management infrastructure

3. POLICY STATEMENT

trustea recognises that its effectiveness and credibility depend on robust risk management practices. The organisation is committed to systematically identifying and managing risks associated with its partners and operations, including those that may arise from unethical practices, non-compliance, conflicts of interest, data mismanagement, or reputational exposure.

trustea further acknowledges that risks may arise from digital systems, including data security, traceability platforms, and information management systems, and commits to ensuring their integrity, confidentiality, and reliability.

All risk management activities are integrated into the broader organisational risk management framework and are periodically reviewed to ensure continued relevance and effectiveness.

4. DEFINITION OF TERMS

- **Enterprise Risk Management** - "ERM" is the process of identifying, analyzing and managing risks. It provides the methodology for integrating risk into the strategic planning and resource allocations processes.
- **Risk** Effect of uncertainty on objectives. Risk includes any issue (positive or negative) that may impact an organization's ability to achieve its objectives,"
- **Risk management:** coordinated activities to direct and control an organization with regard to risk
- **Stakeholder/Interested Party:** person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
- **Risk source:** element which alone or in combination has the potential to give rise to risk
- **Event:** occurrence or change of a particular set of circumstances
- **Consequence:** outcome of an event affecting objectives
- **Likelihood:** chance of something happening
- **Control:** measure that maintains and/or modifies risk
- **Analysis** - is the process of determining the likelihood of a particular event, trend or course of action occurring and the impact on operational or strategic objectives if it does.
- **Risk Owners** - personnel typically responsible for one or more functions, and are directly responsible to implement risk treatments as directed by management.
- **Risk Register** - a list of identified enterprise risks which documents the risk analysis, risks scores, risk treatments, direction, result of risk treatments and status of each risk.
- **Risk Tolerance** - sometimes known as risk appetite, is the level of risks the organization is willing to accept for any event, trend or course of action. Risktolerance will vary depending on the potential effect of the risk on the organization's operational or strategic objectives.
- **Risk Treatment** - sometimes known as risk control, is the measures used to modify the risk to fall within the organization's risk tolerance for that risk. Options include accept, mitigate, transfer, avoid or exploit the event, trend or course of actions.

5. BENEFITS

After successful implementation of ERM, trustea Foundation expects the following benefits:

a) More efficient use of capital and resources

b) Reduced likelihood of operational loss

c) Earlier detection of non-compliant activities

d) Fewer surprises

e) Focus on prevention rather than resolution strategies

f) Using risk information to streamline and improve processes

g) Increased awareness and integrated view of risks (existing and emerging)

h) Systematic, repeatable approach to mitigate risks and identify opportunities

i) Clearer, better-informed decision making

j) Maintain the credibility and level of trust amongst stakeholders

6. ROLES AND RESPONSIBILITIES

Trustea Foundation has established the framework of responsibilities and actions which are consistent with the following generally recognized basic principles of sound risk management practice.

a. The development of risk management processes that provide for risk and exposure monitoring;

b. The embedding or integration of risks management into all activities as an integral part of the enterprise's business activities; and

c. Clearly defined accountability and responsibility for the ERM

6.1 Key accountability and oversight:

The Director of the trustea Foundation will hold the executive accountability of the ERM subject to oversight by the trustea Foundation Council as per existing governance protocol.

The trustea Foundation Council will undertake oversight of the program, including:

• Responsibility for approving the Policy, reviewing the effectiveness of the risk management processes and articulating the risk appetite of Trustea Foundation;

• Responsibility for approving policies on governance, risk and

• Delegating responsibility to Executive Management in managing the program.

6.2 The Executive Management:

The roles and responsibilities of the trustea Foundation Executive management led by the Director and the direct reports, includes but is not limited to the following:

- Risk management planning and oversight;
- Ensuring sound risk management systems and practices are established and maintained to give effect to this Policy
- Designing and implementing appropriate risk management processes and controls; and
- Establishing a sound risk aware culture

6.3 The Risk Management Committee

The Risk Management Committee ("RMC") under the leadership of the Director presently comprises the following members:

1. Director
2. Assurance Systems Head
3. IT Head

Based on the nature of the risk or occurrence, the RMC may co-opt specialists to provide necessary inputs.

In discharging its governance responsibilities relating to risk management, the RMC will:

- Review and recommend for the approval of the risk management policy, risk management strategy, risk management implementation plan, organization's risk tolerance, and risk identification and assessment methodologies.
- Evaluate the extent and effectiveness of integration of risk management within the organization;
- Assess implementation of the risk management policy and strategy (including plan);
- Evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the organization;
- Develop its own key performance indicators
- Meet as per defined meeting schedule-presently defined as one review per quarter
- Provide timely and useful reports to the Trustea Foundation Council on the state of risk management, together with accompanying recommendations to address any deficiencies identified.

6.4 Employees

Employees are responsible for integrating risk management into their day-to-day activities. Some highlevel responsibilities include:

- Applying the risk management process in their respective functions;

- Implementing the delegated action plans to address the identified risks;
- Informing the management of new risks and significant changes in known risks; and
- Co-operating with other role players in the risk management process and providing information as required.

7. CATEGORIES OF RISK

trustea adopts a comprehensive approach to risk identification by categorising risks across key domains relevant to scheme operations, partner engagement, and system integrity. Each category reflects potential exposure areas, typical risk scenarios, and indicative control measures. Compliance risks related to legal, regulatory, and standard requirements including but not limited to:

Risk Category	Description	Examples of Risk Exposure	Potential Impact	Indicative Mitigation / Control Measures
Legal & Compliance Risk	Risks arising from non-compliance with applicable laws, regulations, and trustea standard requirements	Non-compliance with labour laws, environmental regulations, statutory violations by partners	Legal penalties, loss of credibility, scheme liability	Prequalification checks, legal compliance verification, periodic audits, mandatory adherence to trustea standards
Reputational Risk	Risks that may damage the credibility and public trust in the trustea scheme due to association with partners	Association with entities involved in unethical practices, media exposure of non-compliance	Loss of stakeholder confidence, reduced market acceptance	Partner due diligence, grievance redressal, transparent communication, suspension/termination provisions
Operational Risk	Risks affecting the effective implementation of certification, assurance, and scheme processes	Poor audit quality, inconsistency in certification decisions, inadequate monitoring	Compromised scheme integrity, inconsistency in outcomes	CB accreditation criteria, witness audits, audit reviews, defined protocols and SOPs
Fraud & Integrity Risk	Risks related to fraudulent activities, misrepresentation, falsification of records, or unethical conduct	Fake audit reports, manipulation of traceability data, false claims of certification	Loss of trust, invalid certification outcomes, systemic failure	Strict contractual clauses, audit verification, traceability checks, investigation and sanctions

Conflict of Interest Risk	Risks arising when partners or stakeholders have competing interests that may compromise impartiality	CB auditing its own consultancy client, financial influence on certification decisions	Bias in certification, reduced impartiality	Conflict of interest declarations, separation of roles, oversight mechanisms
Data Integrity & Traceability Risk	Risks related to inaccurate, incomplete, or manipulated data within the system	Incorrect farm data, traceability gaps, unverified sourcing	Breakdown in traceability, credibility issues	Digital traceability systems, data validation, periodic checks, audit verification
Information Technology (IT) & Cybersecurity Risk	Risks related to failure, misuse, or breach of IT systems and data infrastructure	Data breaches, unauthorised system access, system downtime, cyber-attacks	Loss of sensitive data, operational disruption, reputational damage	Secure database systems, access controls, data backup, system monitoring, restricted user roles
Partner Performance Risk	Risks arising from inadequate performance or capability of partners	CBs not meeting audit quality requirements, vendors failing service delivery	Ineffective implementation, inconsistent results	Performance monitoring, periodic evaluation, contractual obligations, corrective actions
Financial & Funding Risk	Risks related to funding sources, financial risk in tea business, misalignment with funders expectation and their sustainability goals	Funding from entities with conflicting interests, financial instability of Tea business reduces certification requirements	Reputational damage, operational disruption,	Due diligence of funders requirements, transparency in funding sources, governance oversight for impartiality
Ethical & Human Rights Risk	Risks related to violations of ethical standards, labour rights, and human rights principles	Child labour, forced labour, discrimination, unsafe working conditions	Severe reputational and compliance impact	trustea standard requirements, zero-tolerance criteria, audits, grievance mechanisms
Stakeholder Engagement Risk	Risks arising from inadequate or biased stakeholder consultation or communication	Exclusion of key stakeholders, lack of feedback integration	Reduced legitimacy, non-aligned standards	Structured stakeholder engagement process, public consultations, feedback systems

Strategic Risk	Risks affecting long-term relevance and effectiveness of the scheme	Outdated standards, misalignment with industry or regulatory changes	Reduced adoption, loss of competitiveness	Periodic review (5-year cycle), MEL inputs, continuous improvement mechanisms
Environmental & Sustainability Risk at certification level	Risks related to failure in achieving intended environmental outcomes	Poor waste management, excessive chemical usage, climate risks	Negative environmental impact, non-achievement of ToC	Environmental criteria in standard, audits, monitoring, evaluation, learning and reporting

8. PARTNER RISK ASSESSMENT APPROACH

STEPSINTHE ERM PROCESS: Five Steps in the ERM process

These five steps will be performed by the RMC in a consultative manner

Step 1: Establish the Context:
The purpose of establishing the context is to set the stage for risk identification. Since "risk" is defined as "any issue (positive or negative) that may impact an organization's ability to achieve its objectives," defining the organization's objectives is a prerequisite to identifying risk.This involves understanding the organisation's objectives, and defining internal activities (e.g., code management, compliance assessments, appeals process, payments and fund allocation, data management etc.) and external environment (e.g., laws, competition, social, economic, technological, reputation etc.) within which Foundation operates.

Step 2: Identify and Measure Risks:
The purpose of this step is to develop an understanding of the risk or opportunity in order to have informed evaluation and decision of whether a response is required. Generate a comprehensive list of threats and opportunities based on those events that might enhance, prevent, degrade, accelerate or delay the achievement of objectives; and identify its sources, causes and potential consequences. Comprehend the nature of the risk or opportunity and determine the level of risk exposure in terms of likelihood and impact using Table 2 Risk Register below as a guide.

Table 2: Trustea Sustainable Tea Foundation Risk Register

									Trustea										
No.	Nature of Risk	Risk Category	Probability of Occurrence 1-5	Severity 1-5	Risk factor	Target Risk Fac	Risk Gap	Risk Treatment	Existing Controls (EC)/Strategy	Revised Probability	Revised Severity	Current Risk	Acceptable/ Not Accepta	Additional Controls Required (Optional in case of revised risk score is acceptable)	Responsibilities for Controls	Schedule for Contr	Performance Indicator	M&E Responsibilities	M&E Schedule	Threat Review Sched
1	Organisation not able to retain personnel	Operational	4	3	12	9	3	Mitigate	Perfomance Based compensation	2	3	6	Acceptable	Review compensation and benefits based on market.Create a policy document on employee retention strategy and seek council approval	Director		Retention rate	Director	Annual	Annual
2	Employee risk-disgruntled employees	Operational	2	4	8	9	-1	Accept	Employee manual					Create a mutually employee separation plan, as when separation arises.	Director		Agreed separation settlement document	Director	Annual	Annual
3	Ineffective service delivery to stakeholders	Operational	3	3	9	9	0	Mitigate	Internal monthly review, Monthly Ops	2	3	6	Accepted	Not required	Program Manager		Stakeholder feedback	AM Operation	Annual	Annual
4	Lack of capability of staff to manage unforeseen risks	Operational	3	4	12	9	3	Mitigate	To manage case by case	2	4	8	Acceptable	Formalise through Risk Management Plan with defined procedure	Program Manager		Risk Event log	Code Manager	Annual	Annual
5	Lack of monitoring and reporting of programme outcomes resulting in inability to achieve programme objectives	Operational	2	4	8	9	-1	Accept	Monthly Council meeting reviews			0			Director			Director	Annual	Annual
6	Program goals not in alignment with key stakeholder expectations	Operational	2	4	8	9	-1	Accept	Monthly Council meeting			0			Director			Director	Annual	Annual

Step 3. Determine Risks Response and Action:

The purpose of the risk response and action step is to decide, based on the results of measuring risks, which risks and opportunities require a response and what your recommended response will be.

a. Opportunity response (treatment): Process to modify or respond to an opportunity. Opportunity response can involve one or a combination of: enhancement, exploitation, ignoring, or sharing.

- **Enhance -** The opportunity equivalent of "mitigating" a risk is to enhance the opportunity. Enhancing seeks to increase the probability and/or the impact of the opportunity in order to maximize the benefit to the organization

- **Exploit-** Parallels the "avoid" response, where the general approach is to eliminate uncertainty. For opportunities, the "exploit" strategy seeks to make the opportunity definitely happen. Aggressive measures are taken which seek to ensure that the benefits from this opportunity are realized by the organisation.

- **Ignore-** just as the "accept" strategy takes no active measures to deal with a residual risk, opportunities can be ignored, adopting a reactive approach without taking explicit actions.

- **Sharing -** the "transfer" strategy for opportunities seeks a partner able to manage the opportunity who can maximize the chance of it happening and/or increase the potential benefits. This will involve sharing any upside in the same way as risks transfer involves passing penalties.

b. Risk response (treatment)

Process to modify or respond to a risk. Risks response can involve one or a combination of: accept, avoid, mitigate or transfer.

- **Accept** - If the risk impact is consistent with the Trustea Foundation's tolerance, the risk may be retained at the current level.
- **Avoid** - If the risk exposure far exceeds the Trustea Foundation's risk tolerance, the Group does not believe it can manage the risk, and the risk is not core to the Group's strategy, then the Group should consider avoiding.
- **Mitigate** - If the risk impact exceeds the Trustea Foundation's tolerance but Executive management is confident that the risk can be reduced to a lower, more acceptable level, risk reduction is an appropriate management strategy
- **Transfer** - If the risk impact is high relative to risk tolerance or the Trustea Foundation cannot believe it can manage the risk on its own but the risk is close to its cored or cannot be avoided, then the organization should consider sharing or transferring the risk to the third parties (e.g., insurance) who have the ability or capacity to accept or manage the risk.

Generally, if the magnitude or severity of the risk under consideration is high, the risk response needs to be strong (mitigate, transfer or avoid). Each risk and related response should be assigned to the manager who is responsible for the area affected by the risk. As part of the response process, management should determine and document what controls are necessary to manage the risk. In case there is any major risk, the risk is to be analyzed, discussed by the RMC and presented to Council as part of Risk Management reporting.

Step 4. Communication of risk and response

The RMC submits the result of the risks analysis to the Trustea Foundation Council at least annually (together with their Annual Budget) or on a Project basis.
The report should contain at minimum as follows:

- Summary of risks and risk scoring;
- Highlight of all that exceed the risk tolerance;
- Timeframe and status of risk management activities or risk responses for each risk;
- Risks that are getting worse, success of treatment plans, and risks that quire additional attention;
- Highlights of any new risks including their risks assessment, risk response and management activities;
- Highlights of untreated risks and risk treatments that are overdue, and their risk owners;
- Emerging risks;
- Summary of exceptions to established policies or limits for key risks.
- Major Risk Event Analysis Form, if any carried out in the reporting period

- Scheme-related unintended effects on producers, workers, communities and market actors shall also be considered during risk assessments.

Step 5. Monitor effectiveness of risk responses

Risks and risk response activities will be monitored by the responsible Risk Owners to ensure that significant risk remain within acceptable risk levels, that emerging risks are identified, and that risk response and control activities are effective and appropriate.

trustea adopts a differentiated risk assessment approach based on the category of partner, recognising that each category presents unique risk exposure.

5a. Certification Bodies (CBs)

Certification Bodies are subject to a formal accreditation and enrolment process, which includes assessment of accreditation status, technical competence, organisational capacity, and legal compliance. Their performance is continuously monitored through witness audits, audit report reviews, and periodic evaluations. Non-compliance, fraudulent behaviour, or breach of agreement may result in suspension, scope reduction, or termination.

5b. Certified Entities

Certified entities are assessed through prequalification and certification audits prior to entry into the scheme. Continuous monitoring is carried out through surveillance audits, non-conformity tracking, and traceability verification. Where risks are identified, corrective actions are mandated, and in cases of severe non-compliance or zero-tolerance violations, suspension or decertification is enforced.

5c. Vendors and Service Providers

Vendors and service providers are evaluated prior to engagement through due diligence processes, including legal compliance verification, contractual agreements, and adherence to responsible business practices. Their performance is monitored throughout the contract period to ensure compliance with agreed terms and ethical standards.

5d. Funders

trustea recognises that association with funders may expose the scheme to reputational, ethical, and conflict-of-interest risks. Therefore, due diligence is undertaken prior to engagement to assess alignment with trustea's sustainability objectives, ethical standards, and governance principles. Any potential risks related to undue influence, misalignment of objectives, or reputational concerns are evaluated and managed through appropriate safeguards, including transparency, governance oversight, and defined engagement terms.

9. RISK IDENTIFICATION AND MONITORING

Risk identification is a continuous process embedded within *trustea*'s operational systems. Risks are identified through multiple channels, including audit findings, non-conformities, witness assessments, grievance and complaints mechanisms, stakeholder feedback, and internal monitoring systems.

In addition, inputs from data management systems, traceability platforms, and IT infrastructure are used to identify risks related to data integrity, cybersecurity, and system reliability.

All identified risks are documented, assessed, and periodically reviewed to ensure timely mitigation.

10. RISK MITIGATION AND CONTROL MEASURES

trustea adopts a proportionate approach to risk mitigation based on the severity and likelihood of identified risks. Mitigation measures may include requiring corrective actions, increasing oversight and monitoring, restricting or suspending activities, or terminating partnerships where necessary.

For IT-related risks, appropriate controls are implemented to ensure data security, restricted access, system backups, and protection against unauthorised use or data breaches.

In cases involving fraudulent or unethical behaviour, strict actions are taken in accordance with contractual provisions and scheme requirements.

11. DATA MANAGEMENT AND CONFIDENTIALITY

trustea is committed to maintaining high standards of data management, confidentiality, and transparency. All partners are required to ensure proper handling of data, including secure storage, controlled access, and sharing of relevant information with trustea as required.

The *trustea* database management system serves as the central platform for certification data, audit records, and traceability information. Certification Bodies and other implementing partners are required to maintain accurate and timely data within this system.

Confidential information is protected in accordance with contractual agreements, while ensuring that necessary data is accessible for oversight, monitoring, and assurance purposes.

12. INTEGRATION WITH ORGANISATIONAL RISK MANAGEMENT

This policy is fully integrated with *trustea*'s overall risk management framework, including the Risk Assessment SOP and Risk Treatment Plan. Partner-related risks and operational risks are incorporated into the organisation's risk registers and are subject to periodic review.

Inputs from audits, stakeholder engagement, monitoring and evaluation systems, and risk assessments are collectively used to update and strengthen the risk management approach.

In addition, trustea shall review sustainability-related risks and opportunities emerging from the ERM process to assess implications for sustainability outcomes, impacts, code relevance, MEL priorities and strategic planning within the tea sector.

13. GOVERNANCE AND RESPONSIBILITY

Oversight of risk management is provided by the *trustea* Council, which ensures that appropriate systems and controls are in place. The Secretariat and Technical Team are responsible for implementing this policy, conducting risk assessments, and monitoring compliance.

All partners, including Certification Bodies, certified entities, vendors, and funders, are responsible for complying with the requirements set out in this policy and associated agreements.

14. REVIEW AND CONTINUOUS IMPROVEMENT

This policy shall be reviewed periodically, at least once every five years, or earlier if required due to emerging risks, changes in the operational environment, or updates in international best practices.

Continuous improvement is ensured through feedback from stakeholders, audit findings, and lessons learned from implementation.

12. RIGHT TO REFUSE OR TERMINATE ASSOCIATION

trustea reserves the right to refuse, suspend, or terminate association with any partner whose actions are found to be inconsistent with the scheme's objectives, integrity, or sustainability principles.

Annex: Mapping to Existing *trustea* Systems (Summary Statement)

The provisions of this policy are operationalised through existing trustea systems, including the Risk Assessment SOP, Table 2 Risk Register, IT Risk Assessment SOP, IT Risk Treatment Plan Procedure, System Assurance Protocol – Part 1 & Part 2, Certification Procedures, Responsible Sourcing Policy, and grievance mechanisms. Together, these systems ensure that risks associated with partners and operations are systematically identified, assessed, and managed in alignment with the requirements of ISEAL Codes of Good Practice.

REVIEW RESULT:	REVIEWED BY: Anandita Ray Mukherjee
Document Reference - tSTF RMP02	ISSUE DATE: March 2021
Revision Date: Jan 2022	APPROVED BY: Rajesh Bhuyan
Revision Date: Jan 2023	REVISION NO.: 2
Revision Date: Jan 2026	REVISION NO.: 3
Next Review Date: Within 5 years of approval	