Trustea Sustainable Tea Foundation

tSTF RMP02

ENTERPRISE RISK MANAGEMENT (ERM) POLICY

SECTION 1.

PURPOSE

This Policy establishes the standards, processes and accountability structure to identify, assess, prioritize and manage key risk exposures ofthe Trustea Sustainable Tea Foundation (hereinafter referred to as "Trustea Foundation"). The Enterprise Risk Management (ERM) process will enable trustea Foundation to systematically evaluate implications of decisions and actions to the highest priority goals and objectives, and effectively manage a broad array of risks in an informed and strategic manner to within an acceptable tolerance level.

SECTION 2.

SCOPE

This Policy applies to all operational areas including plans, activities, business processes, assurance system, policies, procedures and employees that comprise the trustea Foundation.

SECTION 3.

POLICY STATEMENT

The Trustea Sustainable Tea Foundation engages in a wide range of activities, all of which give rise to some level of risks. It is the policy of the trustea Foundation to:

1. Embed risk management into the culture and operations

2. Integrate ERM into strategic planning, activity planning, performance management and resource allocation decisions

3. Manage risk and leverage opportunities in accordance with best practices

4. Regularly re-assess the risk profile and the effectiveness of risk response in the context of the various strategic plans

5. Anticipate and respond to changing social, technological, environmental, government and other applicable requirements.

SECTION 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.

RiskEffect 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.

Trustea Sustainable Tea Foundation

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.

SECTION 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

Trustea Sustainable Tea Foundation

SECTION 6.

ROLES AND RESPONSIBILITIES

Trustea Foundationhas established the framework of responsibilities and actions whichare 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

The Risk Management Committee

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

1. Director
2. Assurance SystemManager
3. ITProject Manager

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.

SECTION 7. COMPONENTS OF ENTERPRISE RISK MANAGEMENT

The Trustea Foundation's Enterprise Risk Management framework is made up of six process components. Objectives are set by the Trustea Council and the Executive Management and are cascaded throughout the organization.

1) Event Identification:

The Trustea Foundation will endeavour to identify internal and external events that may affect the achievement of the Foundation's objectives. It should be inclusive and draw as much as possible on unbiased independent sources, including the perspective of important stakeholders.

2) Risk Assessment:

A systematic process used to quantify or qualify the level of risk associated with a specific threat or event, to determine how they should be managed. The main purpose is to help the organization to prioritize the most important risks as the organization is not expected to have the capacity to deal with all risks in an equal manner.

3) Risk Response:

A response is determined based upon the overall risk exposure or opportunity, considered as a function of likelihood and impact of the occurrence. Risk or Opportunity responses may include avoiding or enhancing, accepting or ignoring, mitigating, exploiting, and sharing or transferring risk. Responding to risks involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option. The management should develop response strategies for all material risks.

4) Control Activities:

Controls activities are established to ensure that risk or opportunity responses are carried out effectively and consistently throughout the organization. This involves formalizing risk response in organization policies, ensuring clear accountability, utilizing selfassessment and monitoring tools and designing controls into our systems and critical business process. Everyone in the organization should have responsibilities for maintaining effective systems of internal controls, consistent with their delegated authority. Internal controls include:

a) Preventive controls

b) Detective controls

c) Corrective controls

d) Management controls

e) Administrative controls

f) Accounting controls

g) Information technology controls

5) Information & Communication:

Information and communication channels are to be put in place to make the organization aware of risks that fall into their area of responsibility and expected behavior and actions to mitigate negative outcome. The organization's risk communication and reporting process should support enhanced decision making and accountability through:

• Dissemination of relevant, timely, accurate and complete information; and

• Communication responsibilities and action.

6) Monitoring

The Management reviewsare to be put in place to ensure that risks are effectively identified and assessed, and that appropriate responses, controls and preventive actions are in place. Monitoring should be affected through ongoing activities or separate evaluations to ascertain whether risk management is effectively practiced at all levels and across the organization in accordance with this Policy, strategy and plan. Monitoring activities should focus on evaluating whether:

a. Allocated responsibilities are being executed effectively;

b. Response strategies are producing the desired result of mitigating risks or exploiting opportunities; and

c. A positive correlation exists between improvements in the system of risk management and organization performance.

While no risk management system can ever be absolutely complete, the goal is to make certain that identified risks are managed within acceptable levels.

SECTION 8. RISKS CATEGORIES

Risks to the of the Trustea Foundation will be grouped in categories, as indicated in Table No.1 as below:

Table No.1: Risks Categories

Category of risk	Description
Regulatory Compliance	Risks of litigation, fines, penalties and regulatory non compliance
Financial	Risks associated with transactions, financial systems, structures and reporting, fraud, management of funds, tax liabilities
Information Technology risk	Risk related to the reliability of information and information services. Includes risks associated with an organization's use of technology, physical access protection through the ability to trace actions and transactions to responsible individuals; and from automatic edits to reasonability analyses for large bodies of data.
Assurance System Risk	Risk related to operational and compliance issues of the Assurance System which will impact the assurance system
Operational/program risk	Operational/program risk results from poor service delivery, reoccurring day to day crisis, staffing issues, program failure where the outcome is detrimental to the organization.
Reputational	Risks related to the potential for negative publicity, public perception or uncontrollable events to have an adverse impact on a company's reputation, thereby affecting its revenue.

Trustea Sustainable Tea Foundation

Section 9. 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 below as a guide.

Trustea Sustainable Tea Foundation

Table No.2: Risk Register

Table 2 Risk register

Trustea

No.	Nature of Risk	Category	Probability of Occurrence 1-5	Severity 1-5	Risk factor	Target Risk Factor	Risk Gap	Existing Controls (EC)	Additional Controls Required	Responsibilities for Controls	Sc
					0		0				
1					0		0				
2					0		0				
3					0		0				
4					0		0				
5					0		0				
6					0		0				
7					0		0				
8					0		0				
9					0		0				
10					0		0				

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'srisk 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 as per the Form No 1,Major Risk Event Analysis Form, discussed by the RMCand presented to Council as part of Risk Management reporting.

Form No 1:

Major Risk Event Response Analysis Form

Created By: **Date:**

Date of risk event

Reported by/source/observation:

Category of risk

Action defined in Risk register?

If yes, was the impact in line with risk management plan?

Is there a need to do CAPA based on the risk impact?

If yes, by whom and when?

If no, has the risk been proposed for inclusion in Risk Register with analysis?

Reporting to Council-

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 require 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(Form No 1), if any carried out in the reporting period

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.

SECTION 10. RISK MANAGEMENT REQUIREMENTS

10.1 RMC is accountable for managing risks and must maintain a risk register relating to material risk exposures of the Trustea Foundation

10.2 Risk registers should be based on the outcomes of thorough risk identification and assessment processes and in accordance with this Policy;

10.3 Review of risk registers are to be conducted at least annually or depends on business requirements, and reporting and escalations should occur in accordance with this Policy;

101.4 The RMC should develop its own risk tolerance and submit to the Trustea Foundation Council for approval

10.5 Any changes to the risk rating/scoring due to business nature/complexity are subject to the Trustea Foundation Council's approval.

SECTION 11. ERM INTEGRATION

Risk management is part of the Trustea Foundation's strategy to promote accountability through good governance and robust business practices, which contributes to our strategic objective. In this regard the Trustea Foundation shall incorporate these practices into its governance, planning, reporting, performance review, and improvement processes. In order to integrate the ERM process in the activities, this policy requires that the following activities shall indicate the risk related review.

a. Annual Corporate/Budget Plan including Strategic/Business Plan

b. Project Plan / Proposal

c. Tax and Legal Management

d. Contracts

h. Policies and procedures

SECTION 14. REPORTING

An annual risk management report will be presented to the Trustea Foundation Council meeting as per the format in Annexure 3 of this policy, will be presented to the Council for consideration and feedback, if any,

SECTION 15. REVIEW – the risk management Policy and statement will be reviewed at least once a year or in case of any change any risk situation.

SECTION 16. EFFECTIVITY This Policy shall take effect immediately from the record date of issue.

Trustea Sustainable Tea Foundation

Reference Documents:

- ISO 31000:2018 - Risk management – Guidelines
- Assurance Guidance Note: Building a Risk Management Plan ISEAL Alliance | July 2018

Forms:

1. Table No2: Trustea Sustainable Tea Foundation Risk Register
2. Form No 1: Major Risk Event Analysis Form
3. Annual risk report format

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