Risk Management Plan: The U.S. Cotton Trust Protocol

Version 0.1 - May 2025

Contents

The organizational assurance team uses risk management as the basis for Trust Protocol development and assurance system management activities. This risk management plan helps focus program activities, policy development, and assurance performance monitoring using a risk-based approach. The growth and evolving operational and market context for the Trust Protocol requires the team to prioritize the type and intensity of program development efforts and assurance performance monitoring activities to effectively and efficiently utilize resources to uphold the integrity of the Trust Protocol Principles and Criteria.

The risk management plan uses ISEAL Alliance guidance as its basis and was developed to ensure that a robust, consistent, and data-driven risk identification, analysis, and treatment process guides the Trust Protocol's team's risk management activities over time. This plan describes the risk management approach taken by the team which is operationalized through periodic review and updating of the organizational risk register. The risk management approach is reviewed through the program's annual organizational assurance management reviews. Verification program risks are reviewed and updated regularly, at a minimum quarterly, by team leads from Trust Protocol departments that identify operational and other risks using the risk register.

Section A - Overview

A1. Implementation and References

A1.1 This plan is used by the Trust Protocol team to support the understanding and ongoing execution of the Trust Protocol risk management approach. It includes reference to relevant roles and responsibilities of team members to ensure that organizational risk management is conducted effectively and consistently through regular review and updates to the organizational risk register. The register can be found in the following Sharepoint folder: Standard > Current Materials [link]

A1.2 The plan includes an internal process to identify, analyze, and treat top risks to program integrity using a risk register as the core management tool. Decisions on risk monitoring effectiveness, and investments in risk analysis and treatment will be reviewed on a quarterly basis by a risk management team composed of team leads from Trust Protocol departments.

A1.3 Note that this plan was created to align with the U.S. Cotton Trust Protocol Issues Preparedness and Risk Management Plan [link]. That plan is aimed at addressing acute risks that may compromise the reputation of the Trust Protocol. This plan will be updated periodically to reflect any updates that are needed based on learning and experience implementing the U.S. Cotton Trust Protocol Issues Preparedness and Risk Management Plan.

A2. Terms and Definitions

Refer to the Trust Protocol Terms and Definitions for definitions of terms used in the verification program. Defined terms are shown in italics in their first use in this document and further in the document for clarity.

Terms specific to risk management and use of the risk register are included in the organizational risk register [link] (see Terms and Definitions tab).

A3. Reference Documents

A3.1 The following key documents are relevant to the risk management plan and they are used alongside this document to execute and update the plan:

NOTE: This is not an exhaustive list.

A3.1.1 ISEAL Alliance guidance note Developing a Risk Management Plan for Assurance (2018)

A3.1.2 U.S. Cotton Trust Protocol Issues Preparedness and Risk Management Plan

A3.1.3 Protocol organizational risk register [link]

A3.1.4 Risk management team roles and responsibilities register

A3.1.5 Trust Protocol Verification Program Issues Log (within the risk register)

Section B - Assurance system risk context and narrative

The first step in understanding and monitoring Trust Protocol program risks is to describe the risk context. This includes describing program opportunities and challenges and determining which of these represent risks to system integrity. The context narrative should be updated as needed, typically annually, and used as a starting point for quarterly reviews of system risks.

Additional steps to building a risk management plan are indicated below and related sections for each step are included in this plan.

B1. Verification program risk context

This section outlines the risk context for the verification program as of the publication date of this document. This summary can provide general context for the risk management team or other Protocol team members to understand the general landscape of risks impacting Trust Protocol verification program integrity. The summary is helpful for understanding which risks can be mitigated or treated through standard or verification process requirements, policies, communications, and engagements with Trust Protocol stakeholders.

Any Trust Protocol team members that contribute to risk management reviews shall review this summary before using the risk register or supporting any risk management decision-making process such as in periodic risk register review and annual system management reviews. This ensures that the risk register is calibrated regularly through updates that reflect the current context of risks in the evolving global cotton and textiles industries and sustainability landscape.

B2. Trust Protocol program risk narrative (top program risks)

The Trust Protocol's verification program development is anchored in the Standards & Assurance team's development of the Trust Protocol Principles and Criteria which represent the program's voluntary sustainability standard. The team develops the policies, requirements, and procedures to support execution of the verification process and ensure the high integrity of the Principles and Criteria (standard) according to ISEAL best practices.

This version of the risk management plan is the Trust Protocol's first effort to document the verification program's risk management approach. The risk management plan is the core system that anchors and helps prioritize Standards & Assurance and other teams' strategies, activities, and resources. This approach is essential given the operational context and integrity risks currently being considered by the program in the U.S. and global cotton industries, as well as the limited resources of the team to effectively manage a growing set of stakeholder needs. The scale of the verification program is also expected to grow in order to meet demand for verification to support the organization's sustainability objectives and business model.

Given the broad network of Trust Protocol stakeholders, growing verification demand, and limited staff capacity, the risk management plan will initially (in 2025) focus on analysis and treatment of the top, most visible risks for the program such as low or no price premiums for U.S. cotton in the global cotton market, emerging or maturing integrity best practices according to ISEAL, and relatively low proportion of demand for U.S. cotton among other sustainable cotton inputs or material inputs in textile value chains.

The success of the risk management plan will depend on internal diligence in consistently adhering to risk management procedures including recording program-level operational concerns and performance, in addition to information on stakeholder engagement signals provided from internal teams. This data-driven approach will enable the team to use a risk-based approach in focusing its limited resources more efficiently in functions such as determining ISEAL integrity best practice focus areas across the organization, identifying operational assurance performance indicators, and refining a centralized stakeholder engagement plan to build effective and integrated verification program operations activities.

B2.1 Top verification program risks (May 2025):

B2.1.1 Low or no price premiums for U.S. cotton in the global cotton market, leading to limited direct value for Protocol growers from engaging with the program.

B2.1.2 Emerging or maturing integrity best practices according to ISEAL leading to vulnerabilities in verification program operations:

- governance structure presenting conflicts of interest in program management and implementation
- lack of a self-sustaining fee-based business model for the verification program
- still emerging or maturing implementation of 2nd and 3rd party assessment requirements under possible scrutiny by external stakeholders and regulatory bodies

- low adoption of ISO-based auditing practices (e.g. documented assurance service contracts, verification assessment score, corrective action plans, verification certificates)

B2.1.3 Potential for a relatively low proportion of demand for U.S. cotton among other sustainable cotton inputs or materials, which could lead to challenges in encouraging stakeholders to invest in the Trust Protocol supply chain and traceability process for only relatively low cotton volumes in their supply chains.

B2.1.4 Organizational assurance process and policy gaps that reinforce operational silos among teams, leading to a lack of coordination among teams and inefficiencies in daily program operations (e.g. normative document development and control, project management)

Section C - Risk Assessment Using the Risk Register

The organizational risk register is the primary tool used by the Trust Protocol team to record, quantify, monitor, and treat verification program risks. This register is reviewed on a quarterly basis at the least, and more frequently when critical risks to program integrity or organizational reputation arise. The register is a helpful tool that indicates the date a risk was identified, a description of the risk, and the risk criticality level. The risk register includes a range of terminology and tools such as a risk level matrix to support its interpretation and consistent use. Risk treatment actions and results of risk treatment are also recorded in the matrix.

An effective risk register should be updated on an established periodic basis and have clear roles and responsibilities related to it for risk management team members so that the register remains updated and accurately reflects organizational risks. It should be a trusted resource and reference when a critical risk arises or when the integrity of the program is put under scrutiny. When these situations occur, the Trust Protocol team should be able to rely on the register to find current information regarding the specific risk or determine if the risk has been previously identified.

One individual is responsible for ensuring the risk register is used effectively, is updated to meet the information needs of the team, and follows a consistent and clear process for updating it.

The risk register is owned by the Assurance Lead. Other team members as described in the Section C2 may access and update the register by adding or modifying information on organizational and verification program risks.

C1. Criteria for using the risk register to record and monitor risks

The organizational risk register should record the set of risks that pose a threat to the integrity and operations of the verification program and the Trust Protocol organization more widely. We understand that many issues and operational challenges could be classified as risks but must take care not to record all of these issues in the risk register as 'risks' since we cannot treat all of the issues that arise. As a general approach, if an issue is incidental, i.e. pertains a one-off incident, or if there is already an existing process to handle the type of issue, it does not need to be elevated to the risk register but can be logged in the Issues Log within the register. If it is an issue that points to a systemic operational issue

or indicative of a larger problem, and/or if there is no existing process to handle the type of issue, it should be logged as a risk. The designated team members responsible for logging issues should consult with the Assurance Lead if unsure about whether to log an issue/risk in the register. The 'Issues Log' tab in the risk register can be used to log issues that arise. The Issues Log would be revised at least once quarterly to determine if any issues should be elevated and logged as risks in the risk register.

When an issue or risk is identified, the below steps should be taken to determine if the issue/risk will be classified as a risk to be added to the risk register and treated through additional dialogue, analysis, and decisions to treat the risk in specific ways that will be monitored over time. All issues shall be added to the Issues Log for monitoring and possible addition to the risk register in the future.

Use of the risk register to record risk information is for the Assurance Lead or Trust Protocol team leads. Trust Protocol team leads will only record risks in the register when the following steps have been completed. Only assigned team members can add information directly in the risk register (see Section C3):

C1.1 Steps for team leads to complete before adding information to the risk register:

C1.1.1 Complete risk management training (including guidance on use of the Issues Log). Contact the Sustainability Implementation Manager to coordinate a brief training.

C1.1.2 Identify the name of the team lead that would record inputs regarding the identified risk using the risk management roles and responsibilities RACI. Team lead discusses the risk with his/her respective team if needed, before recording inputs in the register.

C1.1.3 Team lead records the risk information as completely as possible in the relevant row of the register. Ask the Assurance Lead if you have any questions.

C2. Critical Risk Matrix: Roles and responsibilities

A critical risk matrix was developed to enable coordinated action on critical risks that may arise for the Trust Protocol which are related to verification program integrity or operations. These could include risks such as a public integrity complaint regarding the verification program, a complaint by a company regarding Trust Protocol services, or allegations from media sources regarding violations of our standard.

The critical risk matrix is a subset of catastrophic or critical risks in the organizational risk register with additional detail on risk treatment and short-term follow-up. The critical risk matrix is owned by the Executive Director and the Head of Communications & Marketing.

The critical risk matrix is a separate document from the risk register although it has similar information to the risk register. This is due to the access rights needed for other Protocol team members to address critical risks in shorter time periods. The matrix is updated on a periodic basis by its owner to provide the broader team additional detail within short periods of time regarding top risks. The information in the matrix enables Protocol teams to plan for rapid risk mitigation and treatment actions while also supporting transparency regarding risk treatment and communications to affected stakeholders.

To access the critical risk matrix, please contact the Head of Communications & Marketing.

C3. Organizational Risk Register: Roles and Responsibilities

The information contained in the risk register forms the basis for risk treatment actions for each risk or the top risks, as resources allow. The risk treatment actions identified may inform resource intensity for different organizational or verification program oversight activities, audits, and other investments such as in policy or program development or changes. **Given the importance of the register for management decision-making, the register must be carefully and consistently managed so that the information within the registry can be trusted to be accurate, relevant, and clear**. Maintaining a current and trusted register is also important because the information therein triggers data-related and risk treatment activities such as data collection and reporting on specific risks. This data-related activity carries a cost, requiring additional resources of staff time and expertise.

As a result of its importance for decision-making, the register shall be updated regularly as risks are identified, and at least on a quarterly basis to be a helpful tool for certification system management decision-making. Updating the details of risk identification, treatment, and follow-up for each risk in the matrix requires a consistent, detail-oriented approach and clear language using program and process terminology.

A set of roles and responsibilities has been developed for risk register updating and ongoing maintenance and decision-making. These roles and responsibilities are outlined below.

C3.1 Using the risk register according to your role:

C3.1.1 General: In the risk management roles and responsibilities RACI ('Risk Management RACI' tab in the risk register), each team member can find their name and relevant role(s) in contributing to, updating, or making decisions relevant to organizational risks.

C3.1.2 Team leads contributing information to the risk register will maintain awareness of the risk management process and consider risk management in the daily operations of their team. The team's intelligence regarding risks will often emerge in our team meetings, internal communications, or engagements with assurance system stakeholders. The team lead should bring awareness to his/her team regarding the risk register and issues log.

C3.1.3 Recording inputs in the register: All team leads can contribute to dialogues regarding organizational and verification program risks, and also record risks in the register to ensure consistency in the register information and appropriate level of detail.

C4. Using the risk register to treat organizational or verification program risks

In addition to identifying and recording risks in the register, the risk management team shall ensure that risks are analyzed and evaluated. This may be done via quarterly meetings of the risk management

team, or other meetings as appropriate. Decisions about how to treat risks are thus mainly the responsibility of the team lead of the respective area most affected by the risk, noting that this may involve interactions or dependencies with other teams or sign off from the leadership team (see C3.1.1 Risk Management RACI). A responsible person is identified as the lead for each of the risk treatment actions recorded in the register. Note that multiple risks could be addressed through the same risk treatment actions, and therefore those actions should be listed next to each risk that it is intended to address.

Section D – Monitoring and review of the risk management plan

D1. Schedule of risk management review activities

This risk management plan and the risk register describe the overall risk management approach for organizational and verification program risk management and decision-making. According to ISEAL Alliance guidance, the risk register should be periodically reviewed and form part of a regular review of the Trust Protocol in the following ways:

- Quarterly risk review: It is important that the risks recorded in the register are reviewed at least on a quarterly basis. During these reviews, the risk register is reviewed by a risk management team (composed of the Trust Protocol team leads) and may include other team members, as needed, to discuss specific top risks.

- Management reviews: The program has annual management reviews to assess the overall functioning and effectiveness of the assurance system. During these reviews, an assessment of the risk management plan is conducted. This assessment includes review of the usefulness of the risk register as a tool for organizational and verification program risk management.

- Extraordinary reviews of the risk register and risk management plan: Significant changes or initiatives that could impact the risk management approach may also trigger review of the risk management plan of the risk register. These may include initiatives such as a change in overall organizational strategy, changes in the assurance model, or a revised Trust Protocol standard.

Schedule of review activities (2025 example):

Activity	Date	Participants	Objective
Q1 Risk register review	***End of March 2025***	Trust Protocol risk team (workstream leads)	Introduction to ISEAL best practice; Review risk context, existing and new risks; review risk treatment actions; ID follow-up
Q2 Risk register review	June 11, 2025	Trust Protocol risk team, after S&A team inputs (asynchronously)	Review risk context, existing and new risks; review risk treatment actions; ID follow-up
Q3 Risk register review	September 10, 2025	Trust Protocol risk team	Review risk context, existing and new risks; review risk treatment actions; ID follow-up
Q4 Risk register review + annual management review	December 10, 2025	Trust Protocol risk team	Year review: Review risk treatment actions; ID follow-up; Assess the overall functioning and effectiveness of the certification system

D2. Quarterly risk management review meeting procedure

The below steps and activities are undertaken during the quarterly reviews of the risk register:

Step	Responsible	Activity	Needs from the team
1.Convene risk management team (pre-scheduled in Outlook at start of the year)	Assurance Lead	Risk review meeting (quarterly)	Set time aside for quarterly risk review with the risk management team
2.Draft and distribute agenda for the risk review meeting	Assurance Lead	Draft focused objectives and list of top discussion topics to address and focus on in the risk register	Prepare for a productive meeting and receive/give inputs from risk team on items for the agenda
3.Complete risk review meeting	Assurance Lead	One-hour sessions (normally) to review the risk register and risk treatment strategy and actions.	Review risk context, existing and new risks; review risk treatment actions; Identify follow-up
4.Summarize findings from the risk review meeting (quarterly)	Assurance Lead, Sustainability Implementation Manager	Draft one-page summary from the meeting as a record of topics discussed and decisions taken to share with other teams; include revised top 5 risks	For record and broader team: Bring awareness and visibility to risk context and actions to treat existing risks
5. Bring inputs from risk review meetings to the assurance management reviews (annual, scheduled in Outlook at start of the year)	Assurance Lead, Sustainability Implementation Manager	Bring analysis of quarterly summaries from the risk review meetings to use as a basis for insights and improvements to the risk management process	Ensure there is a feedback loop between the risk management approach and overall improvements to the organization
6. Summarize risk management findings and insights for the broader team (as requested)	Assurance Lead, Sustainability Implementation Manager	Add slide to decks in all team presentations or other meeting opportunities; include data and visualizations on risk treatment where possible	Ensure the practice of risk management is visible to the broader team and other teams addressing top risks

*The agenda for risk review meeting can include review of the following:

1. Top risks (critical risk matrix) are reviewed as well as new information on other risks added to the register since the last quarterly review.

2. Discuss current risk identification, analysis, and treatment actions

3. Discuss and refine risk management approach

4. Decide on continued risk treatment actions or adjustments to them, or determine additional analyses or information needed.

5. Identify new risk treatment actions

6. Record specific actions for risk treatment or other risk management follow-up

D3. Risk management in the context of organizational assurance processes

The risk management plan is a central feature of a sustainability system's strategic operations to support effectiveness, efficiency, and address potential threats to its reputation. The team members and information that support risk management decision-making ultimately inform all areas of the organization and program. Since the risk management process sits within the operations team functions, it serves as an information anchor to inform the organization's activities and required coordination of other important functions. These functions include overall strategy, impacts strategy, stakeholder engagement, standard-setting, assurance, claims management, and monitoring and evaluation.

The information managed as part of the risk management process also forms part of the organization's knowledge management function.

For questions about this risk management plan and to propose additions or changes to the plan, please contact the Sustainability Implementation Manager.