ISCC PLUS 204
RISK MANAGEMENT

Version 1.0

ISCC
International Sustainability & Carbon Certification
PLUS

Document Title: ISCC PLUS – 204 RISK MANAGEMENT

Version 1.0

Valid from: 01 July 2025

Content

Table of Abbreviations

Abbreviation	Full Description
APS	Audit Procedure System
CB	Certification Body
GHG	Greenhouse Gasses
ILO	International Labor Organization
ISCC	International Sustainability and Carbon Certification
ISEAL	International Social and Environmental Accreditation and Labelling
LUC	Land Use Change
NGO	Non-Governmental Organization
OECD	Organizations for Economic Co-operation and Development
RED	Renewable Energy Directive

1 Introduction

High quality verification

Clear requirements on how to manage risks in the ISCC PLUS framework are an integral part of ISCC's quality policy. They are key factors for ensuring the integrity, reliability, credibility, and high quality assurance of ISCC.

Risk management process

The principles regarding risk management lay down the general process on how to identify, evaluate and address risks appropriately in the scope of ISCC PLUS and during audits. The risk management principles are applied to ISCC as an organisation, to Certification Bodies (referred to hereafter as CBs), auditors cooperating with ISCC, and ISCC PLUS System Users (referred to hereafter as System Users).

2 Scope and Normative References

Best practice principles

This document outlines the requirements for implementing the risk management process within the ISCC PLUS system. It defines how risk management is applied across all ISCC PLUS activities and highlights the implications of identified risks for ISCC PLUS audits. The risk management process takes into account the best practice principles of the ISEAL "Code of Good Practice for Sustainability Systems" and ISAE 3000 "Assurance Engagements Other than Audits or Reviews of Historical Financial Information" (ISAE 3000 Revised). These requirements are intended to complement the provisions set out in in the ISCC PLUS System Documents. They are applicable to ISCC PLUS, System Users and recognised CBs conducting ISCC PLUS audits.

3 Risk Management

3.1 Definitions and Levels of Application

Definition risk

Within the framework of ISCC, risk is defined as the likelihood of an event occurring that could adversely affect the mission, objectives, or integrity of the ISCC system. Risks are classified based on the probability of the event happening and the potential consequences if it does occur.

Definition risk assessment

Risk assessment is the process of identifying, evaluating, and classifying potential risks. This includes determining both its probability to occur and its potential impact. Risk indicators are quantitative or qualitative variables that help identify potential risks. These risk indicators provide insights into events or situations that may pose threats to ISCC. By analysing the relevant risk indicators for each process, potential contexts of non-conformity with ISCC PLUS requirements can be identified. Once a risk is identified, it must be evaluated for its relevance to the specific situation. The result of the evaluation leads to the classification of the risk. Within the ISCC PLUS audit framework,

risk are evaluated and classified according to a risk level (regular, medium or high) and assigned a corresponding risk factor (1.0, 1.5, or 2.0).

Definition risk management

Risk management is the process of conducting a risk assessment (identification, evaluation and classification of the risk) followed by the identification and implementation of risk control measures to reduce the likelihood and/or mitigate the negative consequences associated with those risks. The risk management process is carried out in the following main steps:

Levels of application

> Identification of risks,
> Evaluation and analysis of the risks,
> Treatment of the risks, and
> Monitoring of risks.

Multi-level risk management

Risk management in the ISCC PLUS system is applied at three different levels: ISCC as the system owner, for CBs cooperating with ISCC, and for System Users being certified under ISCC PLUS. At each level, risk management must be appropriately implemented to ensure effective mitigation measures and to safeguard the integrity of the ISCC PLUS system. The approach is guided by key principles, including proportionality, a risk-based methodology, continuous monitoring, stakeholder engagement, transparency, and adaptability.

3.1.1 ISCC

Continuous monitoring

Risk management is an integral part of all operations and decisions in the ISCC system. ISCC continuously monitors potential risks to the integrity of ISCC through:

> The multi-stakeholder dialogue of ISCC and the ISCC stakeholders, e.g., during Stakeholder Committees and Working Groups.
> Regular meetings with recognised CBs to exchange feedback and practical experiences.
> Continuous feedback from System Users including complaints or reports of non-conformity or alleged fraudulent behaviour.
> The ISCC Integrity Programme.
> A continuous internal review of audit documentation submitted to ISCC.

Stakeholder involvement

If risks to ISCC are identified in specific regions or regarding specific topics, ISCC will engage with relevant stakeholders and may establish a Stakeholder Committee or Working Group to develop appropriate risk control measures. The development of these appropriate risk control measures must be based on a fact-based analysis of the identified risk.

Promotion of risk management tools

Furthermore, ISCC supports the development of new tools and measures to enhance the risk management process. This includes using risk assessment tools, such as remote sensing analysis, to evaluate land use change and other land-related sustainability criteria. Additionally, databases are used to improve the traceability of certified material and the accuracy of related sustainability claims, helping to reduce the risk of fraud.

ISCC Audit Procedure System

The use of the Audit Procedure System (APS) is mandatory for CBs and auditors. APS minimises the risk of human errors and automates the detection of inconsistencies in audit reports. It also streamlines the preparation of the Main Audit Reports and Summary Audit Reports. The use of the conventional audit procedures (in Word format) may only be used in exceptional circumstances (e.g., severe problems with IT components, system breakdowns, etc.) or when new audit procedures have not yet been integrated into APS.

ISCC Integrity Programme

The ISCC Integrity Programme is an important tool for the ongoing identification and analysis of risks to the ISCC System, including the implementation of requirements by System Users and their verification by CBs. Within the ISCC Integrity Programme, ISCC conducts independent Integrity Assessments to evaluate the performance of cooperating CBs, individual auditors, and certified System Users. These Integrity Assessments may take place at the CB´s head office or at the operation sites of System Users. It is also possible to conduct an Integrity Assessment or parts of it remotely. The outcomes of the Integrity Programme form the basis for ISCC's risk management activities and are used to improve the system quality and reduce the risk of non-conformities. See System Document *ISCC PLUS – 102 Governance* for further information.

Internal review

Audit documentation has to be submitted by the CB to ISCC after an audit has been conducted. ISCC internally reviews this documentation as a part of the risk management process. Such internal reviews ensure a consistent application of ISCC and a level playing field for CBs and System Users. See System Documents *ISCC PLUS – 201 System Basics* and *ISCC PLUS – 103 Requirements for Certification Bodies and Auditors* for further information.

3.1.2 Certification Bodies

Risk management procedures

For CBs cooperating with ISCC, risk management focuses both on the CB's internal processes and on the services provided to System Users during ISCC PLUS audits. Internally, CBs should have appropriate risk management procedures in place covering potential risks for the integrity of ISCC PLUS. These procedures must include addressing risks that could arise from the CB´s own actitivites, such as conflict of interest, auditor competence, and quality management. As CBs conduct ISCC PLUS audits for System Users, CBs must also have an internal procedure on how to conduct reliable risk assessments for System Users to be certified.

Risk assessment during audits

Before conducting an ISCC PLUS audit, the CB must conduct a risk assessment for the System User to be certified. The CB must consider the

results of the self-assessment performed by the System User, the design of the System User´s management system, and any measures implemented to address and mitigate the identified risks to the integrity of ISCC PLUS system. The risk assessment must also take into account relevant risk indicators applicable to the System User´s operational context. During this risk assessment, the CB identifies, evaluates and classifies the level of risk according to one of the three ISCC risk categories: regular, medium, high.

Risk identification

Based on their professional judgement and the information provided by the System User, CBs must pay close attention to risks which could lead to a material misstatement[1], such as inaccurate sustainability claims, misreported information, or fraudulent documentation. To enhance the reliability of the risk assessment, CBs may refer to ISCC PLUS documentation and other credible sources. CBs are encouraged to gather country-specific information, including data from NGOs, media reports, or governmental bodies, regarding any social or environmental issues relevant to the region where the audit will take place. The findings from this research must be considered in the identification and evaluation of risks, as well as in the planning and conduction of audits.

Audit intensity and sample size for group certification

The results of the risk assessment directly influence the audit intensity and sample size (in the case of group certification). Higher risk levels call for more detailed and comprehensive audits to ensure conformity with ISCC PLUS requirements. This may include increased document verification and more extensive audit trails (e.g., traceability of transactions flows). In the case of group certification, auditors must audit a sample of the group members (sampling). The sample size of the group members is calculated based on a specific formula that takes into account the risk factor assigned by the CB and the total number of members. For more detailed information, refer to System Document *ISCC PLUS – 203 Traceability and Chain of Custody*.

Risk-based audit planning and adjustment

During audits, the CB must follow a risk-based approach. This involves prioritising areas, processes and products identified as higher risk during the risk assessment, while placing less emphasis on areas assessed as lower risk. When planning the audit, the CB must also consider the results of previous audits. As part of the ongoing audit process and to allow for adaptability, CBs may revise the initially assigned risk level (by either increasing or decreasing the risk level), considering fact-based findings[2] or newly obtained information during the audit planning process.

Participation in ISCC Integrity Programme

Furthermore, cooperating CBs are required to participate in office audits conducted by ISCC as part of the ISCC Integrity Programme. While not mandatory, it is recommended that CBs also take part in Integrity

[1] Aligned with ISAE 3000, a "*material misstatement*" is considered any significant inaccuracy, omission, or misrepresentation in the information provided by the System User that could influence the decisions of stakeholders relying on the certificate. These stakeholders could include regulatory bodies, customers or any other parties who depend on the integrity and accuracy of the certification.

[2] "*Fact-based findings*" refer to conclusions or observations made during an audit that are supported by verifiable evidence. These findings are objective, impartial, and based on concrete data rather than opinions or assumptions.

Assessments of System Users certified by the respective CB. ISCC regularly invites the cooperating CBs to exchange feedback, share practical experiences and discuss potential risks identified during the daily operations of the CBs and of ISCC.

3.1.3 ISCC PLUS System Users

Internal risk management

The risk management at the level of System Users focuses on their internal processes and the risk of non-conformity with the applicable ISCC PLUS requirements and principles outlined in the ISCC PLUS system documents.

Self-assessment

System Users registered for certification under ISCC PLUS must conduct at least once a year an internal risk assessment (self-assessment) to identifiy potential risks of non-conformity and define appropriate control measures to mitigate these risks. The self-assessment should be guided by the principles and risk indicators outlined in subchapter 3.2 of this document. Based on the results of the self-assessment, the System User must design its internal management system in a way that appropriately addresses and minimises the identified risks that its activities may pose to the integrity of ISCC. The results of the self-assessment must be shared with the CB prior to the ISCC PLUS audit.

Integrity Programme

All System Users are required to participate in Integrity Assessments scheduled by ISCC in the framework of the ISCC Integrity Programme. Failure to cooperate with the Integrity Programme is considered a critical non-conformity and will be sanctioned accordingly (see System Document *ISCC PLUS – 102 Governance* for further details).

3.2 Risk Assessment

3.2.1 Identification of Risk

Analysis of risk indicators

The first step in the ISCC PLUS risk assessment process is the identification of potential risks. This is done through the analysis of the risk indicators. The analysis of the risk indicators serve as the foundation for evaluating potential risk to the conformity with ISCC PLUS requirements and to the integrity of ISCC.

Context-specific risk indicators

Risk indicators must be taken into account during all ISCC PLUS audits. They help identify possible non-conformities and must be tailored to reflect the specific set-up of each System User. The scope of risk indicators should cover various types of risks, including those related to specific materials, products, industrial sectors, and sustainability issues. They should also consider geographic areas with heightened exposure to risk, as well as internal risks linked to the operations of the System User, including suppliers and producers. Where necessary, additional indicators should be defined by the CB to ensure a thorough assessment of the individual context.

Remote risk assessment

A risk assessment may be conducted remotely through a desk-based review. If necessary, this remote assessment can be supplemented by on-site verification, also referred to as ‘ground-truthing’. To support a harmonised

approach and ensure a level playing field, ISCC may require System Users and CBs to use specific online tools for defined audit scopes.

Assessment of farms/plantations and forests

When ISCC PLUS audits involve the verification of farms/plantations or forests, a dedicated risk assessment must be conducted. This assessment aims to determine the risk of non-conformity with the ISCC sustainability requirements for agricultural and forest biomass, as outlined in the System Documents *ISCC EU 202-1 Agricultural Biomass: ISCC Principle 1*, *ISCC EU 202-2 Agricultural Biomass: ISCC Principles 2-6*, *ISCC EU 202-3 Forest Biomass: ISCC Principle 1* and *ISCC EU 202-4 Forest Biomass: ISCC Principles 2-6*. Particular attention must be given to the the risk of violations of ISCC Principle 1. This includes determining whether the farm/plantation/forest is located near or within the areas where biomass production is prohibited under ISCC requirements.

Tools for identifying environmental and social risks

The risk of non-conformity of farms/plantations/forests should be assessed using appropriate and reliable sources, such as databases or remote sensing tools. These tools should enable a well-balanced and meaning assessment for the respective region. This may include verifying land use change through satellite imagery, analysing biodiversity information from recognised databases, consulting sources on protected or high conservation value areas and conducting web-based research on relevant social and environmental issues. An example of how satellite data can be used to assess risks for risk assessment of farms/plantations/forests is shown in Figure 1.

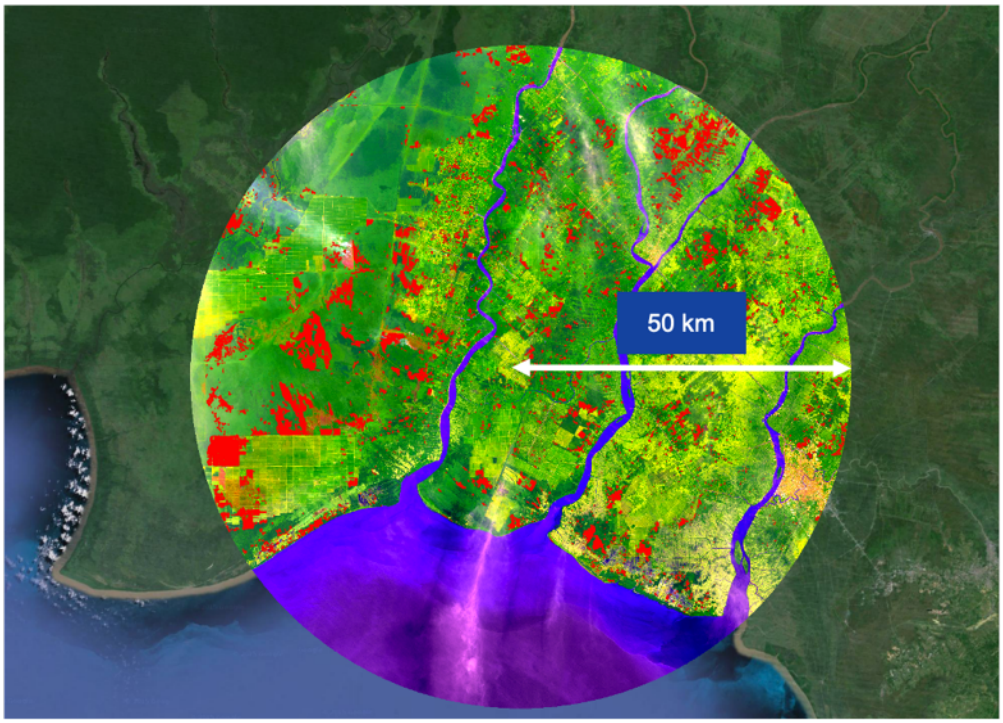

Figure 1: Example of a risk assessment of farms/plantations/forests using satellite data (red areas indicate potential land use change in an area after January 2008)[3]

[3] *Source: GRAS - Global Risk Assessment Services, 2020*

Land use change after January 2008

If, during the risk assessment or audit, it is determined that land use change (LUC) ocurred after January 1st 2008, the CB must provide a detailed explanation to ISCC on how conformity with ISCC Principle 1 was verified. This explanation must include a visual representation of the areas where the LUC took place, the land category of those areas prior to the land conversion and a description of the method used to determine the land category. Additionally, the CB must provide information on the qualifications and expertise of the individual who verified the LUC, whether it was the auditor or another expert appointed by the CB. For further guidance on the qualifications, refer to the System Document *ISCC PLUS 103 – Requirements for Certification Bodies and Auditors.*

Assessment of waste or residues

When ISCC PLUS audits involve waste and residues, the risk assessment must focus on identifying the risk of false claims and the risk of the 'intentional' production of waste and residues, e.g., for the purpose of accessing specific incentives. The assessment should prioritise verification at the Point of Origin to determine whether the material qualifies as a genuine waste or residue in line with ISCC criteria and rules. It must also assess the accuracy and consistency of how the material is classified and declared by both the Point of Origin and the Collecting Point. For further details, refer to System Document *ISCC PLUS 202-5 Waste and Residues*.

Traceability and chain of custody

Traceability and chain of custody are main components of the ISCC PLUS risk assessment for all System Users. The assessment must evaluate whether there are specific risks that non-certified material could be misrepresented, sold, or delivered as ISCC-certified. This includes examining the integrity of documentation, the robustness of internal controls, and the reliability of data management systems used to track certified material throughout the supply chain. Furthermore, it must be verified that the System User fully complies with ISCC PLUS chain of custody requirements, including the proper implementation of the chosen chain of custody option (e.g., mass balance, controlled blending or physical segregation) and the accurate handling of Sustainability Declarations at all relevant stages. For further information, see System Document *ISCC PLUS 203 – Traceability and Chain of Custody*.

GHG emissions

When applicable, the risk assessment must consider whether there is a risk of errors in the calculation of greenhouse gas (GHG) emissions, incorrect use of default values, or false declarations. Any deficiencies in data handling, documentation, or technical knowledge may increase the risk of non-conformity. For detailed requirements and methodologies, refer to *ISCC PLUS Greenhouse Gas Emissions Add-on*.

General risk indicators

In the context of ISCC PLUS risk assessment, some examples of general risk indicators are listed below. The risk assessment should not be limited only to these indicators. ISCC encourages the use of other relevant risk indicators to identify possible risks when the risk assessment is performed by CBs and System Users.

- Determination, structuring, organisation and documentation of the number of workflows and their complexity (in-house processes).
- Number, structuring, organisation, expertise, management, involvement and monitoring of subcontractors and external service providers.
- Number and structuring of the workflows that are carried out by subcontractors compared to the ones that are carried out by permanent in-house staff.
- In-house quality management system, internal audits (structure and documentation).
- Transparency (public reporting, involvement of local interest groups, independent audits, social, environmental and economic aspects of sustainability).
- Mechanisms for conflict resolution established independently, documented and implemented.
- Management of conflicts of interests and prevention of corruption.
- Risk of corruption and fraud (e.g. according to OECD list, Transparency International Corruption Perceptions Index, etc.), i.e. how serious is the external risk of corruption and how does this influence implementation.
- Yield or conversion factors in internal processes, especially if several products with different conversion factors are processed.
- Individual calculation of GHG emissions (if applicable).
- Switch from the use of default values to individual GHG emissions calculation (if applicable).
- In case of group certification: Adding group members (e.g. farms/plantations) to the group for which GHG emissions are calculated individually (if applicable).
- Certification history, including previous or current ISCC certification and certification under other sustainability certification systems, as well as previous failed audits, and withdrawn or suspended certificates under the schemes mentioned above.
- Frequency of changes in certification system (so-called “scheme hopping”).
- Frequency of changes of the CB conducting audits under ISCC (so-called “CB-hopping”).
- Accuracy of records and documents.
- Degree of topicality, frequency of updating records and documents

> Accessibility of records and documents.

> Completeness of records and documents.

> Risk of single consignments (batches) being claimed more than once (so-called “double-accounting or multiple-accounting”).

LUC related risk indicators

Risk indicators for farms/plantations and forest sourcing areas include but are not limited to:

> Proximity to and/or overlap with no-go areas (forest land, peatland, wetlands, highly biodiverse grassland, etc.).

> Land conversion shortly before or after January 1st 2008.

> Production on slopes, fragile or problematic soils (e.g. regarding the avoidance of soil erosion and compaction).

> Factors significantly influencing the output per acreage and the output per hectare (ha).

> Natural vegetation areas within or in close vicinity of the production area.

> Springs and natural watercourses within or in close vicinity of the production area.

> Application of pesticides and fertilizers (e.g. regarding restrictions on the use of plant protection products, soil and water contamination, health and safety, etc.).

> Employment of migrant workers (e.g. regarding forced labour, equal opportunities, etc.).

> Ratification and degree of implementation of ILO core labour standards (Freedom from forced labour, freedom from child labour, freedom from discrimination at work, freedom to form and join a union and to bargain collectively).

Waste/residues related risk indicators

Risk indicators related to waste and residues include but are not limited to:

> Type of Point of Origin (e.g. restaurant, processing plant, landfill, etc.).

> Size of Point of Origin and amount of waste/residue material generated per month (high amounts of waste/residues may indicate a higher risk of non-conformity or fraud).

> Status of the material (genuine waste/residue) and acceptance or recognition by relevant authorities.

> Eligibility for extra incentives for materials in a specific region or country (e.g. double-counting).

> Declaration or labelling of the material (e.g. according to official waste catalogues or waste codes).

> Risk of deliberate or willful ‘production’ of waste or residues.

> Use of feedstocks based on waste/residues and virgin materials.

> Risk of deliberate or willful modification or contamination of products to be declared or claimed as waste or residues.

3.2.2 Evaluation of Risk

Aspects for evaluation and classification

The second step of the risk assessment is to evaluate and classify the identified risk. For the evaluation of the identified risk, the following elements must be taken into consideration:

> The sources and causes of the risk.

> Identification of potential consequences from the risk if it would occur, including the severity of its impact (e.g. negligible, moderate, critical) and the likelihood of its occurrence (e.g. unlikely, occasional, likely).

> Factors that may influence both the impact and the likelihood of the risk.

> Differing stakeholder perspectives regarding the significance or priority of the risk (e.g., a CB might view documentation gaps as a high risk to system integrity, while a System User may perceive them as minor or administrative).

Risk levels and factors

Based on the risk evaluation, the risk is classified according to one of the three risk levels:

> Regular[4] (risk factor 1.0)

> Medium (risk factor 1.5)

> High (risk factor 2.0)

To support the classification process, a risk assessment matrix (See Table 1) may be used as a tool to facilitate consistent and structured risk evaluation.

Consequences	Probability of Occurrence		
	Likely	Occasional	Unlikely
Critical	High	High	Medium
Moderate	Medium	Medium	Regular
Negligible	Medium	Regular	Regular

Table 1: Example of a risk assessment matrix

[4] *The risk level „regular“ has to be applied if the risk assessment conducted by the CB identifies a low risk for the auditee.*

ISCC sustainability principles

With respect to the evaluation of the risk on farm/plantation and forest sourcing area level, the principles and requirements specified in the System Documents *ISCC EU 202-1 Agricultural Biomass: ISCC Principle 1*, *ISCC EU 202-2 Agricultural Biomass: ISCC Principles 2-6*, *ISCC EU 202-3 Forest Biomass: ISCC Principle 1* and *ISCC EU 202-4 Forest Biomass: ISCC Principles 2-6* must be considered. Relevant risks on farm/plantation and forest sourcing area level include:

> Biomass production on land with high biodiversity value, high carbon stock or with a high conservation value (see ISCC Principle 1),

> Biomass production with a negative environmental impact, e.g. on soil, water and air (see ISCC Principle 2),

> Unsafe working conditions (see ISCC Principle 3),

> Violations of human rights, labour rights or land rights (see ISCC Principle 4),

> Violations of applicable legislation (see ISCC Principle 5), and

> Not implementing good management practices (see ISCC Principle 6).

Documentation

Accurate and reliable documentation is essential for ensuring traceability, demonstrating conformity, and safeguarding the integrity of the ISCC PLUS system. Therefore, special attention should be given to identifying potential weaknesses or inconsistencies in documentation practices. The following guidance supports CBs in evaluating and classifying such risks during the risk assessment process:

> The risk may be classified as ‘regular’ if all required records and documents are accurate, complete, up to date, and readily accessible. There should be no indication of non-conformity with ISCC PLUS requirements. For example, the risk of non-conformity with traceability requirements may be considered regular if a reliable and auditable track-and-trace database is in use and can be accessed by the CB during the audit.

> The risk should be classified as ‘medium’ if records and documents are not maintained accurately or are not easily accessible, potentially hindering effective verification during the audit.

> The risk must be classified as high if records and documents are not kept up to date, are incomplete, missing, withheld, or inaccessible, or if there are indications of non-conformity or fraud.

Non-conformity

Specific indications of non-conformity with ISCC PLUS requirements must be taken into account when evaluating and classifying the risk. If a System User is found to have non-conformities during the certification period, the risk must be classified as high for that audit. This applies in particular where the non-conformities have an impact on the downstream supply chain, for example: cases involving non-conformity with the chain of custody requirements, false

or inaccurate information in Sustainability Declarations, incorrectly determined GHG emission value (if applicable). In such cases, a high risk classification must also be applied for the subsequent recertification audit of the respective System User.

Adjustment of risk level

It is at the discretion of the CB to discontinue the audit if the risk is classified as 'High' and either the documentation is not easily accessible or the volume of missing documentation prevents the proper conduction of the audit. Based on actual findings during the audit and the evidence gathered, the CB may also revise the initially assigned risk level to the audit (either increasing it or decreasing it).

Higher risk in case of frequent changes of CB

System Users are free to select any CB recognised by ISCC to carry out ISCC PLUS audits and may also change their contracted CB. However, frequent changes of CB, may be considered an indicator of potential 'CB hopping' (i.e. changing CBs with the intention concealing non-conformities or violations of ISCC PLUS requirements). In this context, frequent means if a System User changes the CB at least twice within a five-year period. If a System User changes its CB for second time within five years, the newly contracted CB must apply a higher risk level for the next scheduled audit, compared to the risk level applied in the previous audit. It is the responsibility of the newly contracted CB to consider this requirement when conducting the risk assessment. This includes reviewing the System User´s certification history and the relevant documentation from the previous audits. See System Document *ISCC PLUS 201 – System Basics* for further information.

Higher risk after suspension or withdrawal of certificate

In the case of non-conformities with ISCC PLUS requirements, ISCC PLUS certificates may be suspended or even withdrawn, depending on the severity of the infringement (see System Document *ISCC PLUS 102 – Governance*). Following a suspension, withdrawal, or any period during which a certificate was suspended, the CB must apply a higher risk level for at least the next two audits. This revised risk level must be higher than the one applied in the audit prior to the suspension or withdrawal.

3.3 Identification and Implementation of Risk Control Measures

Elements of risk control

After risks have been identified and evaluated, they must be appropriately managed to ensure that the probability of non-conformity with ISCC PLUS requirements is continuously minimised. Considering the risk and its priority, some applicable control measures could be:

For System Users

> Adapting internal policies based on risks information to improve the quality assurance assessment data

> Removing the root cause of the risk entirely or choosing not to initiate or continue an activity that creates risk.

- Reducing the likelihood or the impact of the risk by taking steps to minimise the potential consequences or decrease the probability of the risk occurring
- Strengthening internal management measures of the System User. This may include:
  - Clarifying responsibilities
  - Providing targeted training for employees
  - Enhancing documentation practices
  - Improving reporting obligations (e.g., submission of information and to the CB or to ISCC)
  - Strengthening internal audits and management system

For CBs

- Adjusting the audit intensity to reflect the identified risk level. For group certifications, this may involve increasing the sample size to be audited. Regarding traceability, it may require verifying a larger number of documents.
- Conducting surveillance audits, either announced or unannounced surveillance audits, if deemed necessary by the risk assessment.

Adjustment of sample size

If the audit involves sample audits of third party locations (e.g. Farms/Plantations, Points of Origin, Storage Facilities or other group certification), the minimum required sample size must be multiplied by the applicable risk factor (1.0, 1.5 or 2.0). This risk factor directly determines the number of locations to be audited. In case where non-conformities are identified among individual group members, the calculated sample size (s) for the current audit must be doubled to ensure a more robust verification process.

Verification intensity of documents

When the audit involves the verification of chain of custody verification (i.e. traceability and plausibility of material quantities), the risk factor determines the depth and intensity of the audit of the documentation review. All records relevant for ISCC PLUS over a full year retrospective must be available during the audit to enable a reliable evaluation of the chain of custody and to allow for plausibility checks between the System User´s reporting and the respective chain of custody results.

3.4 Risk Monitoring

Continuos monitoring

Risk monitoring is a critical stage in which identified risks and the corresponding risk control measures are continuously observed and assessed. This process ensures that the risk management system remains effective and efficient over time. By actively monitoring risks, CBs can detect changes in risk levels, identify emerging threats, and evaluate whether implemented strategies and control measures are mitigating the risk of non-

conformity with the ISCC PLUS System. Records of the risks detected during the Risk Assessment performed by the CB and their respective treatment strategies must be included in the CB annual evaluation report to ISCC.

4 Assurance Engagement and Audits

Audit assurance

Within the framework of the audits conducted by the CBs and considering ISAE 3000, an assurance engagement refers to the level of confidence that the result of the audit provides to stakeholders and ISCC about the reliability of information or adherence with the requirements of the ISCC PLUS system. The scope and depth of testing and evaluation depends on whether the engagement is conducted at a limited or reasonable assurance level.

Limited assurance

Limited assurance refers to the engagement conducted by the auditor in which fewer and less detailed procedures, such as inquiries and analytical reviews, are conducted to determine whether the information provided is free from material misstatement.[5] The conclusion is expressed in a negative form, meaning that nothing has come to the auditor´s attention that would indicate material errors or non-conformity.

Reasonable assurance

On the other hand, in a reasonable assurance, the auditor conducts a more extensive testing, including detailed document reviews and substantive procedures, to ensure the information provided is free from material misstatement. The conclusion is expressed in a positive form, meaning the CB confirms that the information is fairly presented in all material respects.

Assurance engagement under ISCC PLUS

For ISCC PLUS certification, the default assurance level is limited assurance. A reasonable assurance level may be required if mandated by national or regional authorities in the context of a specific certification scheme under which ISCC PLUS is recognised. Also, a reasonable assurance may be applied if the CB considers it necessary based on the results of the risk assessment. This approach aligns with the ISEAL Code of Good Practice, which emphasises that assurance levels should be based on a risk assessment. In general, limited assurance is considered sufficient to uphold the integrity of ISCC PLUS certification, as it focuses on verifying the most relevant risk indicators related sustainability and/or traceability claims.

Traceability checks

In the context of verifying the documents, , it is generally not necessary for the CB to verify every individual document (e.g., weighbridge tickets, Sustainability Declarations, contracts, etc.) covering the entire previous year. Instead, the CB must apply a random and risk-based sampling approach to assess whether the documentation meets the traceability requirements. The CB is responsibility for defining a sample size that allows it to reach a level of confidence sufficient to justify the issuance of a certificate. The following guidelines can be applied, depending on the assessed level of risk:

[5] According to ISAE 3000 (revised), a misstatement is *a difference between the subject matter information and the appropriate measurement or evaluation of the underlying subject matter in accordance with the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions.*

- Regular risk: random document samples covering three successive months are sufficient to assess whether the applicable ISCC PLUS requirements are met.
- Medium risk: in addition to random document samples from three successive months, all documents from one full month, should be reviewed in detail.
- High risk: all documents covering three successive months should be reviewed completely.

Selecting sample of group members

In the context of determining the sample of group members (once the sample size has been calculated), the selection must ensure a balanced representation of the entire group, using a combination of risk-based and random selection. The auditor must consider at least the following factors:

- Type of raw material supplied (if applicable, ensure appropriate representation)
- Supplier size variation
- Geographical location (e.g. clustering by risk level)
- Indications of non-conformity or fraud

At least 25% of the sample must be selected randomly. For the risk-based portion, preference should be given to members with signs of non-conformity or fraud, or those in high-risk areas. If remote sensing (e.g. satellite data or databases) identifies varying risk levels, previous audit results from the area (if available) must also be considered.). For more detailed information, see System Document *ISCC PLUS 203 – Traceability and Chain of Custody*.