ISCC
International Sustainability & Carbon Certification

ISCC EU 204
RISK MANAGEMENT

Document Title: ISCC EU 204 Audit Requirements and Risk Management

Version 4.2

Valid from: 21 May 2025

Content

Summary of Changes

The following is a summary of the main changes to the previous version of the document (ISCC EU Document 204 v4.2). The revision of the document includes relevant adjustments based on the revised Renewable Energy Directive (RED) EU/2018/2001 also referred to here as RED III. Minor amendments, e.g. corrections of phrasings and spelling mistakes, are not listed.

Summary of changes made in version 4.2	Chapter
General: All reference regarding the RED refer to the revised Renewable Energy Directive EU/2018/2001 (also referred to here as RED III)	
Amendment: 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).	2
Addition: New Definition Risk	3.1
Amendment: Adjusted definition of risk indicator, analysis of risk indicator and its role in the risk assessment	3.1
Amendment: Main steps of the risk management process has been redefined	3.1
Addition: Principles of the risk management principles in the levels of application	3.1
Addition: These procedures should address possible risks that could arise from the CB’s own activities, such as conflict of interest, auditor competence, and quality management.	3.1.2
Addition: The CB should consider the results of the self-assessment performed by the System User and the measures the System User implemented to address and minimise the identified risks to the integrity of ISCC.	3.1.2
Amendment: (…) Additionally, the CB must consider the results of previous audits when planning current audits. As part of the ongoing audit and adaptability of the process, CBs have the authority to adjust the risk level based on fact-based findings (by either increasing or decreasing the risk level), as new information emerges during the planning process.	3.1.2
Amendment: (…) “It is recommended that CBs also participate in Integrity Assessments at System Users certified by the respective CB. On a regular basis, ISCC invites cooperating CBs to exchange feedback and practical experiences to discuss potential risks identified during the day-to-day operation of the CB. (…)	3.1.2
Addition: “Self-assessment should be conducted as part of the internal audit and the results of the self-assessment must be shared with the CB prior to the ISCC audit. The CB will consider the self-assessment results as a basis for developing its own risk assessment.” (…)	3.1.3
Addition: “Implemented risk indicators shall reflect all types of possible risks related to product, species, or industrial sectors than can be linked to sustainability issues, geographic areas that are more exposed to risk than others, and to internal risks related to the individual organisation, suppliers and producers, among others.”	3.2.1
Amendment: “CB shall provide ISCC with a detailed description of the verification of compliance with ISCC Principle 1, when in the framework of the risk assessment performed for the audit, it has been established that land use change (LUC) took place after January 1st, 2008.”	3.2.1
Addition: “Some examples of general risk indicators are listed below. It is important to note that risk assessment should not be limited only to these indicators. ISCC	3.2.1

Summary of changes made in version 4.2	Chapter
encourages the use of other relevant risk indicators to identify possible risks when the risk assessment is performed by CBs and System Users."	
Addition: 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*.	3.2.1
Addition: "With respect to the evaluation of the risk on (…) forest level, the principles and requirements specified in (…) ISCC EU 202-3 Forest Biomass - ISCC Principle 1, and ISCC EU 202-4 Forest Biomass - ISCC Principles 2-6 must be considered.	3.2.2
Amendment: "This is particularly relevant when these non-conformities affect the downstream supply chain, such as non-compliance with mass balance requirements, inaccuracies in sustainability declarations (e.g. false information), or deviations from greenhouse gas requirements (e.g. incorrectly calculated GHG emission values)."	3.2.2
Amendment: "It is at the discretion of the auditor's professional judgment to discontinue the audit if the risk is classified as high, and either the documentation is not readily accessible, or the volume of unavailable documentation prevents a thorough and professional audit."	3.2.2
Amendment: Risk control measures suggested for CBs and for System Users	3.3
Addition: Monitoring of risk	3.3
Addition: Assurance Levels for ISCC Statements based on the Risk Assessment	3.4
Addition: Risk Evaluation Template and example	Annex 1

1 Introduction

High quality verification

Clear requirements on how to manage risks in the ISCC 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. Furthermore, they facilitate consistent verification of the legal requirements laid down in the revised Renewable Energy Directive EU/2018/2001 (often referred to as RED III)[1].

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 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 System Users (referred to hereafter as System Users).

2 Scope and Normative References

Best practice principles

The scope of this document covers the requirements on how the risk management process under ISCC is applied to all activities of ISCC and the implications of risks for ISCC audits. The risk management process considers 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). The requirements for risk management complement the requirements laid down in the ISCC System Documents. They apply to ISCC, System Users and recognised CBs conducting ISCC audits.

3 Risk Management

3.1 Definitions, Process 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 a risk according to its probability to occur and the significance of its consequences. Risk indicators can be used to identify potential risks. Risk indicators are quantitative and qualitative variables that help identify potential risks. These risk indicators provide insights into events or situations that may pose threats

[1] *The "Directive (EU) 2018/2001 on the promotion of the use of energy from renewable sources (recast)" has been amended by Directive (EU) 2023/2413. The text of the revised Directive EU/2018/2001 is in the following referred to as RED III*

to ISCC. Through a detailed analysis of the risk indicators applicable to each process, it is possible to identify a potential risks context of non-compliance to ISCC requirements. Once a risk is identified it must be registered and evaluated according to its relevance in the specific situation. The result of the evaluation leads to the classification of the risk. Within the ISCC audit framework, risks are evaluated and classified according to a risk level (regular, medium or high) and assigned to a corresponding risk factor (1.0, 1.5, or 2.0).

Definition risk management

Risk management means the entire process of risk assessment (identification and evaluation of the risk) followed by the identification and implementation of risk control measures to reduce the probability and/or the negative consequences associated with a risk. Therefore, the risk management process within the scope of ISCC is carried out according to the next steps:

- Identification of risks,
- Registration of the risks,
- Evaluation and analysis of the risks,
- Treatment of the risks, and
- Monitoring of risks.

Levels of application

Risk management is relevant at three different levels in the ISCC system: for ISCC as an organisation, for CBs cooperating with ISCC, and for System Users being certified according to ISCC. At each level, the principles for risk management must be appropriately considered and applied to ensure effective risk mitigation and the integrity of the ISCC system. The principles of risk management emphasize a proportional and risk-based approach, 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-compliance 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 implement a Stakeholder Committee or Working Group for the development of appropriate risk control measures. For the development of appropriate risk control measures a fact-based analysis of the risk must be considered.

Promotion of risk management tools

Furthermore, ISCC supports the development of new tools and measures to enhance the risk management process. This includes the application of risk assessment tools such as remote sensing analysis, to assess land use change and other land-related sustainability criteria, or the use of databases to improve the traceability of sustainable material and the accuracy of related sustainability claims, reducing the risk of fraud.

ISCC Audit Procedure System

The use of the Audit Procedure System (APS) is mandatory for CBs and auditors. APS reduces the risk of human errors and automates the detection of inconsistencies within the audit report. APS 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 cases (e.g. severe problems with IT components, system breakdowns, etc.) or when new audit procedures have not been integrated into APS.

ISCC Integrity Programme

The ISCC Integrity Programme is an important tool used by ISCC to continuously identify and analyse potential risks to the ISCC System, the practical application of ISCC by System Users, and the verification by CBs. Within the ISCC Integrity Programme, ISCC conducts independent Integrity Assessments to evaluate the performance of CBs and individual auditors, as well as of certified System Users. Integrity Assessments can be conducted at the cooperating CBs head office or at the sites of the certified System Users. It is also possible to conduct an Integrity Assessment or parts of it remotely. The results of the Integrity Programme are the basis of ISCC's risk management and are used to improve the quality of the system and to reduce the risk of non-conformity. See ISCC EU System Document 102 "Governance" for further information.

Internal review

Audit documentation must be submitted by the CB to ISCC after an audit has been conducted. The ISCC head office internally reviews this documentation as a part of the risk management process. Such internal reviews ensure a consistent application of ISCC requirements and a level playing field for CBs and System Users. See System Documents ISCC EU 102 "Governance" and ISCC EU 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 the CB provided to System Users (ISCC audits). Internally, CBs should have appropriate risk management procedures in place covering potential risks for the integrity of ISCC. These procedures should address possible risks that could arise from the CB's own

activities, such as conflict of interest, auditor competence, and quality management. CBs conducting ISCC audits for System Users must have an internal procedure on how to perform reliable risk assessments for System Users to be certified. The general requirements for CBs are specified in ISCC EU System Document 103 “Requirements for Certification Bodies and Auditors”.

Recognised CBs are obliged to participate in office audits scheduled by ISCC in the framework of the ISCC Integrity Programme. It is recommended (but not mandatory) that CBs also participate in Integrity Assessments at System Users certified by the respective CB. On a regular basis, ISCC invites the recognised CBs to exchange feedback and practical experiences and to discuss potential risks identified during the day-to-day work of the CBs and of ISCC.

Risk assessment during audits

At the beginning of each ISCC audit, the CB must conduct a risk assessment for the System User to be certified. During this risk assessment the CB identifies, evaluates and classifies the risk according to one of the three ISCC risk levels (regular, medium, high). The CB should consider the results of the self-assessment performed by the System User and the measures the System User implemented to address and minimise the identified risks to the integrity of ISCC. Relevant risk indicators applicable to the System User’s processes must be considered for performing the risk assessment.

Based on the CBs professional judgement and the information submitted by the System User, the CB should pay close attention to possible risks which could lead to a material misstatement such as inaccurate sustainability claims, misreported information, or fraudulent documentation. To enhance the reliability of the risk assessment, CBs may refer to ISCC documents, tools or other reliable sources and check available country-specific information for the region where the audit will be conducted. This can include, for example, a web-based inquiry of current reports from NGOs, journals or other media reports regarding social or environmental issues relevant to the region where the audit will take place. The result of this investigation must be taken into consideration for the identification and evaluation of risks and to determine when audits are planned and conducted.

Sample size and audit intensity

The result of the risk assessment directly influences the audit intensity and sample size during the certification process. As higher the determined risk factor, the lower engagement risk is acceptable and more detailed and comprehensive the audit needs to be conducted to verify and ensure compliance with ISCC requirements. In case of group certification, auditors conduct audits of a sample of the group members (sampling), the risk factor determined by the CB drives the sample size of group members to be audited (see ISCC EU System Document 203 “Traceability and Chain of Custody”).

During audits, the CB must follow a risk-based approach that involves prioritizing areas, processes and products identified as higher risk during the risk assessment, while placing less emphasis on those classified as a lower

risk (see risk-based audit approach on ISCC EU System Document 201 “System Basics”). Additionally, the CB must consider the results of previous audits when planning current audits. As part of the ongoing audit and adaptability of the process, CBs have the authority to adjust the risk level based on fact-based findings (by either increasing or decreasing the risk level), as new information emerges during the planning process.

Cooperating CBs are obliged to participate in office audits scheduled by ISCC in the framework of the ISCC Integrity Programme. It is recommended that CBs also participate in Integrity Assessments at System Users certified by the respective CB. On a regular basis, ISCC invites cooperating CBs to exchange feedback and practical experiences to discuss potential risks identified during the day-to-day operation of the CB. The general requirements for CBs are specified in ISCC EU System Document 103 “Requirements for Certification Bodies and Auditors”.

3.1.3 ISCC System Users

Self-assessment

System Users must initiate the certification process of ISCC by conducting an internal risk assessment (self-assessment) regarding potential risks its activities could have for the integrity of ISCC. Self-assessment should be conducted as part of the internal audit and the results of the self-assessment must be shared with the CB prior to the ISCC audit. The CB will consider the self-assessment results as a basis for developing its own risk assessment. More information regarding the annual internal audit is stipulated in the ISCC EU System Document 203 “Traceability and Chain of Custody”.

Analogous to the external risk assessment conducted by the CB, the self-assessment can be conducted based on the principles and risk indicators specified in chapter 3.2.1. Based on the result of the self-assessment, the System User should design its internal management system in a way to appropriately address and minimise the identified risks its activities could have for the integrity of ISCC.

Integrity Programme

All System Users are obliged to participate in Integrity Assessments scheduled by ISCC in the framework of the ISCC Integrity Programme. Non-cooperation/participation in the Integrity Programme is regarded as a critical non-conformity and sanctioned accordingly (see ISCC EU System Document 102 “Governance”).

3.2 Risk Assessment

3.2.1 Identification of Risk

Analysis of risk indicators

The first step during the risk assessment is to identify potential risks by analysing the risk indicators (some examples are listed at the end of this section). The analysis of the risk indicators forms the basis for risk assessment in the framework of ISCC. Risk indicators shall be considered during all ISCC audits to identify potential risks of non-conformity with the ISCC requirements

or for the integrity of ISCC and must be supplemented by further risk indicators if required to properly assess the individual set-up of a System User. Implemented risk indicators shall reflect all types of possible risks related to product, species, or industrial sectors than can be linked to sustainability issues, geographic areas that are more exposed to risk than others, and to internal risks related to the individual organisation, suppliers and producers, among others.

A risk assessment may be conducted remotely via a desk assessment, e.g. by verifying land use change with satellite data, by analysing biodiversity information in databases, by searching databases on protected areas or by conducting (web-based) research on social and environmental issues. If necessary, the remote assessment may be supplemented by the verification of the results at the specific location (so-called “ground-truthing”). ISCC may require System Users and CBs to use specified online tools for specific audit scopes to enable a harmonised approach and by this to provide a level playing field.

Assessment of farms/plantations and forests

If ISCC audits include the verification of farms/plantations and forests, a risk assessment must be conducted to determine the risk of non-conformity with the ISCC sustainability requirements for agricultural and forest biomass (see ISCC EU System Documents 202-1, 202-2, 202-3 and 202-4). It is particularly crucial to assess the risk of violations related to ISCC Principle 1. This means, it must be assessed if a farm/plantation/forest is located within the proximity of areas where the cultivation of biomass is prohibited under ISCC. The risk of non-conformity of farms/plantations/forests should be assessed with appropriate and reliable databases or remote sensing tools allowing for a meaningful and well-balanced result for the respective region. If available, such a risk assessment should be performed with tools or systems which may be recognised by the European Commission in the framework of the RED III (so-called non-typical voluntary schemes). An example for risk assessment of farms/plantations/forests using satellite data is provided in Figure 1.

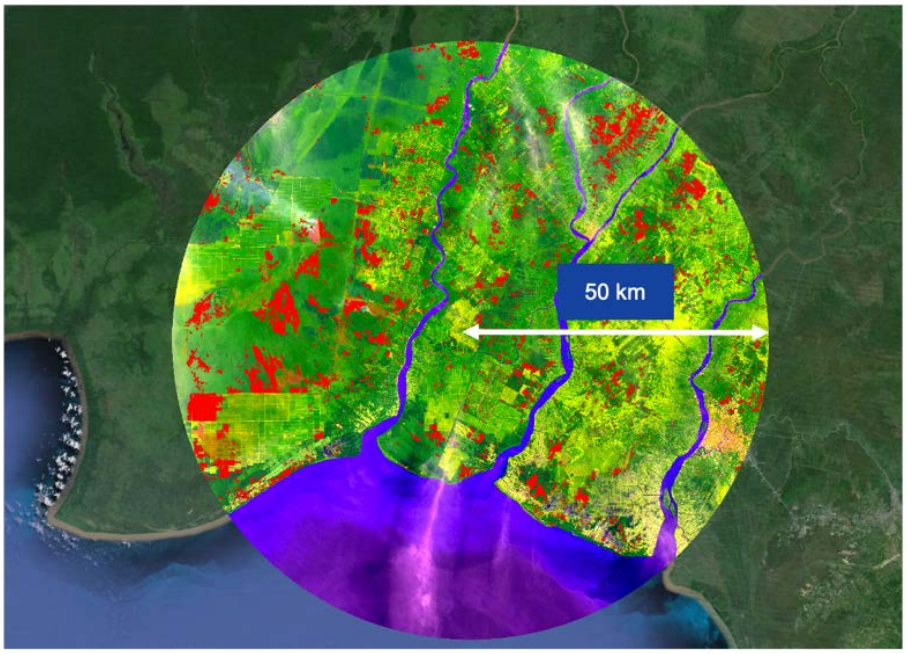

Figure 1: Example of a risk assessment of farms/plantations/forests using satellite data (red areas indicate potential land use change in an area after January 2008)[2]

Land use change after January 2008

CB shall provide ISCC with a detailed description of the verification of compliance with ISCC Principle 1, when in the framework of the risk assessment performed for the audit, it has been established that land use change (LUC) took place after January 1st, 2008. This includes displaying the areas where the LUC took place, the land category of the respective areas prior to the land conversion and how the land category was determined, as well as information on the expertise of the LUC verifier (auditor or CB expert). See also ISCC EU System Document 103 "Requirements for Certification Bodies and Auditors".

Assessment of waste or residues

If ISCC audits include waste and residues, the risk assessment must focus on determining the risk of false claims and the risk of "intentional" production of waste and residues, e.g. with the intention to receive special incentives. This means that the focus should be on the verification at the point of origin of whether a material is a genuine waste or residue (the material meets the definition for waste and residues), and on the correct and consistent declaration of the material by the point of origin and by the collecting point (see ISCC EU System Document 202-5 "Waste and Residues").

Traceability and chain of custody

The traceability and chain of custody of sustainable material is an important aspect of the risk assessment for all System Users (see ISCC EU System Document 203 "Traceability and Chain of Custody"). It must be assessed if there are specific risks that non-certified material is sold or delivered as ISCC certified and if the requirements on mass balance are complied with.

GHG emissions

With regards to the greenhouse gas emission value of sustainable material, it must be assessed whether there is a risk of mistakes when calculating the

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

emission value, a risk of false declaration of emissions or a risk of mistakes when applying default values (see ISCC EU System Document 205 “Greenhouse Gas Emissions”).

General risk indicators

Some examples of general risk indicators are listed below. It is important to note that 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.), e. g. 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.

> Switch from the use of default values to individual GHG emissions calculation.

> In case of group certification: Adding group members (e.g. farms/plantations) to the group for which GHG emissions are calculated individually.

> Certification history, including previous or current ISCC certification and certification under other sustainability certification systems, especially those recognised by the European Commission within the

framework of the RED, 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 certification body 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”).

Land related risk indicators

Risk indicators for farms/plantations and forests 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 EU Member States or other incentives granted by law.
- Declaration or labelling of the material (e.g. according to official waste catalogues or waste codes).
- Risk of deliberate or wilful "production" of waste or residues.
- Use of feedstocks based on waste/residues and virgin materials.
- Risk of deliberate or wilful 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 and analysis of the identified risk, the following elements must be taken into consideration:

- Sources and causes of the risk.
- Identification of potential consequences from the risk if it would occur, the impact (negligible, moderate, critical) and the probability of its occurrence (unlikely, occasional, likely).
- Factors influencing the consequences and the probability of the risk to occur.
- Differing perceptions of the importance of or emphasis on the risk by different stakeholders.

Risk levels and factors

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

- Regular[3] (risk factor 1.0)
- Medium (risk factor 1.5)
- High (risk factor 2.0)

A risk assessment matrix as shown in Table 1 may be used to facilitate the classification of the risk.

[3] *The risk level „regular" has to be applied if the risk assessment conducted by the certification body identifies a low risk for the auditee.*

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

ISCC Risk Evaluation Template

The risk evaluation template (Annex 1) indicates the minimum elements of a risk assessment approach for the activities audited within the ISCC System. CBs can use this template to identify the basic requirements for a risk assessment of the ISCC System. System Users may use this template as a reference to identify the elements to develop their self-assessment.

ISCC sustainability principles

With respect to the evaluation of the risk on farm/plantation/forest level, the principles and requirements specified in ISCC EU System Documents 202-1 Agricultural Biomass - ISCC Principle 1, ISCC EU 202-2 Agricultural Biomass - ISCC Principle 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/forest 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

With respect to the risk of flawed or deficient documentation the following guidance can be given for the risk evaluation and classification:

> If the necessary records and documents are kept accurately, up to date, complete, easily accessible, and there is no indication of non-conformity with ISCC requirements, the risk can be classified as regular. The risk of non-conformity with traceability requirements can be considered to be regular if, for example, appropriate track-and-trace databases are used and can be accessed by the CB during the audit.

> If the necessary records and documents are not kept accurately and are not easily accessible, the risk should be classified as medium.

> If the records and documents are not continuously up to date and not kept to full extent, e. g. files are missing, files are not accessible, files are not disclosed, or if there is indication of non-conformity or fraud the risk should be classified as high.

Non-conformity

Specific indication of non-conformity with ISCC requirements must be considered during the risk evaluation and classification. If non-conformities are detected during an ISCC audit that relate to claims made by the System User during the certification period, a high level of risk must be applied during the audit. This is particularly relevant when these non-conformities affect the downstream supply chain, such as non-compliance with mass balance requirements, inaccuracies in sustainability declarations (e.g. false information), or deviations from greenhouse gas requirements (e.g. incorrectly calculated GHG emission values). In this case, a high-risk level of risk 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 auditor's professional judgment to discontinue the audit if the risk is classified as high, and either the documentation is not readily accessible, or the volume of unavailable documentation prevents a thorough and professional audit. Depending on the actual findings during the audit, the CB is entitled to increase or reduce the risk level applied during the audit.

Higher risk in case of frequent changes of CB

System Users have the flexibility to select any certification body working in cooperation with ISCC to conduct ISCC audits and may also choose to switch to a different CB if desired. However, if a System User frequently changes the CB conducting the audits under ISCC, this may be regarded as an indicator of so-called "CB hopping" (e.g. change of CB with the intention to cover up infringements or violations of ISCC requirements). In this context, frequent means if a System User changes the CB at least twice within five years. The CB that is contracted by the System User with the second change of CB within five years must apply a higher risk level for the next scheduled audit, e.g. the risk level must be higher than the risk level applied for the previous audit. It is the responsibility of the newly contracted CB to take this requirement into account when conducting the risk assessment, as well as considering the certification history of the System User and the relevant audit documents from the previous audits. See ISCC EU System Document 201 "System Basics" for further information.

Higher risk after suspension or withdrawal of certificate

In the case of non-conformities with ISCC requirements, ISCC certificates may be suspended or even withdrawn, depending on the severity of the infringement (see ISCC EU System Document 102 "Governance"). For at least the next two audits following the suspension or withdrawal of a certificate or a period of suspension the CB must apply a higher risk level, e.g. the risk level must be higher than the risk level applied for the previous audit.

3.3 Identification and Implementation of Risk Control Measures

Elements of risk control

After the risk is identified, evaluated and classified it must be managed properly to ensure that the probability of non-conformity with ISCC requirements is continuously minimised. According to the risk and its priority, some applicable control measures could be:

For CBs:

> Adjusting the intensity of audits to adequately consider the risk level. In the case of group certifications, this means that the size of the sample may be adjusted. With regards to traceability, this means adjusting the number of documents to be verified by the CB.

> Carrying out announced or unannounced surveillance audits, if necessary.

> Adjusting the tasks of the management of a System User, with regards to:
  - Specification of responsibilities,
  - Training of employees,
  - Documentation,
  - Duty to report (including reporting and submitting documents to the CB or to ISCC), and
  - Internal auditing and management system.

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 minimize the potential consequences or decrease the probability of the risk occurring.

Adjustment of sample size

If the audit includes sampling of third-party locations, e.g. farms/plantations, points of origin or storage facilities, the minimum sample size must be multiplied with the determined risk factor (1.0, 1.5 or 2.0). The risk factor therefore determines the number of locations which must be audited. In case of non-conformity of individual group members, the determined sample size of the current audit must be doubled.

Verification intensity of documents

If the audit includes chain of custody verification, e.g. traceability and plausibility of amounts, the risk factor drives the intensity of the audit with respect to the documentation that needs to be verified. All documentation relevant for ISCC for a complete year must be available during an ISCC audit to evaluate the mass balance calculation and allow for plausibility checks between company reporting and mass balance results. However, it is (usually)

not necessary for the CB to verify every single document (e.g. weighbridge tickets, Sustainability Declarations, contracts, etc.) from an entire year. Instead, the CB is entitled to and must be able to take random and risk-based document samples to check whether records and documents meet the requirements for traceability. It is the CB's responsibility to define the size of the sample that will permit the CB to reach the level of confidence necessary to issue a certificate. The following guidelines can be applied:

> If the risk is classified as "regular", random document samples from three successive months are sufficient to assess whether the applicable ISCC requirements are met.

> If the risk is classified as "medium", random document samples from three successive months, as well as all documents from one complete month, should be checked.

> If the risk is classified as "high", the documents of three successive months should be checked completely.

Monitoring of risks

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-compliance with the ISCC 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]. ISCC is entitled to use this information to fulfil its reporting obligations to the European Commission and to competent national authorities.

3.4 Assurance Levels for ISCC Statements based on the Risk Assessment

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 sustainability information provided is free from material misstatement. 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-compliance.

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 sustainability claims are 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.

[4] Each individual risk detected during audits does not have to be stated in the report, but risks that were detected in a few audits (recurrent) should be clustered under sector, material, geographic area, or producer. This is important for gathering information on risks that require more focus during future audits, and which may be addressed and clarified within the ISCC System.

Assurance Engagement

Within the framework of the audits conducted by the CBs and considering ISAE 3000 standard, 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 System. The level of testing and depth of evaluation depends on whether the engagement is for limited or reasonable assurance.

The result of the risk evaluation and classification determines the expected level of assurance engagement of the statements in the audit, which in turn marks the development of the audit plan and the intensity of the audit.

A limited assurance level of engagement is possible in case the risk level has been classified as regular (risk factor 1.0), except in the initial audit of a new scheme participant or a re-certification of existing scheme participant under a revised regulatory framework that shall always as a minimum provide reasonable assurance on the effectiveness of its internal processes. A reasonable assurance level of engagement is expected in case the risk level has been classified as medium (risk factor 1.5), or high (risk factor 2.0).

Annex I: Risk Assessment Template

Risk assessment should not be limited only to the information presented in this template. ISCC encourages the use of other relevant information to identify, evaluate, classify and monitor possible risks when the risk assessment is performed. An example of the template has been included at the end of this section.

1. Identification of the risk:
   - *Description of the risk:* A detailed explanation of the specific risk, including what could go wrong, how it could occur, and the potential impact on the certification process or sustainability requirements.
   - *Associated ISCC requirement:* ISCC System Document or specific requirement that the identified risk relates to, providing context and a reference for compliance.

2. Evaluation of the risk (Table 1)
   - *Probability:* The likelihood of the risk occurring, measured on a scale (likely, occasional, unlikely).
   - *Consequences:* The severity of the impact if the risk materializes, including potential effects compliance and integrity of the ISCC System, or sustainability outcomes, measured on a scale (critical, moderate, negligible).

3. Classification of the risk (Table 1)
   - *Risk level:* The overall categorization of the risk based on its probability and consequences, expressed as regular, medium, or high.
   - *Risk factor:* A numerical value derived from combining the probability and consequences, used to prioritize and rank risks and expressed as 1.0 for regular level risk, 1.5 for medium risk, and 2.0 for high risk.

4. Treatment of the risk
   - *Priority:* The urgency or importance of addressing the risk, based on its classification and potential impact. Measured as low for a risk factor of 1.0, and high for a risk factor bigger than 1.0.
   - *Mitigation actions (for System Users):* Specific actions or strategies implemented by System Users to reduce the likelihood or consequences of the risk.
   - *Control measures:* Additional mechanisms or processes to prevent, detect, or respond to the risk effectively, ensuring compliance with ISCC requirements.
   - *Responsible:* Individual(s) or team(s) accountable for implementing and overseeing the mitigation actions and control measures.

5. Monitoring the risk

- *Effectiveness of actions / control measures:* An evaluation of how well the implemented actions and control measures are working to manage the risk, ensuring continuous improvement.
- *Review:* Regular assessments of the risk and its management strategies to adapt to changes, identify new risks, and ensure alignment with ISCC requirements.

Example:

Risk Identification		Risk Evaluation		Risk Classification		Risk Threatment				Risk Monitoring	
Description of the Risk	**ISCC requirement**	**Probability**	**Consequ**	**Risk Level**	**Risk Factor**	**Priority**	**Mitigation Actions**	**Control Measures**	**Responsible**	**Effectiveness**	**Review**
Economic incentives for the use of materials considered as waste/residue	ISCC EU 202-5 Waste and Residues	Likely	Critical	High	2.0	High	Verify that the material meets the definition for waste and residues	Verify that declaration of the material by the point of origin and by the collecting point is correct	System User Responsible 1	Yes	6 months