

# ISCC 204 AUDIT REQUIREMENTS AND RISK MANAGEMENT

Version 3.0



#### Copyright notice

© 2016 ISCC System GmbH

This ISCC document is protected by copyright. It is freely available from the ISCC website or upon request.

No part of this copyrighted document may be changed or amended. The document may not be duplicated or copied in any form or by any means for commercial purpose without permission of ISCC.

Document Title: ISCC 204 Audit Requirements and Risk Management

Version 3.0

Valid from: 09 August 2016 (Date of Commission Implementing Decision (EU) 2016/1361)

## Content

1	Introduction .....	4
2	Scope and Normative References.....	4
3	Audit Requirements.....	4
3.1	Definitions and General Requirements.....	4
3.2	Audit Procedures and Reports .....	10
3.3	Specific Audit Requirements .....	11
3.3.1	Farms and Plantations .....	11
3.3.2	Point of Origin .....	13
3.3.3	Central Office.....	13
3.3.4	First Gathering Point and Collecting Point.....	14
3.3.5	Processing Unit.....	15
3.3.6	Storage Facilities and Logistic Networks .....	16
3.3.7	Traders .....	16
3.3.8	Other Elements of the Supply Chain .....	17
3.4	Non-Conformities .....	17
3.4.1	Definition and General Requirements.....	17
3.4.2	Sanctions .....	18
3.4.3	Conflict Resolution .....	19
4	Risk Management .....	19
4.1	Definitions, Process and Levels of Application .....	19
4.1.1	ISCC .....	19
4.1.2	Certification Bodies .....	20
4.1.3	ISCC System Users .....	21
4.2	Risk Assessment.....	22
4.2.1	Identification of Risk.....	22
4.2.2	Evaluation of Risk .....	25
4.3	Identification and Implementation of Risk Control Measures .....	27

## 1 Introduction

Clear requirements on how to conduct audits and how to manage risks in the framework of ISCC 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 a consistent verification of the legal requirements laid down in the *Renewable Energy Directive 2009/28/EC* amended through *Directive (EU) 2015/1513 (RED)* and *Fuel Quality Directive 2009/30/EC* amended through *Directive (EU) 2015/1513 (FQD)*<sup>1</sup>.

*High quality verification*

The audit requirements specified in this document describe the relevant aspects to be considered and procedures to be followed when carrying out ISCC audits. The audit requirements include the aspects relevant to all ISCC audits as well as the criteria which are only relevant to specific scenarios, e.g. depending on the type of operation to be audited.

*Audit process and aspects*

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 and auditors cooperating with ISCC (in the following referred to as CBs), and to ISCC System Users (in the following referred to as System Users).

*Risk management process*

## 2 Scope and Normative References

The scope of this document covers the requirements on how ISCC audits are to be conducted at different elements of the supply chain, the risk management process under ISCC applicable to all activities of ISCC and the implications of risks for ISCC audits. The risk management process takes into account the best practice principles of the ISEAL "Code of Good Practice for Assuring Compliance with Social and Environmental Standards". The principles for risk management and carrying out audits complement the requirements laid down in the ISCC system documents. They apply to ISCC, System Users and recognised CBs conducting ISCC audits.

*Best practice principles*

## 3 Audit Requirements

### 3.1 Definitions and General Requirements

General audit requirements apply to all ISCC audits irrespective of the individual specifications or conditions of the audited site or operation. The general requirements are mandatory for all types of System Users audited in the framework of ISCC.

*General audit requirements*

---

<sup>1</sup> In the following referred to as RED and FQD.

Specific audit requirements apply only to audits of specific System Users or under specific circumstances. Such audit requirements depend on the particular type of operation being audited or the materials handled by the audited System User, e.g. waste and residues.

*Specific audit requirements*

Certification audits<sup>2</sup> are audits which are the basis for a CB to issue an ISCC certificate.

*Certification audit*

Surveillance audits can be imposed by the CB to verify compliance with ISCC requirements during the validity period of a certificate issued by the respective CB. Surveillance audits may focus only on the implementation of partial aspects of ISCC requirements.

*Surveillance audit*

System Users that register with ISCC and want to receive a certificate are subject to an audit during which a recognised CB verifies compliance with the applicable ISCC requirements. An ISCC audit must always be conducted before a certificate can be issued.

*Registration with ISCC*

Prior to any ISCC audit, System Users must have concluded a certification contract with one of the recognised CB's cooperating with ISCC. After concluding the contract with a CB, the System User must register with ISCC. During the registration process, the System User provides basic information to ISCC including the applicable scope for certification (e.g. the type of operation). If it turns out, that the registered scope is not (entirely) correct, the System User's registration with ISCC must be adjusted before the certificate can be issued. The ISCC certificate must only cover the scope that correctly represents the activities of the System User. It is not possible to audit a scope or type of operation which is not correctly representing the activity of the System User or is actually not relevant for the System User.

*Certification contract*

Prior to any ISCC audit, the certification history of the System User must be evaluated. This is usually done during the risk assessment. The CB is obliged to assess if the System User is not currently suspended from certification due to major non-conformities under another relevant sustainability certification system, especially under one of the systems recognized by the European Commission within the framework of the RED and FQD. If a System User is suspended (or "blacklisted") by another sustainability certification system, a certification under ISCC is not possible, until the suspension expires. The System User is obliged to report to ISCC and to its CB immediately, if certificates from other sustainability certification systems are withdrawn due to non-conformities. If the CB receives notice of such a withdrawal of a certificate, the CB is obliged to inform ISCC immediately. ISCC will assess and evaluate such situations and possible consequences on a case-by-case basis taking into account the potential risk for the integrity of ISCC.

*Certification history*

<sup>2</sup> In the following the term „audit“ refers to a certification audit unless specified otherwise.

System Users are obliged to provide accurate and true information to ISCC and to the CB. Furthermore, System Users are obliged to declare to ISCC and to the CB the names of all other sustainability certification systems they are participating in simultaneously to ISCC, or sustainability certification systems they have previously been participating in (certification history). System Users are obliged to make available to the CB all relevant information including the mass balance data and the auditing reports also regarding other sustainability certification systems used. If a System User that was previously in major non-conformity with these requirements or with any other aspect of the mandatory sustainability criteria seeks recertification, the CB is obliged to inform ISCC.

*Accurate and true information*

ISCC audits are retrospectively and focus on the verification of claims made during the previous period of certification. An exception to this rule is the first (initial) audit of a System User during which a retrospective audit of claims is not possible and thus the focus of the audit is on the necessary procedures to appropriately implement and apply ISCC.

*Retrospective audit*

An audit to verify compliance of a System User is required at least every twelve months. System Users should arrange for audits to be conducted in a way that reduces the risk of a gap between two certificates. If there is indication of non-conformity or fraud the frequency or intensity of audits may be increased. This means, that a CB is entitled to conduct additional (surveillance) audits e.g. in case there is reasonable doubt of compliance with the ISCC requirements or in order to verify substantiated allegations of fraudulent behaviour. It is the CB's responsibility to define the intensity of the audit or the size of a sample that will permit the CB to reach the level of confidence necessary to issue a certificate.

*Annual audit*

ISCC audits have to be conducted on-site at the location of the System User registered for certification. Audits are conducted throughout the entire supply chain up to (but not including) the final consumer. All System Users need to be audited individually. Group auditing and sampling can only be applied only at the beginning of the chain of custody as well as for storage facilities according to the requirements specified in ISCC Document 206 "Group Certification". An example of a simplified supply chain is provided in figure 1.

*On-site audit*



Figure 1: Example of a supply chain including supply chain elements to be audited

Particular aspects of an audit, especially the risk assessment or the verification of a greenhouse gas calculation methodology can be based on desk audit. Under specific circumstances, the ISCC audit to verify compliance with the ISCC requirements may be conducted based on desk audit by using appropriate tools providing at least the same level of assurance as an on-site audit. Especially risk assessments and the analysis of land use change after 2008 on a specific area may be conducted on-site,

*Desk audit*

or by using tools which may even provide a more reliable level of assurance than an on-site audit, or by a combination of on-site and desk audit. The use of independent traceability databases may also allow for an equivalent level of assurance as an on-site audit. Precondition for verifying compliance with ISCC requirements based on such tools is the analysis and approval of the respective tool by ISCC as being appropriate to provide at least the same level of assurance as an on-site audit.

ISCC will carry out assessments of such tools based on the following criteria:

- > Methodology and algorithms of the tool are transparent
- > Information sources used are transparent
- > The tool must allow for clearly reproducible and consistent results
- > The tool should include latest available data
- > Traceability databases must cover all sustainability data required by ISCC
- > CBs must have access to the tool and must be enabled to verify compliance with the requirements
- > Mechanisms to avoid fraud and misuse must be in place

If a tool has been approved by ISCC, ISCC will communicate this to its System Users and will publish this information on the website. ISCC will indicate the scope for which the tool has been approved and for which countries or regions the tools can be used.

In any case, audits must follow a risk-based approach and take into account the risk according to the principles specified in chapter 4. This means, if the result of a desk audit based on tools or systems approved by ISCC does not provide a sufficient level of assurance or even indicates non-conformity with ISCC requirements (e.g. indication of land use change in the area of cultivation), the CB must take appropriate further actions to sufficiently verify compliance, e.g. the verification on-site. An example for a desk audit would be the audit of a farm located within an EU Member State that complies with the Cross Compliance (CC) requirements and that can provide to the CB evidence of compliance with CC (e.g. approved application for direct payments) as well as detailed information about the farm area (geo-coordinates and shape-files of the farm and fields). In this case, the verification of compliance with ISCC Principle 1 may be conducted equivalently to an on-site audit by using remote sensing tools, high quality satellite images of the cultivation area and databases (e.g. regarding protected areas, areas with high biodiversity, peatland, etc) which are approved by ISCC for providing reliable information e.g. on the relevant time period or area.

The address or location of the operational unit registered and audited will be published on the ISCC certificate. The address of the operational unit to be

*Assessment  
process*

*Publishing of  
approved tools*

*Risk based  
approach*

*Site-specific  
certificate*

certified cannot be a post box. So-called “letterbox companies” cannot participate in the ISCC system.

Each System User registered for certification under ISCC must conduct an internal assessment (self-assessment) of compliance with the ISCC requirements at least once a year. This internal assessment should focus on the ISCC requirements applicable at the respective type of operation and on relevant risks (also see chapter 4.1.3). The results of the internal assessment must be documented, reviewed and signed by the management of the System User. The results of the internal assessment must be made accessible to the CB during the certification audit.

*Internal  
assessment*

During each audit a risk-based approach according to the principles specified in chapter 4.3 should be followed by the CB. This means, that a higher risk classification results in a higher sample size (in case sampling is part of the audit) and/or in an increased number of documents to be verified by the CB. During the audit, the CB must identify the activities undertaken by the System User which are relevant for ISCC. This includes the identification of relevant systems and the overall organisation especially with respect to the applicable ISCC requirements and the effective implementation of relevant control systems. During the audit the CB should draw up a verification plan which corresponds to the risk analysis and the scope and complexity of the System User’s activities and which defines the sampling methods to be used with respect to the System User’s activities. The CB should carry out the verification plan by gathering evidence in accordance with the defined sampling methods, plus all relevant additional evidence, upon which the CB’s verification decision will be based. It is the System Users obligation to provide any missing elements of audit trails, to explain variations, or revise claims or calculations, before the CB can reach a final verification decision (i.e. the decision to issue a certificate).

*Risk-based audit  
approach*

In the case a System User currently participates in or has recently participated in more than one sustainability certification system, the CB must always verify that multiple claiming (so called “double-accounting”) of sustainability characteristics cannot and did not occur. For this verification, the CB is entitled and obliged to assess the relevant documentation (e.g. mass balance, auditing reports) of all relevant certification systems. This is especially necessary to verify the overall plausibility of incoming and outgoing sustainable material and ensures that not more sustainable material is sold than has been received. The CB must be given access to all documentation that is deemed necessary to get a complete understanding of the individual situation. Access to be given to the CB includes access to databases used by the System User to handle sustainable material.

*Verification of  
claims*

System Users must have a documentation and quality management system which can be audited by the CB. Such a system must include evidence related to the claims the System Users makes under ISCC, e.g. Sustainability Declarations, Proofs of Sustainability, or related contracts. The relevant documentation must be kept for at least five years. System Users

*Documentation  
and quality  
management*

are responsible and obliged for preparing any information related to the auditing of such evidence and documentation. Such a system should normally include e.g. the following aspects<sup>3</sup>:

- > a description of the relevant products,
- > quality objectives and the organisational structure, responsibilities and powers of the management,
- > corresponding manufacturing, quality control and quality assurance techniques, processes and systematic actions that will be used,
- > quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.

If an audit includes the verification of individual greenhouse gas emission calculations, the requirements specified in ISCC Document 205 “Greenhouse Gas Emissions” must be met.

Audits should be conducted taking into account the principles specified in ISO 19011 (plan, do, check, act) or a justified equivalent. The CB must establish at least a “limited assurance level” when conducting audits. A “limited assurance level” implies a reduction in risk to an acceptable level as the basis for a negative form of expression by the CB such as “based on our assessment nothing has come to our attention to cause us to believe that there are errors in the evidence” (also see ISCC Document 103 “Requirements for Certification Bodies and Auditors”).

*Plan, Do, Check, Act*

If compliance with the ISCC requirements has been verified during the audit, the CB can issue an ISCC certificate. The certificate must be issued not later than 60 calendar days after the audit of the System User registered for certification was conducted. CB’s conducting ISCC audits must comply with the requirements specified in ISCC Document 103 “Requirements for Certification Bodies and Auditors”. The CB is responsible to properly plan, conduct and report on the audit especially with respect to nature, timing and extent of evidence gathering procedures. The audit must be conducted in such a way that a meaningful level of assurance for a decision regarding compliance with the ISCC requirements is available.

*Issuance of the certificate*

An overview on the certification process based on the principles of ISO 19011 is provided in figure 2.

---

<sup>3</sup> Also see: Points 2 and 5.2 of Module D1 (Quality assurance of the production process) of Annex II of the Decision on a common framework for the marketing of products (Decision No 768/2008/EC).

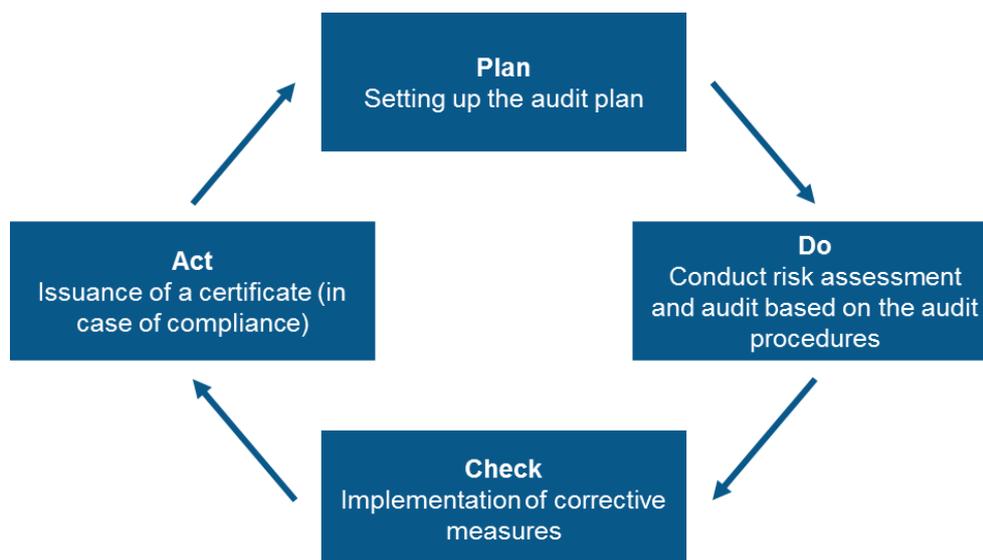


Figure 2: Certification process based on the principles of ISO 19011

Independent of the type of operation participating in ISCC certification, the CB must especially consider the requirements specified in the following documents during each audit to be conducted:

- > ISCC 201 System Basics
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 204 Audit Requirements and Risk Management
- > ISCC 205 Greenhouse Gas Emissions

### 3.2 Audit Procedures and Reports

On the basis of the ISCC system documents, ISCC provides technical (working-) documents to CBs and System Users. These “audit procedures” or “checklists” ensure that all ISCC audits are conducted on the basis of the requirements specified in the ISCC system documents. The audit procedures support the work of the CBs and facilitate a consistent and comparable verification of the ISCC requirements during ISCC audits. CB’s have to use the audit procedures in the latest applicable version provided by ISCC during any ISCC audit. System Users can use the audit procedures to conduct internal assessments, for internal training or to prepare for an audit. The audit procedures include relevant details of the audit including e.g. the length of the audit, the address where the audit was conducted, the audit participants, audited documents as well as information relevant for the certificate (e.g. type of sustainable material, scope of certification).

*Audit procedures  
(checklists)*

The audit procedures may contain relevant data about the amounts of sustainable material handled by System Users. This is necessary to enable ISCC to accumulate reliable information about the total amounts of sustainable material covered by ISCC certification and/or the total cultivation area complying with ISCC requirements. ISCC will treat the information from individual System Users confidential if not required otherwise by law or by

*Data collection  
and reporting*

competent authorities. ISCC is entitled to gather, accumulate and publish such data about the system (in anonymised form), especially in order to fulfil legal reporting obligations. Specific reporting obligations of ISCC are specified in ISCC Document 102 “Governance”. The CB verifies the correctness of such data during the audit and submits the data to ISCC. System users are obliged to provide correct and complete data about the sustainable amounts handled to the CB.

After the audit has been conducted, the CB submits the audit procedures used during the audit to ISCC. In the case of a positive certification decision, the CB is obliged to prepare a report, containing the relevant audit results. This report must be provided to ISCC. The ISCC procedures and the audit report must be submitted together with the certificate issued by the CB. The audit report may be published on the ISCC website. In the event that the external audit showed that the audited System User did not meet the requirements of ISCC, the audit procedures must be submitted to ISCC immediately after termination of the audit. If elements of the supply chain (which are part of a group) were audited non-compliant the CB must send the information of such group members to ISCC.

*Audit procedures  
and report*

### 3.3 Specific Audit Requirements

#### 3.3.1 Farms and Plantations

The CB verifies all requirements relevant and applicable to farms and plantations (in the following only referred to as “farm”), especially those requirements as laid down in this document and in the following documents:

*Relevant system  
documents*

- > ISCC 201 System Basics
- > ISCC 202 Sustainability Requirements
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 205 Greenhouse Gas Emissions
- > ISCC 206 Group Certification

The ISCC Document 202 specifies the six principles for the cultivation of sustainable biomass under ISCC. The requirements of ISCC Principle 1 specify the legal requirements set within the RED and FQD and must always be complied with. Violations of ISCC Principle 1 are critical non-conformities and cannot be subject to corrective measures. ISCC Principles 2 to 6 are comprised of major and minor must requirements. All major must requirements must be complied with in order to be considered compliant with ISCC. Additionally to the major must requirements, at least 60% of the minor must requirements must be complied with. Within EU Member States which have implemented Cross Compliance (CC), farmers that fulfil the criteria through the implementation and official recognition of CC, are only audited with respect to the requirements set out in ISCC Principle 1.

*ISCC  
sustainability  
principles*

A farm is either defined as a distinct legal entity or as an organisation managing an agricultural operation, and having control regarding compliance with the ISCC requirements. The audit of a farm must always cover the entire land (agricultural land, pasture, forest, any other land) of the farm including, any owned, leased or rented land. Biomass produced on land, which is in compliance with the ISCC principles 1 to 6, is considered to be sustainable. Partial compliance (e.g. only fulfilling principle 1 requirements) is not sufficient to declare the biomass produced as sustainable. This means, that the area of the farm relevant for ISCC certification is not limited to such areas where sustainable material is cultivated. Areas that are not fully compliant with ISCC principles 2 to 6 may engage in a continuous improvement process to become fully compliant in a specified time period. This is only possible if compliance with ISCC principle 1 for the entire land of the farm is ensured, the compliant and non-compliant areas can be clearly separated, and a plan for achieving full compliance of those areas does exist. In this case, the partially compliant areas can be treated as separate organisational units. The selection of individual areas of the farm, which comply with the ISCC requirements whereas other areas of the farm may not comply with the requirements (“cherry picking”), is not allowed under ISCC. If the farm audit is conducted on the site of the farm the audit includes an on-site inspection of at least a part of the cultivation area.

*Full compliance  
with ISCC  
sustainability  
requirements*

Farms participating in ISCC are obliged to enable the full assessment and evaluation of all applicable ISCC requirements, including relevant activities which are outsourced to sub-contractors or service providers. Relevant sub-contractors or service providers, e.g. for the application of plant protection products, must be included in the farm audit if this is necessary to evaluate full compliance with ISCC. This should be included appropriately in contractual agreements between the farmer and the relevant sub-contractors and service providers. Contractual agreements must be accessible during the ISCC audit.

*Service  
providers and  
sub-contractors*

Farms are either audited and certified as single entities or as part of a producer group. It is the choice of the farm to decide whether to be audited and certified as a single (individual) entity or as part of a group. The group certification process and rules for sampling are specified in ISCC Document 206. The sample size of farms is driven by the result of the risk assessment (see chapter 4.3). It is the CB’s responsibility to select a representative sample of individual group members for verification of compliance.

*Individual or  
group  
certification*

Farms participating in group certification must conduct a self-assessment and fill in and sign a self-declaration either to the first gathering point or to the central office responsible for the group. On the self-declaration the farmer declares conformity with the ISCC requirements based on the self-assessment. By signing the self-declaration the farmer furthermore gives permission to the CB and to ISCC to verify compliance with the ISCC requirements during an audit. A copy of the self-declaration should be available during the audit. Farms participating in group certification do not

*Self-assessment  
and self-  
declaration*

receive an individual certificate, as they will be covered by the certificate of the first gathering point or the central office of the group. Farms registered for individual certification do not need to sign a self-declaration. In this case, they will receive an individual certificate upon a positive audit.

Farms which are audited non-compliant or which do not agree to participate in an audit must be excluded from ISCC. This is valid until the respective farm based on its own initiative passes a successful ISCC audit. ISCC must be informed by the CB about such farms, which are audited non-compliant or which refuse to be audited as a part of a sample.

*Non-compliance*

### 3.3.2 Point of Origin

The CB verifies all requirements relevant and applicable to the point of origin, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 201-1 Waste and Residues
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 205 Greenhouse Gas Emissions
- > ISCC 206 Group Certification

Points of origin delivering sustainable material under ISCC are obliged to enable an assessment and evaluation of all applicable ISCC requirements to ensure that the material generated is a genuine waste or residue. A major requirement for points of origin to comply with, is to demonstrate that any waste or residue material occurring at their premises is not generated deliberately. The specific requirements for points of origin are specified in ISCC Document 201-1.

*Waste prevention*

Points of origin participating in group certification must fill in and sign a self-declaration either to the collecting point or to the central office. On the self-declaration the point of origin declares conformity with the ISCC requirements. By signing the self-declaration the point of origin furthermore gives permission to the CB or to ISCC to verify compliance with the ISCC requirements during an audit. A copy of the self-declaration should be available during the audit. Points of origin participating in group certification will not receive an individual certificate, as they will be covered by the certificate of the collecting point or the central office. Points of origin registered for individual certification do not need to fill in and sign a self-declaration. They will receive an individual certificate upon a positive audit.

*Self-declaration*

### 3.3.3 Central Office

The CB verifies all requirements relevant and applicable to the central office, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 205 Greenhouse Gas Emissions
- > ISCC 206 Group Certification

The audit of a central office always consists of an audit of the central office itself (head office responsible for the group) and a sample of group members. A central office can either represent a group of farms or a group of points of origin. For the ISCC audit of members of the group, the requirements for farms or for points of origin apply respectively. A list of all farms participating in group certification must be available during the audit and must be submitted to ISCC together with the audit documents. This list must include at least the name and address or location of the individual group members. ISCC is entitled to further specify the information to be provided on the list of farms. ISCC is entitled to require that a list of all points of origin participating in group certification is to be submitted to ISCC including at least the name and address or location of the point of origin. ISCC is entitled to further specify the information to be provided on such a list.

*List of group members*

### 3.3.4 First Gathering Point and Collecting Point

The CB verifies all requirements relevant and applicable to the first gathering point or collecting point, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 201-1 Waste and Residues
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 205 Greenhouse Gas Emissions
- > ISCC 206 Group Certification

All first gathering points and collecting points that want to receive and deliver sustainable material to downstream customers must be certified. Group certification of first gathering points or collecting points is not possible.

*Individual certification*

First gathering points and collecting points must keep all contracts and related documentation about incoming sustainable material received from suppliers, e.g. directly from farms, from points of origin, or from other certified suppliers. Furthermore, they must keep the respective documents for all outgoing deliveries of sustainable material. Material, which is received from farms or from points of origin, complying with the ISCC requirements (having completed and signed the ISCC self-declaration) must be considered as sustainable input. However, the first gathering point or collecting point can choose to sell the sustainable input as non-sustainable. A list of all farms participating in group certification must be available during

*List of suppliers*

the audit and must be submitted to ISCC together with the audit documents. This list must include at least the name and address or location of the individual group members. ISCC is entitled to further specify the information to be provided on the list of farms. ISCC is entitled to require that a list of all points of origin participating in group certification is to be submitted to ISCC including at least the name and address or location of the point of origin. ISCC is entitled to further specify the information to be provided on such a list.

The first gathering point or collecting point is responsible to ensure the traceability of sustainable material back to its origin and to comply with the mass balance requirements under ISCC. A mass balance must be kept for each location where sustainable material is stored on behalf of the first gathering point or collecting point.

*Traceability and mass balance*

Warehouses or collection sites that store sustainable biomass entirely on behalf of a certified first gathering or collecting point are considered as dependent warehouses or collecting points. These are such supply chain elements that do not individually buy biomass from suppliers (farms or points of origin) and sell it to customers in their own name. Such dependent supply chain elements can be covered by the certificate of the first gathering or collecting point. For such entities, sampling can be applied as the overall responsibility regarding the implementation of the ISCC requirements is with the certified first gathering point or collecting point. All warehouses or other storage facilities, which are used by the certified first gathering point or collecting point to store sustainable biomass have to be included in the certification process. A sample must be audited.

*Storage facilities*

It is the responsibility of the first gathering point or collecting point to provide evidence to the CB, which sustainable materials are (or will be) received from farms or from points of origin. Evidence regarding the type of sustainable material can include self-declarations, delivery documentation, or contracts with suppliers. The respective materials will be published on the ISCC certificate.

*Responsibility to provide evidence*

### 3.3.5 Processing Unit

The CB verifies all requirements relevant and applicable to the processing unit, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 205 Greenhouse Gas Emissions

All processing units (e.g. oil mills, oil refineries, biodiesel plants, ethanol plants, or other processing units) that want to deliver sustainable material must be certified individually. Sampling or group certification of processing units is not possible.

*Individual certification*

During the audit of a processing unit the CB must especially verify the traceability and plausibility of the incoming and outgoing amounts of sustainable material as well as the conversion procedure applied within the processing unit. A part of the assessment of the conversion process is the determination of conversion factors describing the relation between sustainable input and sustainable output. It is the responsibility of the processing unit to provide evidence to the CB, which types of sustainable material are (or will be) received and processed at the respective unit. Evidence can include production reports from the previous year, delivery documentation, or contracts with suppliers. The respective materials will be published on the ISCC certificate.

*Traceability and conversion factors*

### 3.3.6 Storage Facilities and Logistic Networks

The CB verifies all requirements relevant and applicable to storage facilities, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 203 Traceability and Chain of Custody

Storage facilities that are used by certified System Users for storing sustainable material must be audited. If the storage facilities belong to a logistic network the logistic centre (head office) plus a sample of the associated storage facilities must be audited. The requirements with respect to traceability and mass balance apply for all storage facilities. In case of a logistic network, the certificate to be issued includes an annex listing all storage facilities covered by the certificate.

*Traceability and mass balance*

During the re-certification audit already audited storage facilities shall not be part of the sample again unless all storage facilities have been audited. A list of all storage facilities participating in group certification must be submitted to ISCC including at least the name and address or location of the storage facility. ISCC is entitled to further specify the information to be provided on the list.

*List of storage facilities*

Operators of storage facilities must enable the CB to verify compliance with the ISCC requirements including granting access to all relevant premises. The CB must at least verify the physical inventory and the related documentation (e.g. weighbridge tickets), the technical equipment (e.g. weighbridge, calibrations, etc.), and the data transfer between the operator of the storage facility and the owner of the sustainable material.

*Ensuring access*

### 3.3.7 Traders

All System Users trading in sustainable material under ISCC must be certified. The CB verifies all requirements relevant and applicable to trading companies, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 203 Traceability and Chain of Custody

Traders are responsible to demonstrate the traceability of the sustainable material and compliance with the chain of custody requirements. During the audit a sample of storage facilities will be audited, which are not certified individually or as a logistic network, if applicable. The audit includes the respective contractual agreements, procedures to transfer information about deliveries and other supporting documents or processes. If a trader uses non-certified storage facilities, it is the responsibility of the trader to enable an on-site verification of the storage facilities.

*Traceability*

The System User is obliged to grant the CB access to the relevant contractual agreements, documenting all transactions related to sustainable material.

*Access to relevant documents*

### 3.3.8 Other Elements of the Supply Chain

Audits may be conducted at other elements of the supply chain that have registered for ISCC certification. Based on the individual type of operation, the CB verifies whether the relevant ISCC requirements are fulfilled, especially those requirements as laid down in this document and in the following documents:

*Relevant system documents*

- > ISCC 201 System Basics
- > ISCC 203 Traceability and Chain of Custody
- > ISCC 205 Greenhouse Gas Emissions

## 3.4 Non-Conformities

### 3.4.1 Definition and General Requirements

Non-conformity means the non-fulfilment of an ISCC requirement by a System User. Non-conformities can be classified according to their impact for the integrity of ISCC. Categories of non-conformities are:

*Definition non-conformity*

- > Minor non-conformities are non-conformities which do not adversely affect the performance, reliability and integrity of ISCC and which can be corrected by a System User after detection
- > Major non-conformities are non-conformities other than critical, which may adversely affect the performance, reliability and integrity of ISCC and which cannot be corrected by a System User after detection. Examples include non-conformities which are related to claims made by the System User during the previous certification period and which therefore have an impact on the downstream supply chain

*Minor*

*Major*

- > Critical non-conformities pose a significant and vital risk to the integrity of ISCC and cannot be corrected. Examples are violations of ISCC Principle 1 and all intentional violations of ISCC requirements (fraud).

*Critical*

There can be supplements, corrections and replacements of documents, records, reports, protocols and other information and data showing compliance with the ISCC principles one to six and with the ISCC traceability, chain of custody and greenhouse gas requirements. This can take place during the audit conducted by the CB or afterwards. However, before an ISCC certificate can be issued all existing non-conformities with mandatory ISCC requirements must be solved. To solve a non-conformity the System User must implement appropriate corrective measures and the CB must verify the implementation and subsequent compliance with all requirements. Corrective measures, e.g. providing missing documents and proofs of compliance to the CB, must be implemented the latest 40 days after the date of the audit of the System User to be certified. If corrective measures are not implemented within 40 days, the issuance of a certificate is not possible and the ISCC audit must be repeated. The audit procedures used during the audit must be submitted to ISCC even if the CB will not issue a certificate due to non-conformities which were not corrected within the respective deadline. Non-conformity with ISCC Principle 1 (No biomass production on land with high biodiversity value, high carbon stock or with a high conservation value) is considered a critical non-conformity and thus cannot be subject of corrective measures. If non-conformity with ISCC Principle 1 has been detected during the audit of a farm, the farm cannot be considered ISCC compliant and must be excluded from ISCC certification.

*Corrective measures*

If non-conformities are detected during an ISCC audit, that relate to claims made by the System User during the previous certification period, ISCC and the CB are entitled to impose conditions for recertification of the System User. Conditions may include the requirement to submit copies of relevant documents for a specific period to ISCC and/or to the CB and that the CB conducts a surveillance audit after a specific period after recertification (e.g. after one mass balance period). This especially applies in case of major non-conformities that have an impact on the downstream supply chain, e.g. non-conformity with the mass balance requirements, non-conformity of Sustainability Declarations (e.g. false information), non-conformity with the greenhouse gas requirements (e.g. incorrectly determined GHG emission value).

*Conditions for recertification*

### 3.4.2 Sanctions

Depending on the type of non-conformity and the individual situation, ISCC may impose sanctions against non-compliant System Users. Sanctions may include the withdrawal of the certificate and the suspension of System Users. The general procedure regarding sanctions in case of non-compliant or fraudulent behaviour of System Users is specified in ISCC Document 102 "Governance".

*Non-conformity during audits*

### 3.4.3 Conflict Resolution

Should any conflicts occur during ISCC audits the principles specified in ISCC Document 102 “Governance” apply.

*Conflicts during audits*

## 4 Risk Management

### 4.1 Definitions, Process and Levels of Application

A risk is the probability of an event happening that may or will have an impact on the mission, the goal or the integrity of ISCC. It is measured in terms of a combination of the probability of the event to occur and its consequences if it does occur.

*Definition risk*

Risk assessment is the process of identifying and evaluating a risk according to its probability to occur and the significance of its consequences. Risk indicators can be used to identify potential risks. A risk indicator is an example describing an event or situation which could possibly pose a risk to ISCC. Once a risk is identified it must be evaluated according to its relevance in the specific situation. The result of the evaluation leads to the classification of the risk. During ISCC audits the risk is evaluated and classified with a risk level (regular, medium, high) and a risk factor (1,0, 1,5, or 2.0).

*Definition risk assessment*

Risk management means the overall 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 in two main steps:

*Definition risk management*

- 1 Risk assessment:
  - > Identification,
  - > Evaluation, and
  - > Classification of risk level and risk factor
- 2 Identification and implementation of appropriate risk control measures

Risk management is relevant on 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. On each level the principles for risk management must be taken into account and applied appropriately.

*Levels of application*

#### 4.1.1 ISCC

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:

*Continuous monitoring*

- > 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 Program, and
- > a continuous internal review of audit documentation submitted to ISCC.

If risks for 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 taken into account.

*Stakeholder involvement*

Furthermore, ISCC promotes new developments, tools and other measures to improve the risk management process. This includes for example the use and application of risk assessment tools e.g. for remote sensing analysis, to assess land use change and other land related sustainability criteria, or databases improving the traceability of sustainable material and the respective sustainability claims and thus reducing the risk of fraud.

*Promotion of risk management tools*

The ISCC Integrity Program is an important tool used by ISCC to continuously identify and analyse potential risks for the ISCC system, the practical application of ISCC by System Users, and the verification by CBs. Within the ISCC Integrity Program, ISCC conducts independent Integrity Assessments to evaluate the performance of CBs 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. The results of the Integrity Program are a basis of ISCC's risk management and are used to improve the quality of the system and to reduce the risk of non-conformity.

*ISCC Integrity Program*

Audit documentation has to be submitted 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 review ensures a consistent application of ISCC and a level playing field for CBs and System Users.

*Internal review*

#### **4.1.2 Certification Bodies**

For CBs cooperating with ISCC risk management focuses on internal processes of the CB as well as on the services the CB provides to System Users (ISCC audits). Internally, CBs should have appropriate risk management procedures in place covering potential risks for the integrity of ISCC which may derive from the activities of the CB. As CBs are conducting ISCC audits for external parties (System Users) CBs must also have an

*Risk management procedures*

internal procedure on how to perform reliable risk assessments for System Users to be certified. The general requirements for CBs are specified in ISCC 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 Program. 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.

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 risk assessment is conducted according to the principles specified in chapter 4.2. Relevant risk indicators applicable to the individual situation must be taken into account for the risk assessment. Based on the CBs professional knowledge and the information submitted by the System User, the CB must especially analyse such risks which could lead to a material misstatement. During the risk assessment for System Users CBs may also investigate ISCC documents or other reliable sources, whether country-specific information is available 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 regarding social or environmental issues relevant for ISCC in the respective region. The result of this investigation must be taken into consideration for the identification and evaluation of a risk and when the audits are planned and conducted.

*Risk assessment during audits*

Depending on the result of the risk assessment the intensity and focus of the audit is determined according to the principles specified in chapter 4.3. This means, the higher the determined risk factor the more thoroughly the audit needs to be conducted to verify and to ensure compliance with ISCC requirements. In case sampling is applied during the audit (group certification), the risk factor determined by the CB drives the sample size of group members to be audited (see ISCC Document 206 “Group Certification”). During audits, the CB should follow a risk-based approach and put a special focus on areas for which the risk assessment has indicated higher risks instead of areas with a lower risk. Furthermore, the CB should take into account the results from previous audits. Depending on the fact-based findings during the audit, the CB is entitled to increase (or reduce) the risk level.

*Sample size and audit intensity*

### **4.1.3 ISCC System Users**

Each System User must start the implementation process of ISCC by conducting an internal risk assessment (self-assessment) in view of potential risks of its activities for the integrity of ISCC. In analogy to the external risk assessment conducted by the CB, the self-assessment can be conducted

*Self-assessment*

based on the principles and risk indicators specified in chapter 4.2. Corresponding to the result of the self-assessment, the System User should design its internal (quality) management system in a way to appropriately address and minimise the identified risks of its activities for the integrity of ISCC.

Prior to the audit of a System User, the CB conducts an independent risk assessment. During this risk assessment the CB should take into account the results of the self-assessment performed by the System User and the design of the System User's management system especially with respect to the identified risks.

*Independent risk assessment*

The risk assessment on the level of System Users focuses on the (internal) processes of the System User and the risk of non-conformity with the applicable ISCC requirements and principles specified in the ISCC system documents.

*Internal processes*

All System Users are obliged to participate in Integrity Assessments scheduled by ISCC in the framework of the ISCC Integrity Program.

*Integrity Program*

## 4.2 Risk Assessment

### 4.2.1 Identification of Risk

The first step during the risk assessment is to identify potential risks by analysing the risk indicators listed in this document. Furthermore, an analysis of the geographic conditions and/or the relevant processes must be conducted. This may require the definition of further risk indicators applicable to the individual situation but not explicitly specified within the ISCC system. A risk assessment may be conducted partially via a desk assessment, e.g. by verifying land use change with satellite data, by analysing biodiversity information in databases, or by searching databases on protected areas. However, a desk assessment requires a verification of the results at the specific location (so-called "ground-truthing"). The risk indicators identified by ISCC form the basis for the risk assessment in the framework of ISCC. They shall be considered during all ISCC audits in order to identify potential risks of non-conformity with the ISCC requirements or for the integrity of ISCC.

*Analysis of risk indicators*

If ISCC audits include the verification of farms, a risk assessment must be conducted to determine the risk of non-conformity with the ISCC sustainability requirements (see ISCC Document 202 "Sustainability Requirements"). Especially the risk of violations of ISCC Principle 1 must be taken into account. This means, it must be assessed if a farm is located within the proximity of areas where the cultivation of biomass is prohibited under ISCC. The risk of non-conformity of farms 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 recognized by the European Commission in the framework of the

*Assessment of farms*

RED and FQD (so-called non-typical voluntary schemes). An example for risk assessment of farms using satellite data is provided in figure 3.



Figure 3: Example of a risk assessment of farms using satellite data (red areas indicate potential land use change after January 2008)<sup>4</sup>

If ISCC audits include waste and residues, the risk assessment must be conducted to determine the risk of false claims and the risk of “intentional” production of waste and residues with the intention to receive special incentives (e.g. double-counting). This means that the focus should be on the verification if a material is a genuine waste or residue, and on the correct and consistent classification and declaration of the material by the point of origin and by the collecting point (see ISCC Document 201-1 “Waste and Residues”).

*Assessment of  
waste or  
residues*

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

*Traceability and  
chain of custody*

<sup>4</sup> Source: GRAS - Global Risk Assessment Services, 2015

With regards to the greenhouse gas emission value of sustainable material, it must be assessed if there is a risk of wrong calculation or false declaration of the emissions (see ISCC Document 205 “Greenhouse Gas Emissions”).

A non-exhaustive overview on significant risk indicators for ISCC is provided in table 1.

General Risk Indicators	Risk Indicators for Farms and Plantations	Risk Indicators for Waste and Residues
<ul style="list-style-type: none"> <li>&gt; Determination, structuring, organisation and documentation of the number of work flows and their complexity (in-house processes)</li> <li>&gt; Number, structuring, organization, expertise, management, involvement and controlling of the subcontractors and external service providers</li> <li>&gt; 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</li> <li>&gt; In-house quality management system, internal audits (structure and documentation)</li> <li>&gt; Transparency (public reporting, involvement of local interest groups, independent audits, social, environmental and economical aspects of sustainability)</li> <li>&gt; Mechanisms for conflict resolution established independently, documented and implemented</li> <li>&gt; Management of conflicts of interests and corruption prevention</li> <li>&gt; Risk of corruption and fraud (e.g. according to OECD list, Transparency International Corruption Perceptions Index, etc.) – i.e. how</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Proximity to and/or overlap with no-go areas (forest land, peatland, wetlands, highly biodiverse grassland, etc.)</li> <li>&gt; Land conversion shortly before or after January 1st 2008</li> <li>&gt; Factors influencing significantly the output per acreage and the output per ha.</li> <li>&gt; Employment of migrant workers</li> <li>&gt; Ratification and degree of implementation of ILO core labour standards.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Type of point of origin (e.g. restaurant, processing plant, landfill, etc.)</li> <li>&gt; 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)</li> <li>&gt; Status of the material (genuine waste/residue) and acceptance or recognition by relevant authorities</li> <li>&gt; Declaration or labelling of the material (e.g. according to official waste catalogues or waste codes)</li> <li>&gt; Risk of intentional “production” of waste or residues</li> <li>&gt; Risk of intentional modification of products to be declared or claimed as waste or residues</li> </ul>

General Risk Indicators	Risk Indicators for Farms and Plantations	Risk Indicators for Waste and Residues
<p>serious is the external risk of corruption and how does this influence the implementation</p> <ul style="list-style-type: none"> <li>&gt; Yield or conversion factors in internal processes</li> <li>&gt; Certification history, including previous or current ISCC certification as well as certification under other sustainability certification systems, especially those recognized by the European Commission within the framework of the RED and FQD</li> <li>&gt; Frequency of changes in certification system (so-called “scheme hopping”)</li> <li>&gt; Accuracy of records and documents</li> <li>&gt; Degree of topicality, updating frequency of records and documents</li> <li>&gt; Accessibility of records and documents</li> <li>&gt; Completeness of records and documents</li> <li>&gt; Individual calculation of GHG emissions</li> <li>&gt; Risk of single consignments (batches) being claimed more than once (so-called “double-accounting”)</li> </ul>		

Table 1: Overview on typical risk indicators

#### 4.2.2 Evaluation of Risk

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:

- > Sources and reasons of the risk
- > Identification of potential consequences from the risk if it would occur, the impact (e.g. negligible, moderate, critical) and the probability of its occurrence (e.g. unlikely, occasional, likely)
- > Factors influencing the consequences and the probability of the risk to occur

*Aspects for evaluation and classification*

- > Differing importance or emphasis of the risk by different stakeholders

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

*Risk levels and factors*

- > Regular (risk factor 1,0)
- > Medium (risk factor 1,5)
- > High (risk factor 2,0)

A risk assessment matrix may be used to facilitate the classification of the risk (see example in table 2).

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

Table 2: Example of a risk assessment matrix

With respect to the evaluation of the risk on farm level, the principles and requirements specified in ISCC Document 202 “Sustainability Requirements” must be considered. Especially the differentiation between “major must” and “minor must” criteria should be taken into account for the evaluation and classification of a risk. Relevant risks on farm level include:

*ISCC sustainability principles*

- > 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).

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

*Documentation*

- > 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 for non-conformity with traceability requirements can e.g. be considered to be regular, if 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, i.e. files are missing, files are not accessible, files are not disclosed, or if there is indication for non-conformity or fraud the risk should be classified as high.

Specific indication of non-conformity with ISCC requirements must be taken into account appropriately 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 risk level must be applied during the audit. This especially applies in case of non-conformities that have an impact on the downstream supply chain, e.g. non-conformity with the mass balance requirements, non-conformity of sustainability declarations (e.g. false information), non-conformity with the greenhouse gas requirements (e.g. incorrectly determined GHG emission value). In this case a high risk classification must also be applied during the subsequent recertification audit of the respective System User.

*Non-conformity*

It is up to the CB's judgement to discontinue the audit if the risk is ranked high and if either the documentation is not easily accessible or the amount of unavailable documentation does not allow for a 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.

*Adjustment of risk level*

### 4.3 Identification and Implementation of Risk Control Measures

After the risk is identified and evaluated it must be managed properly to ensure that the probability of non-conformity with ISCC requirements is continuously minimized. This is done by applying the following elements:

*Elements of risk control*

- > Adjusting the intensity of audits to adequately take into account the risk. In case of group certification 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, in particular with regards to
  - > Specification of responsibilities
  - > Training of employees

- > Documentation
- > Duty to report (including reporting and submitting documents to the CB or to ISCC)
- > Internal auditing and management system
- > Extending the definition of risk factors for certain areas by ISCC

If the audit includes sampling of third party locations, i.e. farms, points of origin or (dependent) 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 (see ISCC Document 206 “Group Certification”). In case of non-conformity of individual group members, the determined sample size (s) of the current audit must be doubled.

*Adjustment of sample size*

If the audit includes chain of custody verification, i.e. traceability and plausibility of amounts, the risk factor drives the intensity of the audit with respect to documentation to be verified. The entire documentation relevant for ISCC for a complete year must be available during an ISCC audit in order to evaluate the mass balance calculation and allow for plausibility checks between company reporting and mass balance results. However, it is (usually) not required that the CB verifies every single document (e.g. weighbridge tickets, Sustainability Declarations, contracts, etc.) of an entire year. Instead, the CB is entitled and must be able to take random 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. Following guidelines can be applied:

*Verification intensity of documents*

- > 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.