ISCC EU 204
RISK MANAGEMENT

Document Title: ISCC EU 204 Risk Management

Version 4.0

Valid from: 1st July 2021

Note: From 1st July 2021, only the version 4.0 of this ISCC document is applicable. This version of the document has been submitted to the European Commission in the framework of the recognition process of ISCC EU under the legal requirements of the Renewable Energy Directive (EU) 2018/2001 (RED II). The recognition of ISCC EU in the framework of the RED II is pending. This ISCC document may be subject to change depending on further legislation and further requirements of the European Commission.

Content

Summary of Changes

The following is a summary of the mainchanges to the previous version of the document (ISCC EU Document 204 v 3.0). The revision of the document is a major review in the framework of the rerecognition of ISCC under the Directive (EU) 2018/2001 (recast) (RED II). Minor amendments, e.g. corrections of phrasings and spelling mistakes, are not listed.

Summary of changes made in version 4.0	Chapter
General: The title of the document was adjusted to "Risk Management" from "Audit Requirements and Risk Management". The contents of the previous chapter 3 covering the audit requirements have been included in other ISCC Documents (mainly in ISCC EU System Documents 201 "System Basics" and 203 "Traceability and Chain of Custody")	
General: All reference to the RED refer to the Renewable Energy Directive (EU) 2018/2001 (recast) (also referred to as RED II)	
Addition: *"The use of the Audit Procedure System (APS) is mandatory for CBs and auditors. This system reduces the possibility of human errors and automates the detection of implausibilities within the audit report and the preparation of final audit reports and Summary Audit Reports. The use of the conventional audit procedures (in Word) is only possible in exceptional cases (e.g. severe problems with IT components, system breakdowns, etc.) or in case of new procedures not already integrated into APS."*	3.1.1
Addition*: "Non-cooperation in the Integrity Programme is regarded as a critical non-conformity and sanctioned accordingly"*	3.1.3
Adjustment: A risk assessment may be conducted *remotely* via a desk assessment	3.2.1
Addition: 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 doing (web-based) research on social and environmental issues".*	3.2.1
Addition: 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 "*and have to be supplemented by further risk indicators if required to properly assess the individual set-up of a System User".*	3.2.1
Addition: "*If in the framework of the risk assessment and audit it could be established that land use change (LUC) took place after January 1st2008, the CB has to provide a detailed explanation on how the compliance with ISCC Principle 1 was verified. 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). This information has to be submitted to ISCC by the CB together with other relevant certification documents."*	3.2.1
Addition: Yield or conversion factors in internal processes, "*especially if several products with different conversion factors are processed"*	3.2.1
Addition*:* 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, withdrawn or suspended certificates under the schemes mentioned above"*	3.2.1
Addition: "*Frequency of changes of the certification body conducting audits under ISCC"*	3.2.1
Addition: Risk of intentional modification "*or contamination"* of products to be declared or claimed as waste or residues	3.2.1

Summary of changes made in version 4.0	Chapter
Addition: Paragraph on higher risk in case of frequent change of CB	3.2.2
Addition: Paragraph on higher risk after suspension and withdrawal of certificate	3.2.2

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 Renewable Energy Directive (EU) 2018/2001 (recast) (often referred to as RED II)[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 takes into account the best practice principles of the ISEAL "Code of Good Practice for Assuring Compliance with Social and Environmental Standards". 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

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 assessment

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

[1] *Directive (EU) 2018/2001 on the promotion of the use of energy from renewable sources (recast), in the following referred to as RED II*

risk. In the framework of ISCC audits the risk is evaluated and classified with a risk level (regular, medium or high) and a risk factor (1.0, 1.5, or 2.0).

Definition risk management

Risk management means the enitre 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:

1 Risk assessment:

  > Identification,

  > Evaluation, and

  > Classification of risk level and risk factor

2 Identification and implementation of appropriate risk control measures

Levels of application

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.

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 taken into account.

Promotion of risk management tools

Furthermore, ISCC promotes new developments, tools and other measures to improve the risk management process. This includes the 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. The use of the Audit Procedure System (APS) is mandatory for CBs and auditors. This system reduces the possibility of human errors and automates the detection of implausibilities within the audit report and the preparation of final audit reports and Summary Audit Reports. The use of the conventional audit procedures (in Word) is only possible in exceptional cases (e.g. severe problems with IT components, system breakdowns, etc.) or in case of new procedures not already 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 has to 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 and a level playing field for CBs and System Users. See ISCC EU Documents 102 "Governance" and 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 on the CB's internal processes 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 conduct ISCC audits for external parties (System Users) CBs must also 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 risk assessment is conducted according to the principles specified in chapter 3.2. 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 should pay particular attention to 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 and should check 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 certification in the respective region. The result of this investigation must be taken into consideration for the identification and evaluation of risks and for deciding when audits are planned and conducted.

Sample size and audit intensity

Depending on the result of the risk assessment the intensity and focus of the audit is determined according to the principles specified in chapter 3.3. This means that the higher the determined risk factor the more thoroughly the audit needs to be conducted to verify and ensure compliance with ISCC requirements. If 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 EU System Document 203 “Traceability and Chain of Custody”). During audits, the CB has to 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 has to take into account the results of previous audits. Depending on the fact-based findings during the audit, the CB is entitled to increase (or reduce) the risk level.

3.1.3 ISCC System Users

Self-assessment

Each System User must start the implementation process of ISCC by conducting an internal risk assessment (self-assessment) with regard to potential risks its activities could have for the integrity of ISCC. Analagous 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. Based on 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 its activities could have for the integrity of ISCC.

Independent risk assessment

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, in particular with respect to the risks identified.

Internal processes

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.

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 in the Integrity Programme is regarded as a criticial 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 below). The risk indicators identified 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 and have to be supplemented by further risk indicators if required to properly assess the individual set-up of a System User.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 that are not explicitly specified within the ISCC system. 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 in order 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 especially important that the risk of violations of ISCC Principle 1 are taken into account. 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 II (so-called non-typical voluntary schemes). An example for risk assessment of farms/plantations/forests using satellite data is provided in figure 1.

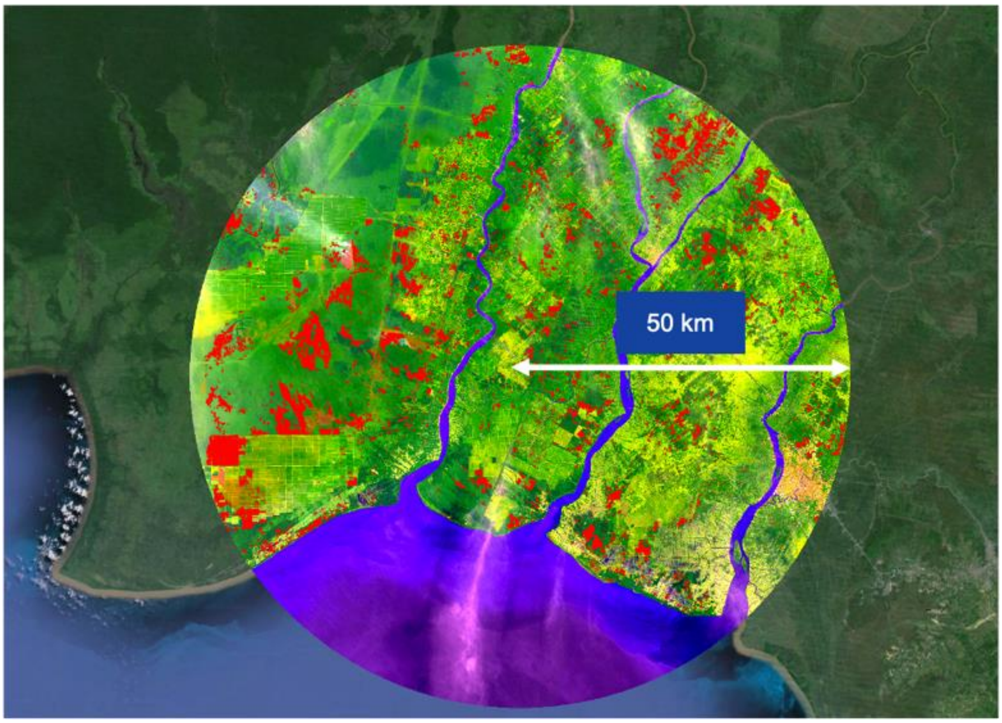


Figure 1: Example of a risk assessment of farms/plantations/forests using satellite data (red areas indicate potential land use change in an area after January 2008)[2]

Land use change after January 2008

If in the framework of the risk assessment and audit it could be established that land use change (LUC) took place after January 1st 2008, the CB has to provide to ISCC a detailed explanation on how compliance with ISCC Principle 1 was verified. 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 (e.g. double-counting). 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 (i.e. whether a 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-sustainable material is sold or delivered as being sustainable and if the requirements on mass balance are complied with.

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

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 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”).

Table 1 provides examples of general risk indicators, examples for land-related risk indicators for production areas (farms/plantations or forests) and for waste and residues:

General risk indicators

General risk indicators include but are not limited to:

- Determination, structuring, organisation and documentation of the number of workflows and their complexity (in-house processes)
- Number, structuring, organisation, expertise, management, involvement and monitoring of subcontractors and external service providers
- Number and structuring of the workflows that are carried out by subcontractors compared to the ones that are carried out by permanent in-house staff
- In-house quality management system, internal audits (structure and documentation)
- Transparency (public reporting, involvement of local interest groups, independent audits, social, environmental and economic aspects of sustainability)
- Mechanisms for conflict resolution established independently, documented and implemented
- Management of conflicts of interests and prevention of corruption
- Risk of corruption and fraud (e.g. according to OECD list, Transparency International Corruption Perceptions Index, etc.), i.e. how serious is the external risk of corruption and how does this influence implementation
- Yield or conversion factors in internal processes, especially if several products with different conversion factors are processed
- Individual calculation of GHG emissions
- 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 “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 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

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 (e.g. double-counting)
- Declaration or labelling of the material (e.g. according to official waste catalogues or waste codes)
- Risk of intentional “production” of waste or residues
- Risk of intentional modification or contamination of products to be declared or claimed as waste or residues

3.2.2 Evaluation of Risk

Aspects for evaluation and classification

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

- Sources and causes 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
- Differing perceptions of the importance of or emphasis on the risk by different stakeholders

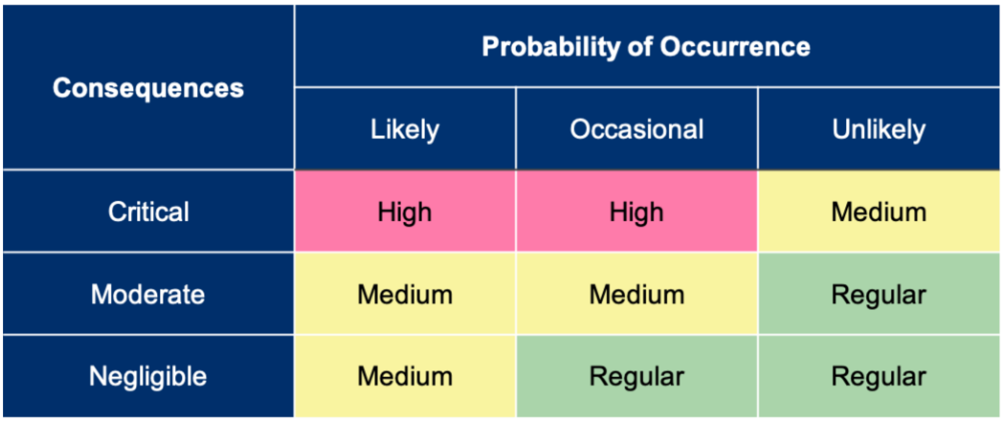
Risk levels and factors

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 sustainability principles

With respect to the evaluation of the risk on farm/plantation level, the principles and requirements specified in ISCC EU System Documents 202-1 “Agricultural Biomass – ISCC Principle 1” and 202-2 “Agricultural Biomass – ISCC Principle 2-6” must be considered. Relevant risks on farm/plantation 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, i.e. 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.

Specific indication of non-conformity with ISCC requirements must be taken into account during the risk evaluation and classification.

Non-conformity

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 must be applied during the audit. This especially applies if those non-conformities 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 level must also be applied during the subsequent recertification audit of the respective System User.

Adjustment of risk level

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.

Higher risk in case of frequent changes of CB

System Users are free to choose any of the certification bodies recognised by ISCC to perform ISCC audits, and may also change which CB they have a contract with. 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" (i.e. 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, i.e. 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 withdrawal of a certificate or a period of suspension the CB has to apply a higher risk level, i.e. 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 and evaluated it must be managed properly to ensure that the probability of non-conformity with ISCC requirements is continuously minimised. This is done by applying the following measures:

> Adjusting the intensity of audits to adequately take into account 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, 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

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 (s) of the current audit must be doubled.

Verification intensity of documents

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 the documentation that needs to be verified. All 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 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 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.