RSPO | Roundtable on Sustainable Palm Oil

CONTINGENCY RSPO AUDIT PROCEDURE FOR SUPPLY CHAIN STANDARD

Version 2

This procedure is only applicable when a force majeure event prevents the audit team from conducting site verifications.

Document Title	:	Contingency RSPO Audit Procedure for Supply Chain Standard (V2)
Document Code	:	RSPO-PRO-T00-006 V2 ENG
Scope	:	International
Document Type	:	Procedure
Approval	:	Approved by the Assurance Standing Committee on 19/05/2022
Contact	:	RSPO Certification Unit, certification@rspo.org

Table of Contents

List of Acronyms

AB	Accreditation Body
CB	Certification Body
CH	Certificate Holder
CSPO	Certified Sustainable Palm Oil
ICT	Information Communication Technology
P&C	Principles and Criteria
RSPO	Roundtable on Sustainable Palm Oil
SCC	Supply Chain Certification
UoC	Unit of Certification

Glossary

Remote Audit

Assessment of a Certificate Holder (CH) conducted by the accredited Certification Body (CB) in full or in part using electronic means and does not take place at the physical location of the unit that is being certified. A remote audit can also be defined as an audit of an organisation that is not conducted on-site. Remote audits may include offline activities when there is limited connectivity (e.g. document review) or real-time virtual approaches (e.g. video calls), or a combination thereof.

Feasible

A conclusion made by the CB based on the result of the risk evaluation related to the possibility of implementing the audit options easily or conveniently.

Situational Risk Evaluation

A situational risk evaluation is a process to identify possible risks/threats and measure the risk level to determine the appropriate options to conduct RSPO Supply Chain Certification (SCC) audits.

Force Majeure

Situation such as war, riots, fire, flood, hurricane, typhoon, earthquake, lightning, explosion, strikes, lockouts, slowdowns, pandemics that prevents the audit team from conducting site verifications.

Travel Restrictions

A situation that has been imposed to prevent people from travelling somewhere and/or from entering a particular area in a state of force majeure.

Introduction

The Roundtable on Sustainable Palm Oil (RSPO) Secretariat has been working closely with RSPO members, Certification Bodies (CBs), and the Accreditation Body (AB) to identify ways to ensure that RSPO standards remain credible, and that the absence of on-site audits do not negatively impact our ability to uphold the high level of assurance that is expected from the RSPO Certification Systems despite the COVID-19 pandemic that has challenged many countries and regions; and the travel restrictions or tight quarantine procedures which imposed by the authorities.

In March 2020, the RSPO Secretariat released an announcement, "***Covid-19 - How we're adapting for RSPO certification audits***" (link **here**) to all its accredited CBs on the conduct of audits against the 2018 RSPO Principles and Criteria (P&C) and 2020 RSPO Supply Chain Certification (SCC) Standard. Further to that, on 25 August 2020, the Secretariat introduced the ***Contingency RSPO Audit Procedure V1***, as a guide for CBs to manage and maintain the status of their certificate holders during the pandemic.

Contingency RSPO Audit Procedure V1

> *"The CBs are allowed to make the decision as to whether an on-site or remote audit is to be conducted for their RSPO supply chain certified clients. If a remote audit is carried out, the CBs need to maintain relevant evidence that demonstrates that they were prevented from conducting the on-site audit. This provision covers the Initial Certification, Annual Surveillance or Recertification audits. The PalmTrace licence for SCC is only allowed to be extended for a maximum of 3-months. Licence extension shall be requested prior to the expiry of the PalmTrace licence and can be done so if a need is determined by the CB."*

Source: Contingency RSPO Audit Procedure V1 (25 August 2020).

The RSPO Secretariat has agreed to revise and replace the previous ***Contingency RSPO Audit Procedure V1*** with this version, which is to be used by all RSPO accredited CBs and Units of Certification (UoC) when conducting RSPO Supply Chain Certification Standard audits in a situation of force majeure, which prevented the audit team from conducting an on-site audit.

OPTIONS TO CONDUCT CONTINGENCY RSPO AUDIT PROCEDURE FOR SUPPLY CHAIN STANDARD AUDITS DURING FORCE MAJEURE

This version introduces only two (2) options for the CB to conduct an RSPO SCC audit to maintain the credibility and high level of assurance associated with RSPO SC certification and the accuracy of information obtained by the RSPO Secretariat, CBs, and AB:

Options to Conduct Contingency RSPO Audit Procedure for Supply Chain Standard Audits during Force Majeure

Option	**Explanation**
Option A: On-Site Audit	Audits are carried out on-site by the CB's lead auditor
Option B: Remote Audit	Audit was fully conducted remotely by the CB's lead auditor

Applicability of Contingency RSPO Audit Procedure for Supply Chain Standard

This procedure is only applicable during force majeure events. CBs must retain all related evidence of security warnings or instructions from authorities, companies, and/ or any other form of evidence deeming it to be high risk for lead auditors and company staffs, in order to justify cases why an on-site audit is not possible. All evidence must be retained for at least five (5) years or one (1) certification cycle.

This procedure is effective for the implementation by the CBs and the CH on 1st September 2022. All requirements in the RSPO Supply Chain Certification Systems and Standard remain unchanged unless stated otherwise in this document.

As soon as travel restrictions/bans have been lifted by the relevant authorities, and/or when the risk is reduced (as defined by the result of the CBs' Risk Evaluation), and/or when there is no force majeure situation, RSPO audits shall be conducted as per the RSPO Supply Chain Certification Systems and Standard.

This procedure will be treated as part of the RSPO Supply Chain Certification Systems, which will be used by AB, CB, CH, and organisations seeking RSPO Supply Chain Certification in the event of a force majeure. The RSPO Secretariat reserves the right to randomly select any audit reports that have been conducted based on Option B for independent review, as part of the process to ensure integrity and adequacy of the coverage during the implementation of this procedure. The RSPO Secretariat has developed a simplified process flow as a guidance for the CBs to evaluate and decide on the appropriate audit option in Annex 1 of this document (Option A or Option B).

In the event of any force majeure, the CB shall comply with the following elements:

1. **Situational Risk Evaluation by the CBs**

   The CBs are responsible for conducting Risk Evaluations of contextual and business-specific risks in order to select the audit option that is feasible for the Unit of Certification (UoC) to conduct the RSPO SCC audit (i.e., Option A, Option B). The CBs' risk evaluation results shall be discussed with the CH, and both parties must agree on the conclusion and justification.

   Elements that should be considered when performing the risk evaluation include, but are not limited to, the following:

   a) Risk Evaluation for On-Site Audit

      - Any force majeure situation that may put the health and safety of the CB's audit team members, auditees and/or company staff at risk.
      - Any travel restriction and/or warnings imposed by the authority, CBs and/or CH that prevents the CB's qualified audit team from conducting an on-site audit at the UoC (e.g., travel restriction and/or warnings by locality, district, state, country, embassy; the use of paramilitary/tsunami/flood/hurricane alert/warning/advisory)
      - Possibility to implement health and safety protocols during travelling and execution of the on-site audit (e.g., crowd control, engineering modification, safe operating procedures, etc.)
      - Availability of the CB's audit team to travel for on-site audits
      - For COVID-19 pandemic specific case:
        - ➢ The number of new and active recorded COVID-19 cases (beyond isolated cases) within the last 14 days of the risk evaluation date in the place of departure and arrival (e.g., from the CB's premises to the UoC).
        - ➢ The number of new and active COVID-19 cases recorded within the UoC, its surrounding area, and/or among the audit team members for the past 14 days.
        - ➢ Vaccination status of the auditee and audit team. (Note: In case of a situation whereby the vaccination rate within the UoC is less than 80%, the CB should define whether an on-site audit is practical, or whether the CB can choose to implement effective measures before going on-site.)

      If the result of risk evaluation for on-site auditing is FEASIBLE, but the risk is high, the CB and CH should discuss and agree on relevant control measures to mitigate the risk level during the on-site audit. The CB should also have an internal system in place to respect the individual lead auditor's right to accept or decline the assigned on-site audit.

b) Risk Evaluation for Remote Audit

When the result for risk evaluation for on-site audit indicates that Option A is not feasible, the following factors need to be considered by the CB to evaluate the risk evaluation for remote audit (refer to Annex 1 of this document).

- The justification and agreement by the CB and CH stating that the on-site audit is not feasible are documented.
- Availability of sufficient resources and tools (e.g., Internet connection, mobile network coverage, hardware, software, competence personnel, etc.) among the CB's audit team, UoC, and other stakeholders to facilitate the information gathering and feedback collection during the remote audit.
- The possibility to make the necessary tools for remote auditing available (e.g., representative may be able to facilitate access for video calls/communications with the relevant parties).
- No ongoing formal complaint/legal cases related to the UoC.

After taking into account, at a minimum, all of the risk elements listed above and determining that remote audits (Option B) is FEASIBLE, the justification must be documented and properly maintained, and the remote audits may proceed accordingly.

In the event that the CB observes that the risk is decreasing, and on-site audit seems feasible, the risk evaluation may be required to be repeated within 21 days prior to the agreed audit date to confirm whether the decision to proceed with the remote audit is still applicable or not. The risk evaluation result shall be reviewed by the CB and agreed upon by both the CB and CH.

2. Auditing RSPO SCC Requirements Remotely

The RSPO Secretariat has identified the expected outcome, at a minimum, for RSPO SCC standard requirements from the audit exercise as presented in the RSPO Supply Chain Certification Standard 2020 Audit Checklist, which can be found on the **RSPO website**.

This audit checklist will only serve as a guide for the CBs during the audit and is not limited to the information provided in the document. For the requirements that are audited remotely, the CB should be able to:

- Define a suitable audit methodology for the lead auditor to gather objective evidence.
- Identify what data is usually collected for the specific requirements during an on-site audit.
- Determine how this information will be obtained and presented through remote alternative means of gathering that data or be able to gain the same objective evidence and insight.

3. Resource Requirement

a) Lead Auditor Training and Qualification to Conduct RSPO SCC Remote Audit

The CB shall establish a mechanism (e.g., training, competency evaluation) to ensure that the competencies of all lead auditors and/or team members (including subcontractors, technical experts, and translators) who will participate in the remote audit are evaluated and recorded, to confirm they have the necessary skills to conduct and deliver the remote audit. Training content should at least include areas related to any changes in audit preparation, planning, use of ICT platform, and execution required for remote audits.

b) Translators

In case the CBs require the support or assistance of a translator during the remote audit, the CB shall ensure that:

- the translator is independent from the organisation being assessed, as stated in the RSPO Supply Chain Certification Systems.
- the name of the translator is included in an audit report.
- the translator is trained in confidentiality management.
- the translator is trained in remote audit procedure/guidelines including the use of ICT platforms (e.g., facilitating conversations through the remote audit).

c) Technical Expert

Similarly, in case the CBs require the support or assistance of a technical expert during the remote audit, the CB shall ensure that:

- the technical expert is independent from the organisation being assessed, as stated in the RSPO Supply Chain Certification Systems.
- the name of the technical expert is included in an audit report.
- the technical expert is trained in confidentiality management.
- the technical expert is trained in remote audit procedure/guidelines including the use of ICT platforms (e.g., facilitating conversations through the remote audit).
- the technical expert is trained by the CB on the RSPO Supply Chain Certification Standard.
- the qualification process of the technical experts complies with the RSPO Supply Chain Certification Systems.

4. RSPO SCC On-Site Audit Process (Option A)

Aside from the Situational Risk Evaluation of the On-Site Audit, the detailed activity of the audit (planning, opening, closing, etc.) shall be conducted following the RSPO Supply Chain Certification Systems.

When the CBs define the risk for on-site audit as FEASIBLE, the justification and agreement shall be documented and properly maintained, and the CBs may proceed with the on-site audits accordingly.

5. RSPO SCC Remote Audit Process (Option B)

a) Planning for Remote Audit

The remote audit requires greater planning and coordination between both parties (the CB and the CH). Both parties should collaborate during the planning to ensure the remote audit can be done smoothly. The planning should consider, among others, the following factors:

- Availability of sufficient resources and tools (i.e., Internet connection, mobile network coverage, hardware, software, competence personnel, etc.) among the audit team, unit of certification (auditee), and other stakeholders to facilitate information and feedback gathering during the remote audit.
- Methodology for the documentation/information sharing platform to access data and/or information during the remote audit. This should include the available options to conduct interviews with staffs and stakeholders.
- Data protection policies should be in place and complied with by all parties.
- A test session for the CB lead auditor and auditee (including stakeholders) is conducted, in order to familiarise themselves with the available Information Communications Technology

(ICT) tools that will be used in the remote audits. A contingency plan must be in place should the technology fail.

- Flexibility and adaptability of lead auditors and auditees, given the risk of misunderstanding with the use of virtual communications tools.
- Definition of the agenda and accommodating dispositions different from an on-site audit (i.e., clear definition of tasks by different team members).

b) Documentation Sharing and Communication Platform for Remote Audit

The CB and CH should discuss and agree on the most feasible documentation and information sharing platform (e.g., Google Drive, One Drive, iCloud, etc.), including available ICT options, to facilitate the remote audit (e.g. Zoom, Microsoft Teams, Google Meet, WhatsApp, Telegram, mobile phone, email).

The type and range of evidence to be shared by the CH will depend on whether the remote audit involves a video call or a phone call, and/or the other available relevant verification options agreed upon by the CB.

It is the CBs' responsibility to ensure the information shared by the CHs are only accessible to the audit team and that data protection rights are maintained and agreed upon by both parties. Any one-on-one conversation during the remote audit should be encrypted (where possible).

The CH should be responsible for advising the audit team on any document that is strictly confidential and not meant to be shared, however, the documents must be made available to the audit team as and when required.

Where there is a limitation of documentation/information sharing (including video, photography, etc.) by law, the CB and the CH shall sign a form to gather approval prior to any verification since this documentation/information may be seen by third parties, i.e., ASI assessors.

c) Execution of the Remote Audit

The remote audit shall include a live visual feed (with live video and audio capabilities), which must be portable around the site, including in the site operation and other facilities. This is to ensure that the CB can observe relevant procedures, compliance, and facilities, and obtain feedback from relevant staff/stakeholders.

In cases where there are limitations and/or no connectivity at the audited site, at the discretion of the CB, photographic and recorded video of several areas and facilities (as deemed required by the lead auditor and audit team) can be considered as evidence sharing as a means of verification during the remote audit. However, all the pre-recorded videos and images shall have clear geotagging information, date, and timestamp for verification by the CB. In this case, the CB shall maintain live communication with the auditee and/or their representative at an alternate location with good Internet connectivity (e.g., head office, regional office, site office) throughout the remote audit process. The use of technology, as required, should ensure that adequate controls are in place to avoid abuses that could compromise the integrity of the audit process.

d) Gathering Information from Staffs and/or Stakeholders during a Remote Audit

Gathering information from staff and/or stakeholders is the most challenging aspect when the audit is conducted remotely. To ensure the smooth process of gathering information or feedback from staff and/or stakeholders during the remote audit, the CB shall have a documented procedure that demonstrates a proactive approach to ensure the inputs are recorded during the remote audit.

The CB shall, at a minimum, establish a documented procedure and guidelines, as well as steps to ensure the integrity and confidentiality of information gathered from staffs and/or stakeholders (e.g., through interviews or other communication platforms), and avoid compromising the safety of the staffs and/or stakeholders (e.g., threats of dismissal, death, rights, etc.).

e) Audit Duration for Remote Audit

Conducting audits remotely can be very challenging and uncertain, given issues such as connectivity challenges, proper information-sharing platforms, familiarity with ICT platforms, time zone differences, etc.).

Therefore, the CB should have a documented procedure to identify appropriate man-days to cover the remote audit activities, which might differ from in-person audits, with more time allocated on audit planning and a potentially longer overall duration for the remote audit.

The key is to allocate the audit effort (hours) differently, focusing more on the preparatory steps and enabling a more focused interaction with the CH. If a remote audit requires much more time than a traditional audit, this should be considered in the initial risk evaluations and justified by the CB.

f) Certification Decision Making for Remote Audit

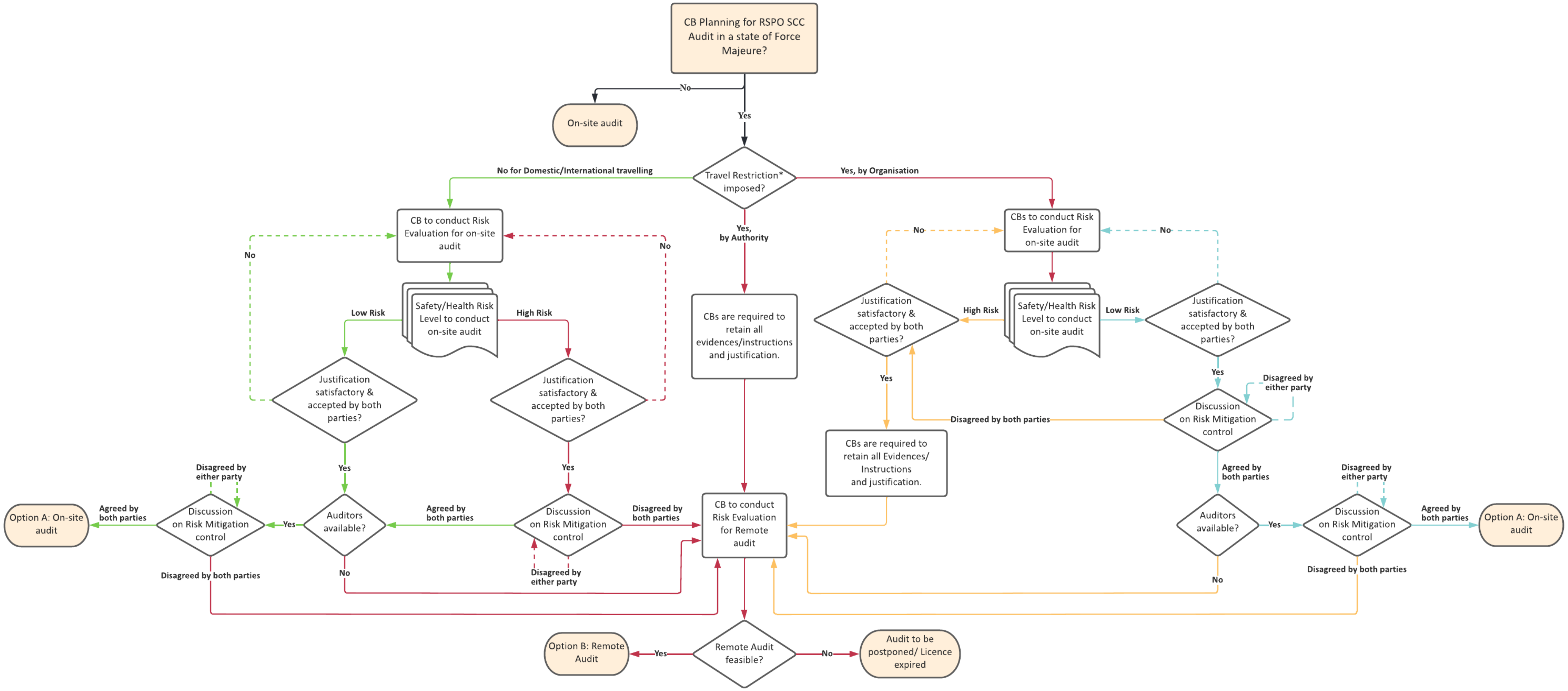
The CB shall then follow their internal procedure on certification decision making based on the results obtained through the remote audit and recommendation from the lead auditor. This should also be consistent with the RSPO Supply Chain Certification Systems.

g) Audit Reporting for Remote Audit

The CB shall provide an audit report that fulfils all the requirements listed in Annex 1 of the RSPO Supply Chain Certification Systems, and include additional information related to the audit methodology, data gathering platform, sampling, etc. This can also include records such as how CHs' operations have been impacted during a force majeure situation.

As the nature and format of data and information collected during the remote audit are likely to be quite different from the traditional audit process, consideration should be given by the CB on how additional information will be recorded and reported, as well as any implications for data privacy and confidentiality.

Annex 1 - CB Planning for RSPO SCC Audit during Force Majeure Flowchart


CB Planning for RSPO SCC Audit in a state of Force Majeure?
No
On-site audit
Yes
Travel Restriction* imposed?
No for Domestic/International travelling
Yes, by Organisation
Yes, by Authority
CB to conduct Risk Evaluation for on-site audit
No
No
Safety/Health Risk Level to conduct on-site audit
Low Risk
High Risk
Justification satisfactory & accepted by both parties?
Justification satisfactory & accepted by both parties?
Yes
Yes
Auditors available?
Discussion on Risk Mitigation control
Disagreed by either party
Agreed by both parties
Option A: On-site audit
Yes
Disagreed by both parties
No
Agreed by both parties
Discussion on Risk Mitigation control
Disagreed by both parties
Disagreed by either party
CBs are required to retain all evidences/instructions and justification.
CB to conduct Risk Evaluation for Remote audit
Remote Audit feasible?
Yes
Option B: Remote Audit
No
Audit to be postponed/ Licence expired
CBs to conduct Risk Evaluation for on-site audit
No
No
Safety/Health Risk Level to conduct on-site audit
High Risk
Low Risk
Justification satisfactory & accepted by both parties?
Justification satisfactory & accepted by both parties?
Yes
Yes
CBs are required to retain all Evidences/ Instructions and justification.
Disagreed by both parties
Discussion on Risk Mitigation control
Disagreed by either party
Agreed by both parties
Auditors available?
No
Yes
Discussion on Risk Mitigation control
Disagreed by either party
Agreed by both parties
Option A: On-site audit
Disagreed by both parties

*A situation that has been imposed to prevent people from travelling somewhere and/or from entering a particular area in a state of force majeure.

Reference Documents

1. IAF ID 3: 2011 - IAF Informative Document for Management of Extraordinary Events or Circumstances Affecting ABs, CABs and Certified Organizations
2. IAF ID 12: 2015 - Principles on Remote Assessment
3. IAF MD 4: 2018 - IAF Mandatory Document for The Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes
4. IAF MD 5: 2019 - Determination of Audit Time of Quality, Environmental and Occupational Health & Safety Management Systems
5. ISEAL Guide on Using Technology and Data to Enable and Enhance Remote Audits, 2021
6. ISO 9001 Auditing Practices Group Guidance on Remote Audits, 2020
7. ISO 19011: 2018 Guidelines for Auditing Management Systems

RSPO is an international non-profit organisation formed in 2004 with the objective to promote the growth and use of sustainable oil palm products through credible global standards and engagement of stakeholders.

www.rspo.org

Roundtable on Sustainable Palm Oil
Unit 13A-1, Level 13A, Menara Etiqa,
No 3, Jalan Bangsar Utama 1,
59000 Kuala Lumpur, Malaysia

Other Offices:
Jakarta, Indonesia
London, United Kingdom
Beijing, China
Bogota, Colombia
New York, USA
Zoetermeer, Netherlands

✉ rspo@rspo.org
🌐 www.rspo.org