

**RSPO**

Roundtable on  
Sustainable Palm Oil

# Contingency RSPO Audit Procedure

FOR RSPO PRINCIPLES AND CRITERIA (P&C)  
AND INDEPENDENT SMALLHOLDER (ISH)  
STANDARD

Version 2

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

*Approved by Assurance Standing Committee on  
22 October 2021*



Document Title : Contingency RSPO Audit Procedure - For RSPO Principles and Criteria (P&C) and Independent Smallholder (ISH) Standard

Document Code : RSPO-PRO-T00-005 V2 ENG

Scope : International

Document Type : Procedure

Approval : Approved by the Assurance Standing Committee on 22 October 2021

Effective Date :

Contact : RSPO Certification Unit, [certification@rspo.org](mailto:certification@rspo.org)

# Contents

<b>1. INTRODUCTION</b> .....	<b>4</b>	<b>6. RSPO P&amp;C ON-SITE AUDIT PROCESS (OPTION A)</b> .....	<b>16</b>
<b>2. APPLICABILITY OF CONTINGENCY RSPO AUDIT PROCEDURE</b> .....	<b>6</b>	<b>7. RSPO P&amp;C REMOTE AUDIT PROCESS (OPTION B)</b> .....	<b>16</b>
<b>3. TERMS AND DEFINITIONS</b> .....	<b>7</b>	a. Planning for Remote Audit .....	16
<b>4. CONTINGENCY AUDIT PROCEDURE</b> .....	<b>8</b>	b. Internal Audit Requirements by the Certificate Holder .....	17
i. Situational Risk Evaluation by the CBs .....	8	c. Submission of Documentation for Remote Audit .....	18
A. Risk Evaluation for On-Site Audit .....	8	d. Documentation Sharing and Communication Platform for Remote Audit .....	19
B. Risk Evaluation for Remote Audit .....	9	e. Execution of the Remote Audit .....	20
ii. Auditing RSPO P&C Indicators .....	10	f. Gathering Information from Workers/ Stakeholders during a Remote Audit .....	21
iii. Initial Certification Audits (Including MS B for RSPO ISH Standard) .....	10	g. Sampling and Risk Factor Requirements during Remote Audit .....	22
iv. Re-Certification (RC) and Annual Surveillance Audit (ASA) for P&C and ISH Standard/ Eligibility (E), Milestone A (MS A)/Scope Extension Audits /NPP Verification/Follow-up Audit (unless on-site audit is deemed required by the CB) .....	14	h. Audit Duration for Remote Audit .....	24
<b>5. RESOURCE REQUIREMENT</b> .....	<b>15</b>	i. Certification Decision Making for Remote Audit.....	25
a. Auditor Training and Qualification to Conduct RSPO P&C Remote Audit .....	15	j. Audit Reporting for Remote Audit .....	25
b. Translator .....	15	<b>8. REFERENCE DOCUMENTS</b> .....	<b>26</b>
c. Technical/Local Expert .....	15	<b>ANNEX 1: CONTINGENCY RSPO AUDIT PROCEDURE FLOW</b> .....	<b>27</b>
d. Audit Facilitator .....	15		

## 01.

# Introduction

In view of the ongoing concern of the COVID-19 pandemic in many countries and regions, and travel restrictions and tight quarantine procedures that are still imposed by authorities, the RSPO Secretariat has been working closely with RSPO members, certification bodies (CBs), and accreditation body (AB) to identify ways to ensure that RSPO standards remain credible, and even though on-site audit could not be enforced, it does not affect our ability to uphold the high level of assurance that is expected from the RSPO certification systems.

In March 2020, the Roundtable on Sustainable Palm Oil (RSPO) Secretariat released an announcement, [COVID-19 - How we're adapting for RSPO certification audits](#), to all its accredited CBs on the conduct of audits against the RSPO Principles and Criteria (P&C) and RSPO Supply Chain Certification (SCC). Further to that, on 25 August 2020, the RSPO Secretariat introduced the [Contingency RSPO Audit Procedure \(V1\)](#) as a guide for CBs to manage and maintain the status of their certificate holders (CHs) during pandemic situations.

[The Contingency Audit Procedure \(V1\)](#) introduced four (4) scenarios that need to be followed in priority order, to cater to the situations where on-site audit activity constitutes a high risk for auditors and company staff, or where movement restrictions make it impossible to travel to the site. It was accompanied by the [Audit Facilitator Guidance](#) document for the CB to perform an RSPO remote audit with the participation of one or more audit facilitators on-site.

The RSPO Secretariat is considering an alternative approach for CBs and CHs in managing the RSPO P&C and ISH certification in light of the continuity and uncertainty of the pandemic situation such as newly reported COVID-19 cases, and the emergence of new variants at national and international levels.



## Options for Contingency RSPO Audit Procedure

As a result, the RSPO Secretariat has agreed to revise and replace the previous Contingency RSPO Audit Procedure with this version, to be used by all RSPO accredited CBs and Units of Certification (UoC) when conducting RSPO Principles and Criteria (P&C) and RSPO Independent Smallholder (ISH) standard audits in a situation of force majeure (e.g. pandemic, natural disaster, civil unrest, etc.) which prevented the audit team from conducting field assessment, to maintain the credibility of the RSPO certification scheme.

### OPTIONS TO CONDUCT RSPO P&C AND ISH AUDIT DURING FORCE MAJEURE

This version introduces only two options for the CB to conduct an RSPO P&C and ISH audit to maintain the credibility and high level of assurance associated with RSPO P&C certification, and the accuracy of information obtained by the RSPO Secretariat, CBs, and AB:

Option	Explanation
Option A: On-Site Audit	<ul style="list-style-type: none"><li>• Audits are carried out on-site by the CB's audit team; or</li><li>• Audits are carried out by the CB's audit team and supported by audit facilitator (i.e. the CB's audit team conducts audits remotely, and they are concurrently supported by the audit facilitator on-site)</li></ul>
Option B: Remote Audit	<ul style="list-style-type: none"><li>• Audit is fully conducted remotely by the CB's audit team, with no assistance from audit facilitator and/or local expert on-site</li></ul>

## 02.

# Applicability of Contingency RSPO Audit Procedure

This procedure must be treated as only applicable during force majeure events, and CBs must retain all related evidence of security warnings or instructions from authorities, companies, and/or any other form of evidence of high risk for auditors and company staffs, in order to justify cases where 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 can be used by the CBs and CHs after 23 Nov 2021 on a voluntary basis, and will formally replace the Contingency RSPO Audit Procedure (V1) on a date that will be announced by the RSPO Secretariat. All requirements in the RSPO Certification System for P&C and ISH Standard remain unchanged unless stated otherwise in this document.

All RSPO P&C and ISH audits shall be conducted in accordance with the RSPO Certification System for P&C and ISH Standard if there is no force majeure situation, such as no travel restrictions by the relevant authorities, and/or when the risk has decreased (as defined by the result of the CB's risk evaluation).





### 03.

## Terms and Definitions

<b>A.</b>	<b>REMOTE AUDIT</b>	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. Remote audit can also be defined as an audit of an organisation that is not conducted on-site. Remote audits may include off-line when there is limited connectivity (e.g. document review) or real-time virtual (e.g. video calls) approaches, or a combination thereof.
<b>B.</b>	<b>FEASIBLE</b>	A conclusion made by the CB based on the result of risk evaluation related to the possibility of implementing the allowed audit options easily or conveniently.
<b>C.</b>	<b>SITUATIONAL RISK EVALUATION</b>	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 P&C and ISH certification audits.
<b>D.</b>	<b>RISK ASSESSMENT</b>	A systematic process of evaluating the potential risks that may be involved in the sampling during an audit process. Factors to be taken into consideration when performing a risk assessment are explained in Section 5.7.3 (for P&C) and 6.4.4 (for ISH) of the RSPO Certification Systems for P&C and RSPO ISH Standard.
<b>E.</b>	<b>COMPLEMENTARY AUDIT</b>	An additional on-site audit that should be carried out to complement the RSPO P&C and ISH Initial Certification that was done via remote audit (Option B).
<b>F.</b>	<b>CB AUDIT FACILITATOR</b>	Either CB's employee or contractor, who is not qualified as an RSPO auditor or lead auditor but supports the CB audit team performing on-site audits through the use of appropriate Information and Communications Technology (ICT), including, but not limited to, video conferences, remote interviews and site tours or verification.

## 04.

# Contingency Audit Procedure

This procedure will be treated as part of the RSPO Certification Systems for P&C and RSPO ISH Standard, which will be used by accreditation body (AB), certification bodies (CB), certificate holders (CH), and organisations seeking RSPO P&C and ISH certification in the event of a force majeure. The RSPO Secretariat reserves the rights 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 the Annex of this document (Option A or Option B).

### i. Situational Risk Evaluation by the CBs

The CBs are responsible to conduct 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 P&C and ISH 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 (e.g. war, riots, fire, flood, hurricane, typhoon, earthquake, lightning, explosion, strikes, lockouts, slowdowns, pandemics) that may put the health and safety of the CB's audit team members, auditees and/or company staff at risk.
- Any travel restriction 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. locality/district/state/country)
- 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 and/or audit facilitator(s) to travel for on-site audits
- For Pandemic Covid-19 Specific Case:
  - The number of new and active recorded COVID-19 cases (beyond isolated cases) within the last 14 days of the date of risk evaluation 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.)

In the event that 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 auditor's right to accept or decline the assigned onsite audit.



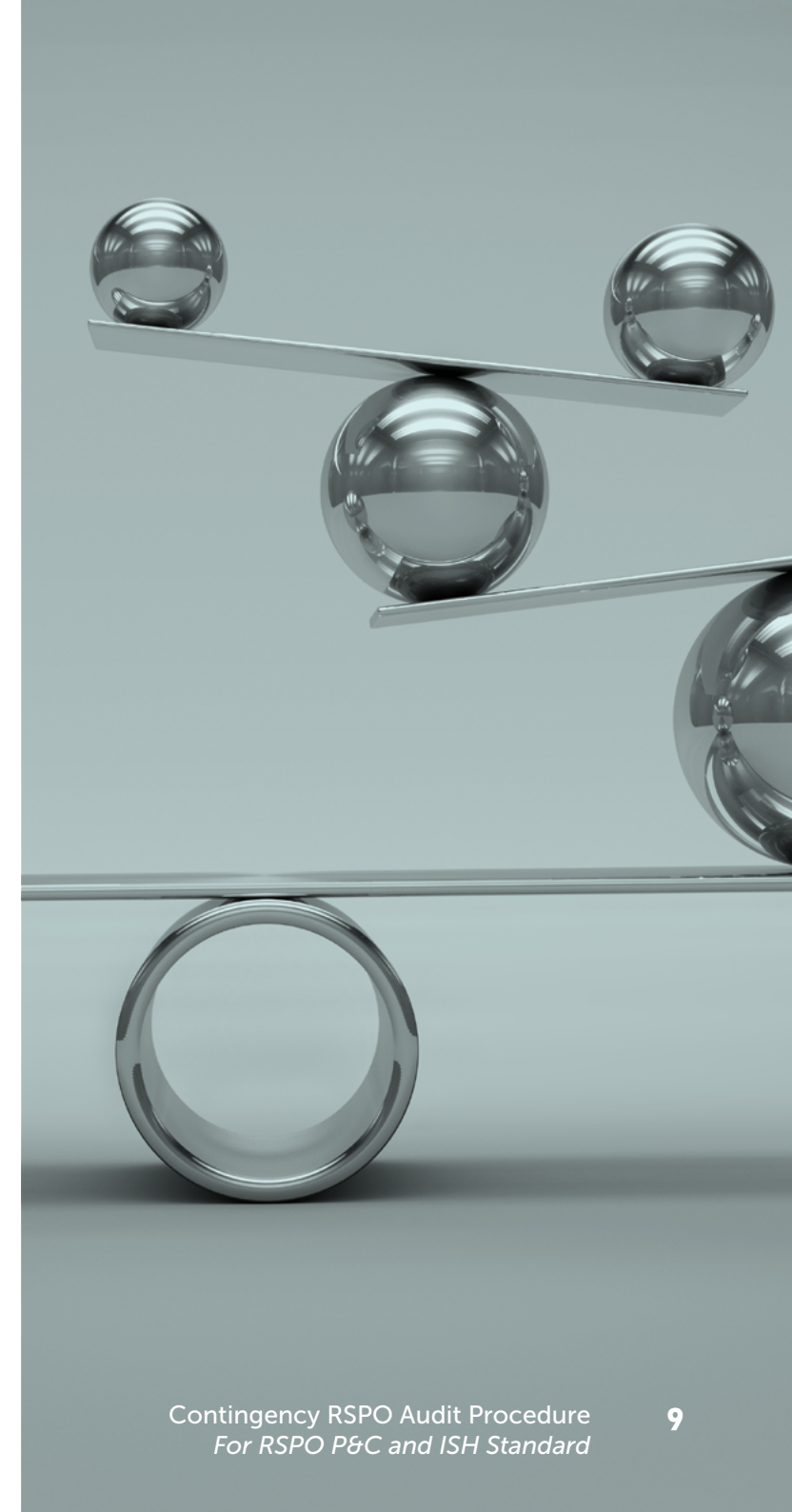
## B. Risk Evaluation for Remote Audit

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 – Contingency RSPO Audit Procedure Process Flow).

- The justification and agreement by the CB and CH for the on-site audit is not feasible are documented
- Availability of sufficient resources and tools (i.e. Internet connection, mobile network coverage, hardware, software, competence personnel, etc.) among the CB's audit team, UoC, surrounding communities, previous land users, and other stakeholders to facilitate the information gathering and collecting feedback during the remote audit
- Possibility to make the necessary tools for remote auditing available (e.g. local representative may be able to facilitate access for video calls with the communities)
- 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 getting lower, 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 if 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 CB and CH.



## ii. Auditing RSPO P&C Indicators

The RSPO Secretariat has identified the expected outcome (at a minimum) for each indicator in the RSPO P&C and ISH standard from the audit exercise as presented in the Generic Audit Checklist (for both RSPO P&C 2018 and ISH Standard 2019), which can be found [on the RSPO website](#).

This generic 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 each of the requirements that are audited remotely, the CB should be able to:

- Define suitable audit methodology for the auditors to gather objective evidence for each RSPO P&C indicator.
- Identify what data are usually collected for the specific indicators during an on-site audit.
- Determine how this information will be obtained and presented through remote alternative means of gathering that data, or gaining the same objective evidence and insight.

## iii. Initial Certification Audits (including MS B for RSPO ISH Standard) by OPTION B

For initial certification (IC), the CB shall conduct a situational risk evaluation (as stated in Section 4 (i)) to evaluate the availability of resources and adequacy of access and tools to conduct the remote audit. Where the remote audit is deemed as feasible by the CB, the IC can be conducted remotely following all requirements set for IC in the RSPO Certification Systems for P&C and RSPO ISH Standard.

For cases where the certification decision and issuance of certificate for IC is made by the CB based on the result of remote audit, all other requirements for IC in RSPO Certification Systems for P&C and RSPO ISH Standard remain unchanged, except for the following:

### Risk Assessment for selection of Samples:

- The CB shall apply a HIGH-RISK multiplier for the sampling calculation as explained in the RSPO Certification Systems for P&C and ISH Standard (5.7.3 and 5.7.4)

**estate to sample(s) =  $(\sqrt{y}) \times (2.0)$ ,  
where y is the number of estates**

- If the result of the calculation of the sample is <4, a minimum of four (4) estates shall be audited. For units of certification that have  $\leq 4$  estates, all estates shall be audited.

### On-site Complementary Audit (by audit team/audit facilitator)

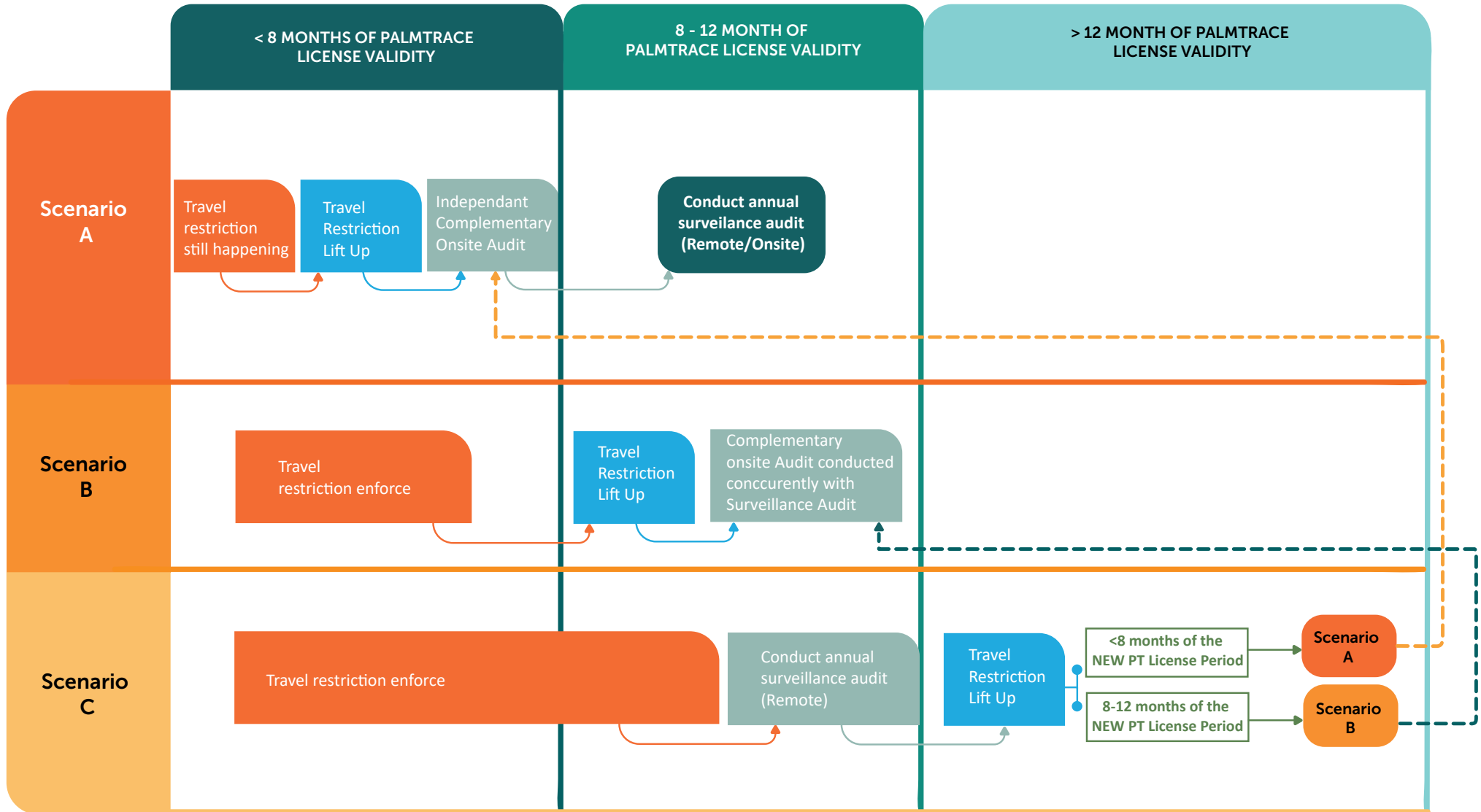
Considering the initial certification is being issued based on the result of remote audit, the CB shall plan an on-site complementary audit to complement the initial certification as soon as travelling is allowed and/or it is safe to visit the UoC.

- The CB and its client shall agree that for any IC certificate issued through a remote audit, an on-site complementary audit to complement the initial certification shall be conducted as soon as travel restrictions are being lifted and/or the situation permits based on the CB's risk evaluation. The complementary audit should be conducted within 60 days after the lifting of travel restriction.
- In case the travelling is allowed and/or it is safe to visit the UoC before the issuance of certificate, the CB should consider to hold the certification decision making, and complete the on-site complementary audit prior to the issuance of certificate.
- During the on-site complementary audit, the CB's audit team shall seek to evaluate the effective implementation of the RSPO P&C and ISH certification requirement by the UoC. The focus is expected to be on site observations and stakeholder interviews (e.g. with workers and local communities) concentrating on aspects that are more challenging to verify during remote audit. The responsibility to plan and conduct the on-site complementary audit lies on the CB, based on risk evaluation. The cost for the complementary audit shall be taken into consideration during the certification contract preparation between the CB and its client (i.e. the cost for the complementary audit shall only be chargeable when it is realised).
- In case the on-site complementary audit is conducted independently (i.e. not conducted in combination with any on-site annual surveillance audit), as a general guidelines, the minimum duration for the complementary audit of a management unit consisting of one (1) mill and one (1) estate should be three (3) man-days.





The on-site complementary audit, however, can be combined with the next on-site annual surveillance audit, if the travel restrictions are lifted and/or the situation permits within the period of eight (8) to twelve (12) months of the licence expiration date. This option is given to prevent two audits from being conducted too soon after each other. This is further explained in the following diagram :



### Addressing major and minor non-compliances:

- Minor non-compliances raised during the on-site complementary audit shall be raised to major if they are not addressed in the next Annual Surveillance Audit.
- Major non-compliances raised during the on-site complementary audits shall be closed successfully within 90 days, or the certificate shall be suspended, and subsequently withdrawn if the major non-compliances are not addressed within an agreed timeframe as set between the CB and RSPO member, not longer than six (6) months from the last day of the audit.
- Recurring major non-compliances (for both P&C and ISH Standard) on the same indicator (including the supply chain indicators) in the on-site complementary audit shall lead to immediate suspension of the certificate. This suspension shall be lifted when the NC is successfully addressed.
- Recurring minor non-compliances on the same indicator in the on-site complementary audits shall be raised to major. Recurring of the non-compliance against this non-critical indicator in the subsequent audits shall be raised as major, which results in immediate suspension.

### Certificate Suspension:

- The CB shall inform its client who has been certified for Initial Certification via remote audit (prior to the completion of the complementary audit); that the RSPO Secretariat and/or the CB have the right to immediately suspend their certificate when the RSPO Secretariat, AB, and/or the CB receive any formal complaint related to the UoC.
- This will be in line with the requirements 5.12 of the RSPO Certification Systems for P&C and RSPO ISH Standard.

**iv. Re-Certification (RC) and Annual Surveillance Audit (ASA) for P&C and ISH Standard / Eligibility (E), Milestone A (MS A)/Scope Extension Audits/NPP Verification/Follow-up Audit (unless on-site audit is deemed required by the CB)**

The CBs are responsible to conduct Risk Evaluations of contextual and business-specific risks in order to select to determine the audit option that is feasible for the whether the Unit of Certification (UoC) to conduct the RSPO P&C and ISH audit (i.e. Option A, Option B)

The RSPO Secretariat has developed a simplified process flow as a guidance for the CBs to evaluate and decide on the appropriate audit option (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.

When the CBs define the risk for on-site audit or remote audits as **FEASIBLE**, the justification and agreement shall be documented and properly maintained, and the CBs may proceed with the agreed option (Option A, Option B) accordingly.



## 05.

# Resource Requirement

<b>a. Auditor Training and Qualification to Conduct RSPO P&amp;C Remote Audit</b>	<p>The CB shall establish a mechanism (i.e. training, competency evaluation) to ensure that the competencies of all auditors and/or team members (including subcontractors, audit facilitators, local or technical experts, translators, and others) who will participate in the remote audit are evaluated and recorded, to ensure that 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.</p> <p>RSPO considers flexibility in the new RSPO P&amp;C auditor qualification (as an audit team member) to account for on-site audit restrictions. A new RSPO P&amp;C auditor can count their supervised (by a qualified auditor/lead auditor) period of training in a practical audit against the RSPO P&amp;C through the remote audit. However, this is not applicable to qualify an RSPO P&amp;C Lead Auditor as required in 4.8.7 (b) of the RSPO Certification Systems for P&amp;C and RSPO ISH Standard.</p>
<b>b. Translator</b>	<p>In case the CBs require the support or assistance of a translator during the remote audit, the CB shall ensure that:</p> <ul style="list-style-type: none"><li>● the translator is independent from the organisation being assessed, as stated in 4.6.6 of the Certification Systems document 2020.</li><li>● the name of the translator shall be included in an audit report.</li><li>● the translator is being trained on the management of confidentiality.</li><li>● the translator is being trained on remote audit procedure/guidelines including the use of ICT platforms (e.g. facilitating conversations through the remote audit).</li></ul>
<b>c. Technical/ Local Expert</b>	<p>Similarly, in case the CBs require support or assistance of a technical/local expert during the remote audit, the CB shall ensure that:</p> <ul style="list-style-type: none"><li>● the technical/local expert is independent from the organisation being assessed, as stated in 4.6.6 of the Certification Systems document 2020.</li><li>● the name of the technical/local expert shall be included in an audit report.</li><li>● the technical/local expert is being trained on the management of confidentiality.</li><li>● the technical/local expert is being trained on remote audit procedure/guidelines including the use of ICT platforms (e.g. facilitating conversations through the remote audit).</li><li>● the technical/local expert is being trained by the CB on the RSPO P&amp;C requirements (including ISH Standard) for a minimum of eight (8) hours before the audit.</li></ul>
<b>d. Audit Facilitator</b>	<ul style="list-style-type: none"><li>● Refer to the RSPO Guidance <a href="#">Participation of CB Audit Facilitator in the RSPO audits</a> which can be found on the RSPO website.</li></ul>

## 06.

# RSPO P&C On-Site Audit Process (Option A)

Aside from the Situational Risk Evaluation of On-Site Audit, the detailed activity of the audit (planning, opening, closing, etc.) shall be conducted following the RSPO Certification Systems for P&C and RSPO ISH Standard.

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.

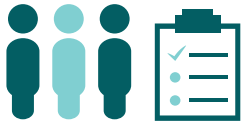
## 07.

# RSPO P&C 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), surrounding communities, previous land users, and other stakeholders to facilitate information and feedback gathering during the remote audit
- Methodology for documentation/information sharing platform to access data and/or information during the remote audit. This should include the available options to conduct interviews with workers, stakeholders, and other interested parties
- Data protection policies should also be in place and complied with by all parties
- Conduct a 'test' session for the CB auditor and auditee (including stakeholders/respondents) to familiarise themselves with the available information communications technology (ICT) that will be used in the remote audits. There is a need for a contingency plan should the technology fail
- Auditors and auditees need to be flexible and adaptable as there would be a risk for misunderstanding through the use of virtual communications tools
- Define the agenda, accommodating dispositions different from an on-site audit (e.g. better definition of tasks by different team members).



## b. Internal Audit Requirements by the Certificate Holder

The CH shall conduct and complete the annual internal audit covering the whole UoC (at the maximum of the last 12 months prior to the date of remote audit). It is recommended that the CH to use the Generic Remote Audit Checklist or any other documents that will represent the overall RSPO P&C requirements.

The internal audit report shall not be only a ‘tick-box’ exercise but should contain sufficient information (e.g. documented procedures, records, interviews, etc.) to explain how the CH complies with each requirement in the standard. It should contain sufficient information for the CB to verify compliance and to challenge any aspects during the remote audit. If the internal audit report does not contain sufficient information for certain indicator(s), the CB may need to request additional information or raise this as non-conformity during the remote audit.

A thorough internal audit would normally identify some non-conformities (based on the CH’s internal audit procedures). When submitting the document to the CB, the CH is not expected to address the corrective action on certain non-conformities. However, before the start of the remote audit, the CH must either have closed out the non-conformity (i.e. demonstrably completed the corrective action, which the CB can review) or have temporary actions in place. These corrective and temporary actions will be reviewed and verified by the CBs during the remote audits.





### c. Submission of Documentation for Remote Audit

The CH shall submit the Internal Audit Report, together with all other supporting information/documents, at least 14 days before the agreed remote audit date by the CB. This is important to allow the CB auditor to have sufficient time to review the document before the audit to ensure that the remote audit is smooth. The CB auditors should plan and conduct a review within 14 days before the scheduled remote audit date.

The CB may provide a list of documents, records, data, and information that are required from the CH in advance, to assist the CH in preparing for the remote audit. The list would be helpful for the CB audit team to verify during the remote audit. It should include, but not necessarily be limited to, the following:

- maps of acceptable quality
- completed RSPO Metrics Template
- an updated list of contact and stakeholder information along with designated representatives (e.g. with details of contact information such as mobile phone number, email, location address, etc.)
- SEIA/HIRARC/HCV/RaCP documents
- summary of meeting/training/consultation
- accident records - Loss Time Injury
- stakeholder's feedback (if any)
- grievance and complaints records
- evidence on the completion of RaCP (where applicable)
- approved HCV-HCS assessment report (where applicable)
- GeoRSPO and Hotspot Hub information
- list of applicable regulations including evidence of evaluation of legal compliance
- videos/photos that provide an overview of selected operations, activities, facilities, HCV area, and other relevant areas required by the CB auditors. The pre-recorded video/photo shall have appropriate 'geotagging' information
- for a new developed area, proof of NPP Assessment Summary report and Notification Statement (if applicable).



#### d. 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 call, 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 phone call, and/or the other available relevant verifications 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, and must be able to preview to the audit team when needed.

Where there is limitation by law of documentation/information (including video, photography, etc.) sharing, 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.



## e. Execution of the Remote Audit

The remote audit shall include a ‘live’ visual feed (e.g. live video and audio capability), which must be portable around the site, including in the field 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 is a limitation 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 his team) can be considered as evidence sharing as 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 the cases mentioned above, 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, sister estate’s 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.





## f. Gathering Information from Workers Stakeholders during a Remote Audit

Getting information from stakeholders and workers is the most challenging aspect and would have a big impact when the audit is conducted remotely. This is also the most typical complaint-based issue received by the RSPO Secretariat.

To ensure the smooth process of gathering information or feedback from workers and/or stakeholders during the remote audit, the CB shall have a documented procedure that demonstrates a proactive approach to ensure the inclusivity of all stakeholders and also ensure that all inputs are captured during the remote audit. This is also applicable for verification of Free, Prior and Informed Consent (FPIC) processes within the management unit.

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 workers and vulnerable individuals (e.g. through interviews or other communication platforms), and to avoid compromising the safety of the workers/stakeholders (e.g. threatened on dismissal, death, rights, etc.).

The procedure shall also include protocols for anonymity and privacy (when requested), and a way to connect with individual workers, (e.g. unique identification numbers/name, etc.) to enable a follow-up if any significant rights issues are raised or discovered. The CB should consider the ability to verify the information gathered and provide feedback (if necessary).

**Some of the good practices to be considered by the CB for effective workers/stakeholder's interviews during the remote audit are as follows:**

- The CB can consider whether workers/stakeholders should be given a phone number, email address, or another communication/messaging platform (e.g. WhatsApp, Telegram, WeChat, etc.) to reach out to the CB if they are retaliated against.
- The technology and tools shall allow auditors to confirm the interviewee's identity. (Note: The CH shall not record the interview themselves for the audit team. Similarly, the CB shall not record the interview session unless mutually agreed upon by both parties).
- The CB shall ensure that no representative from the CH is present during the interview session with stakeholders.
- As much as possible, the auditor should aim to use video communication while conducting remote interviews. It is important to use video to see facial expressions and body language and ensure interviews can be conducted in confidence.
- Ensure that timestamps and the interview location of the stakeholders in the report is captured accordingly.



## g. Sampling and Risk Factor Requirements during a Remote Audit

The CB shall follow the sampling requirements as stated in 5.7 and 6.4 of the RSPO Certification Systems for the P&C and ISH Standard to calculate the samples to cover during the remote audit.

In determining the risk factors, the CB shall consider, but not necessarily be limited to, the following matters in the risk assessment:

- geographic locations and distance of estates
- land size
- complexity of the labour force
- landscape setting (e.g. presence of HCV/peat/protected areas/forest, etc.)
- complexity of supply sheds
- number of communities
- known conflicts/legal issue
- availability of resources and tools to facilitate the remote audit (i.e. Internet connection, mobile network coverage, hardware, software, competence personnel, etc.)

For the first full remote audit assessment at the specific UoC, the CB shall increase the remote audit intensity to cover the previous years' performance (i.e. records, interviews, complaints/grievances, environmental, safety and health, labour issues, stakeholders input, etc.).

To accommodate the increase in the audit intensity to evaluate the previous year's performance (e.g. 2020 and 2021), the CB should increase the allocated man-days (if necessary) to facilitate the additional audit intensity and/or audit samples (if required).

The CB shall ensure that the reporting data of actual production and sold volume are covered from the last reporting period (as of the last on-site audit) until the full remote audit took place.

The data reporting should be presented using the template below. For example:

- If the data reported during the last on-site audit (e.g. carried out in January 2019) covered the period from 1 December 2017 to 30 November 2018, and the first full remote audit was carried out in February 2022, the reporting period for this full remote audit should cover the period from 1 December 2018 to 30 January 2022.
- The reporting period should continue to suit the original licence period (continue the scenario in the first bullet), if the normal reporting period for example covers 1 December 2019 to 30 November 2022, then the next assessment (remote/on-site) should continue to report from 1 December 2022 to 30 November 2023.
- The CB is allowed to edit the table to suit any case such as multi-mill scope, etc.

Description	Reporting Period: MM/YY to MM/YY		
	CSPO (MT)	CSPK (MT)	
Certified Volume (MT) *following previous year's approved volume			
Actual Production during reporting period (MT)			
Actual Sold Volume - RSPO Certified (MT)			IP
			MB
Actual Sold Volume - Other schemes (MT)			
Actual Sold Volume - Conventional (MT)			
TOTAL Actual Sold Volume			



## h. Audit Duration for Remote Audit

It has been recognised that conducting audits remotely can be very challenging and uncertain (depending on the connectivity issue, information-sharing platform, familiarity with ICT platform, 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 duration overall for the remote audit.

**As a guideline, the duration of the remote audit (e.g. Nine (9) man-days to cover one (1) mill and one (1) estate should be distributed to cover the following elements:**

- Meeting/calibration of the remote audit methodology with the CH (e.g. familiarisation on ICT platform, communication medium, etc.) before the remote audit date
- Documentation/information submission period by the CH (e.g. before the actual remote audit date)
- Preliminary documentation/information review by the CB (e.g. before the actual remote audit date)
- Review and evaluation of compliance based on live discussion, documentation, and information review, and/or virtual tour

**The key is to allocate the audit effort (hours) differently, focusing more on the preparatory steps and enabling 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.**





### i. **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 Clause 5.8 of the certification system.

For IC and RC audits, the CB shall submit the result of Risk Evaluation as required in Section 4(i) of this document as part of the audit package during the Peer Review process. The peer reviewer will consider the risk evaluation made by the CB to confirm certainty of the risks.



### j. **Audit Reporting for Remote Audit**

The CB shall provide an audit report that fulfils all the requirements listed in Annex 3 of the RSPO Certification Systems for P&C and RSPO ISH Standard, 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 by COVID-19.

All reports shall include a description of the audit methodology used, how the stakeholders/previous land users are consulted, and other related information as required in this procedure.

As the nature and format of data and information collected through 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 captured and reported, and any implications for data privacy and confidentiality.

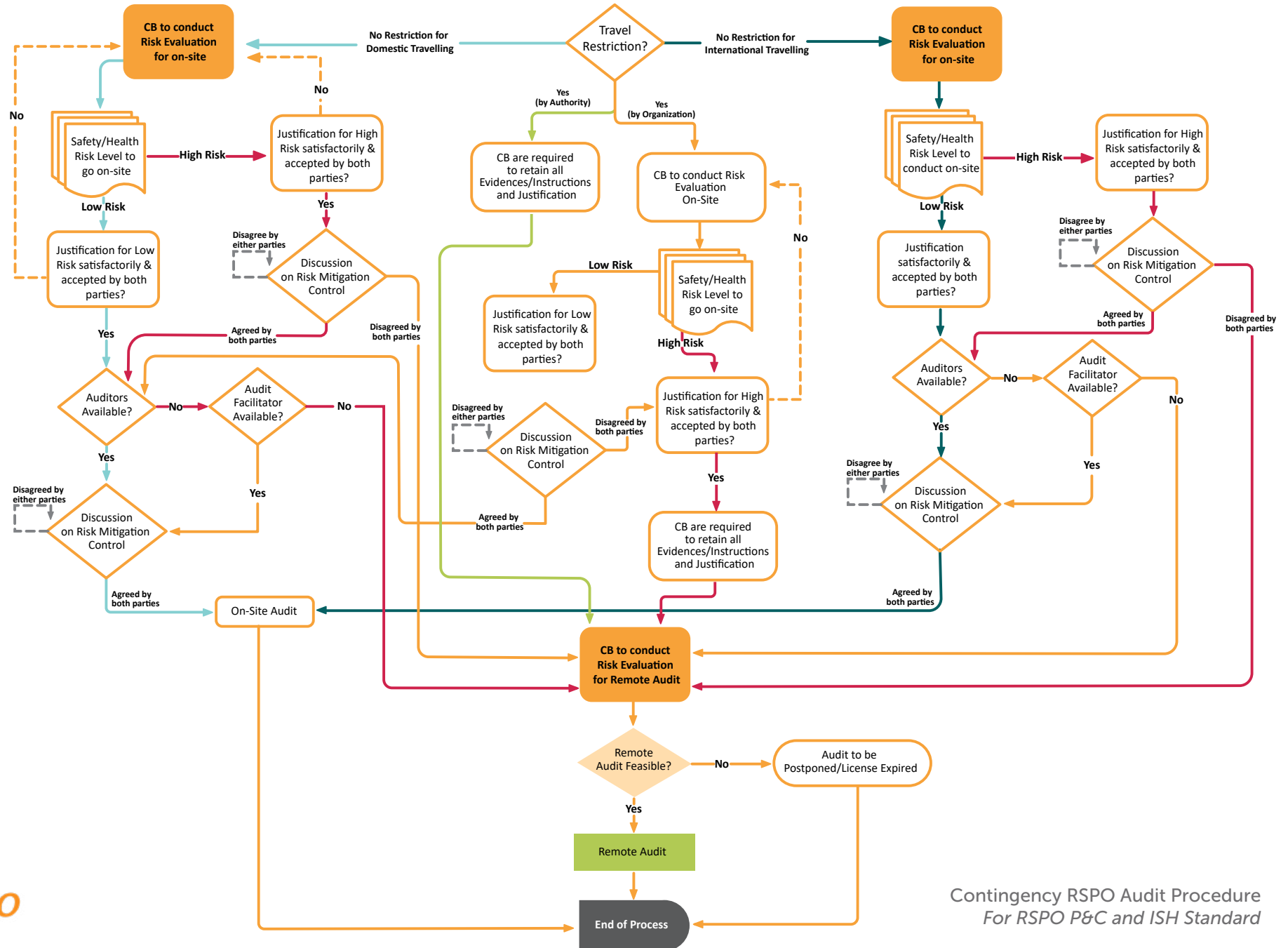
## 08.

# Reference Documents

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

# Annex 1: Contingency RSP0 Audit Procedure Process Flow

## CB Planning for RSP0 P&C Audit





## **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