Remote Auditing Good Practices
ISEAL Guidance – Draft v0.1 – March 2021

Table of Contents
1. Introduction ................................................................................................................................. 3
   1.1. Context ................................................................................................................................. 3
   1.2. Scope .................................................................................................................................. 3
   1.3. Alignment.............................................................................................................................. 3
   1.4. Normative references.......................................................................................................... 4
2. Audit Policies and Procedures ..................................................................................................... 4
   2.1. Derogation policy .................................................................................................................. 4
   2.2. Certificate extensions .......................................................................................................... 4
   2.3. Remote audit policy applicability ....................................................................................... 5
   2.4. Overall approach to remote audits ..................................................................................... 5
   2.5. Risk assessment to qualify eligibility ............................................................................... 5
   2.6. Initial certification audits .................................................................................................... 6
   2.7. Surveillance audits .............................................................................................................. 6
   2.8. Full recertification audits .................................................................................................. 7
   2.9. Chain of custody audits ...................................................................................................... 7
   2.10. Hybrid audits .................................................................................................................... 8
   2.11. Auditor training and qualifications .................................................................................... 8
   2.12. Requirements for assurance providers ............................................................................. 8
   2.13. Safety preconditions for on-site audits .......................................................................... 9
3. Audit Implementation ................................................................................................................ 10
   3.1. Pre-audit planning ............................................................................................................... 10
   3.2. Client preparation ............................................................................................................... 10
   3.3. Facilitators (for hybrid audits) .......................................................................................... 11
   3.4. Interpreters ........................................................................................................................ 11
3.5. Assessment Process ................................................................. 11
3.6. Audit duration ........................................................................... 12
3.7. Implications for Fees................................................................. 12
3.8. Audit Decision-making .............................................................. 12
3.9. Audit reporting .......................................................................... 12
3.10. Oversight requirements for remote auditing .................................. 13
3.11. Publicly available information .................................................. 13
4. Data Management and Technology ................................................. 14
   4.1. Good data management practices ............................................. 14
   4.2. Selecting technology for remote audits...................................... 14
   4.3. Accessing client data .............................................................. 15
   4.4. Data privacy and consent ....................................................... 15
   4.5. Data security .......................................................................... 16
   4.6. Gathering information from workers ........................................... 16
   4.7. Remote locations and accessibility ........................................... 17
1. Introduction

1.1. Context

Sustainability systems and assurance providers have adapted their auditing procedures and practices to the new virtual realities imposed by COVID-19. This has led to rapid innovation and evolution in remote auditing practices, grounded in improvements to data management and governance. We are now at a stage where it is useful to document some of these emerging practices as input for collective discussion and alignment around the practices that will best support implementation of effective remote auditing.

We anticipate that many of the practices currently being implemented due to COVID-19 will become more permanent fixtures in how assurance is delivered in the future. Remote auditing has the potential to reduce the need for onsite assessments; create opportunities for increased efficiency and safety, better timing, the inclusion of assurance personnel who may not otherwise be available; and avoid travel delays and restrictions, among other things. Most significantly, it has the potential to improve sustainability systems’ capacity for effective data and risk management in implementation of their assurance programmes.

This ISEAL Guidance seeks to capture some of the core elements and good practices that are emerging as a result of this innovation. It is intended both as a source of inspiration and reference for sustainability systems that are seeking to strengthen their remote auditing practices and as a living document that can evolve over time as our collective knowledge and experience refines what we know about effective approaches and tools.

This first draft of the ISEAL Remote Auditing Guidance will be used as the basis for consultation and dialogue with sustainability standards and assurance providers and will be refined as a result of that consultation.

1.2. Scope

This Good Practice Guide applies primarily to sustainability systems that are implementing or requiring remote auditing approaches within their assurance or verification programmes. Since some systems defer management of their assurance processes to assurance providers like certification bodies, the guidance is also applicable to these assurance providers.

This guidance is non-normative and can be used as a checklist or reference for initiatives as they think about all the things that need to be in place to ensure the quality, integrity and efficiency of remote auditing practices.

1.3. Alignment

Part of the impetus for looking at areas of potential alignment in remote auditing practices is to ensure that both producing enterprises and supply chain buyers are not faced with widely varying and potentially even conflicting policies and practices across different sustainability systems. Initial research suggests that it may be easier to align around how specific areas of the assurance process are impacted by a remote approach rather than aligning on the practices themselves. Areas to explore range from risk management approaches to data management, and from surveillance and hybrid audit processes to principles in selecting ICT tools.

Comparatively few opportunities for alignment in the practices themselves may be due to:

- the strong influence of standards’ technical requirements and assurance system contexts and scopes on remote auditing processes

---

1 ASI. March 2020. ASI FAQs in response to Coronavirus.docx
• widely varying levels of assurance system geographic reach (key factor due to the nature of Covid-19 restrictions which may affect country-by-country practices)
• varying levels of organizational digital maturity (impacting risk-based approaches to audit eligibility/processes as well as data management practices)

1.4. Normative references

The following table lists a range of existing normative references that include information relevant to remote auditing and that may be useful for sustainability systems to review as background for the refinement of their own remote auditing procedures.

<table>
<thead>
<tr>
<th>Normative reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU General Data Protection Regulation (EU GDPR)</td>
</tr>
<tr>
<td>IAF ID 3: 2011 Management of Extraordinary Events or Circumstances Affecting ABs,</td>
</tr>
<tr>
<td>CABs and Certified Organizations</td>
</tr>
<tr>
<td>IAF ID 12: 2015 Principles of Remote Assessment</td>
</tr>
<tr>
<td>IAF MD 4: 2018 The Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes</td>
</tr>
<tr>
<td>IAF MD 5: 2019 Determination of Audit Time of Quality, Environmental, and Occupational Health &amp; Safety Management Systems</td>
</tr>
<tr>
<td>ISO 19011: 2018 Auditing Management Systems</td>
</tr>
</tbody>
</table>

2. Audit Policies and Procedures

The first step that many sustainability systems took in response to COVID-19 restrictions was to revise their policies related to the timing and nature of assessments and validity of certificates. Audit policies are important because they set the framework conditions within which remote auditing can take place. Collectively they should represent a coherent strategy and approach for managing the risks to assurance integrity inherent in remote auditing practices.

This section highlights the different types of policies that a sustainability system should have in place, some of which are specific to remote auditing, others that can be revised or updated to take remote auditing practices into account.

2.1. Derogation policy

**Sustainability systems should have in place an audit derogation policy that allows assurance providers to request exceptions or deviations based on an acceptable rationale for the derogation request.**

Audit derogation or variation policies define the conditions under which exceptions or deviations from regular assurance and surveillance audit procedures, requirements, or timelines are allowed. Derogation policies apply more broadly than remote audit policies and one type of derogation may be the use of remote audits.

2.2. Certificate extensions

**Sustainability systems should define the conditions under which they allow for extensions of the validity of existing certificates and the allowable length of those extensions.**
Certificate extensions shall be requested prior to the expiry of the certificate but not more than one month in advance of the certificate expiry date due to the changing nature of COVID-19 restrictions. Certificate validity may be extended for a maximum period of 6 months where a risk assessment conducted by the assurance provider indicates a low risk of non-compliance.

Where the periodicity of full reassessments is greater than one year, a certificate that is due to expire may be extended for up 12 months by performing a remote surveillance audit.

2.3. Remote audit policy applicability

Sustainability systems should have a remote audit policy that documents the conditions under which the policy and, by extension, remote auditing is applicable. This policy should include definitions for how terms specific to remote auditing are being applied by the sustainability system.

For example: The ISO 9001 Auditing Practices Group has developed a checklist on feasibility and risk analysis for remote audits (see Annex 1).

For example: GlobalGAP requires that the remote audit policy shall apply only when official travel or gathering restrictions are in place in the country or region where the inspection is to take place, e.g. travel to/from regions identified as high-risk by the national Ministry of Foreign Affairs or the World Health Organization. The scheme owner or assurance provider shall keep evidence of the emergency status to justify use of the procedure.

2.4. Overall approach to remote audits

As part of their remote audit policy, sustainability systems should define the basis on which they determine when to allow remote audits for different types of assurance.

Assurance audit types include initial audits, surveillance audits, chain of custody audits, and re-certification audits (though these are sometimes referred to by different terms in different sustainability systems). There are three broad approaches for determining eligibility for remote versions of these audit types:

- **Audit type-driven**: Clear definition and criteria for allowing remote versions of eligible audit types (e.g. initial, surveillance, re-certification). Unlikely to require assurance providers to conduct risk assessments as basis for eligibility.

- **Scenario-driven**: Eligibility for remote audit, as well as the audit process itself determined by a combination of audit type and risk factors presented by the certified entity or client.

- **Data-driven**: Assurance data and technical factors inform a risk assessment used to identify eligible operations and audit types. Approach is not typically prescriptive about categorizing eligible audit types.

2.5. Risk assessment to qualify eligibility

Where sustainability systems require use of a risk assessment to determine whether an enterprise qualifies for one or more types of remote audit, they should define the risk assessment process, including classification of risk levels and implications of each risk level for the assessment process.

Underlying this policy should be a consideration of the risks to the integrity of the assurance process and validity of the assessment results. Good data and a strong data management system will be critical to support
an understanding of where the risks are of non-compliance and how effectively the remote assurance practices are identifying non-compliant performance based on those risks.

**For example:** The Aluminium Stewardship Initiative (ASI) bases eligibility for remote audits according to a maturity rating assessment of the operation assigned by the auditor across the dimensions of ‘systems’, ‘risks’ and ‘performance’. The ‘performance’ dimension cannot be adequately assessed for the Maturity Rating unless the on-site audit has been completed. This system engages auditors in the remote auditing decision-making process and allows for highly differentiated decision-making for each assurance audit type using ratings and risks.

**For example:** FSC annual audits may be conducted as remote desk audits in instances where the certificate holder does not exhibit any of the following criteria:

- has open major or critical non-compliances that cannot be verified without site visit
- has high volume of active negative media attention or stakeholder feedback
- has a history of poor performance, e.g., suspended more than one time, history of recurring major non-compliances related to field-based implementation
- is involved in a credible, active stakeholder complaint, dispute or external investigation
- is subcontracting / outsourcing certified activities in response to the coronavirus outbreak.

In all cases for FSC, minor non-compliances that require onsite verification to evaluate and close shall not be closed during fully remote audits and shall have their deadline extended by 12 months.

**2.6. Initial certification audits**

Sustainability systems should consider the conditions under which they will allow for remote initial audits of new clients, if at all. Where remote initial audits are allowed, these should be classified as high risk, with consideration of any restrictions on the nature of the assessment (e.g. partial assessment) and of the assurance status of the client (e.g. conditional certification).

**For example:** ASI (Aluminium) auditors could recommend Provisional Certification on the basis of the desktop review component where appropriate, with a Surveillance Audit scheduled at a later date to address the on-site component.

**For example:** Fair Trade USA offers the option to accept new client applications and postpone the initial audit or conduct a desktop review of some components while delaying the certification decision until an on-site audit is possible. Initial Certifications are not granted until an onsite audit (either a full onsite audit or hybrid audit including an onsite component) is completed.

**2.7. Surveillance audits**

Sustainability systems should define the conditions under which remote surveillance audits (or follow-up audits) are to be conducted. This can include consideration of any limitations on what can be assessed or changes in the frequency or intensity of the audit process as a result of it being conducted remotely.

**For example:** FSC surveillance audits may be conducted as desk audits if an assessment of the scale, intensity and risk of the enterprise’s activities concludes that a desk audit can credibly be conducted.
For example: RSPO requires that remote audits are conducted every 3 months, resulting in a 3 month certificate extension. When an on-site audit is once again feasible, the sample size of sites visited is to be increased by 50% from the previous on-site audit.

For example: SAAS indicates that, assuming other criteria are met, consecutive off-site surveillance audits are allowed one time for clients on a semi-annual surveillance programme but are not allowed for clients on an annual programme.

2.8. Full recertification audits

*Sustainability systems should determine if any additional restrictions need to be in place for full recertification audits beyond those in place for surveillance audits. This can include risk analysis to qualify eligibility for remote, determination of any criteria that require on-site inspection, and limited or conditional certification status.*

For example: ASI (Aluminium) auditors can recommend Provisional Certification on the basis of a desktop review where appropriate, with a Surveillance Audit scheduled at a later date to review the on-site component. However, even provisional certification can be put on hold where one or more of the following is identified:

- There is an insufficient number or range of criteria that have been adequately assessed during the remote audit component;
- There is a substantial number of high-risk or significantly material criteria that have not been assessed during the remote audit component;
- The overall level of objective evidence obtained and reviewed remotely by the auditor is deemed insufficient to continue or progress to a Full Certification status;
- Insufficient rigour has been applied to the auditing of one or more criteria of material significance to the Entity and its Certification Scope;
- There is insufficient sampling of businesses and/or facilities for Certification Scopes that include multiple operations.

For example: FSC assurance providers shall conduct a risk assessment of each applicant according to the scenarios/factors provided by FSC to determine the option of conducting a fully remote audit (low risk), a partially remote audit (medium risk), or if a mandatory on-site audit is required (high risk).

The risk assessment is to be undertaken at the level of a single site and not at the certificate level. For multi-site certificates, FSC requires that the risk assessment is undertaken for each participating site (or for each site selected by sampling) during the evaluation audit. When an applicant falls into more than one risk category, the CB adopts the precautionary approach and applies the audit type of the higher category.

2.9. Chain of custody audits

*Sustainability systems should consider when to allow remote assessments for chain of custody audits, and when the results of risk assessments require on-site follow-up.*

For example: FSC ‘Medium risk’ clients have a two-stage chain of custody audit process which includes a desktop audit for Stage 1 and an on-site audit for Stage 2, when on-site audits are possible in the future.
2.10. Hybrid audits

Sustainability systems should determine and document which criteria are not able to be assessed remotely. Where full assessments cannot be conducted credibly using remote methods, sustainability systems should consider splitting the audit into two parts, consisting of a remote audit and a separate on-site audit at a future date. Sustainability systems should set limits for the time that can elapse between the remote and on-site elements of the audit (commonly 6 months).

Remote audits usually fall into two categories:

- Fully remote audits where desktop reviews, data collection, and remote interviews are sufficient to assess compliance with all of the standard’s requirements.
- Partially remote audits and ‘hybrid audits’ that consist of a remote review of a portion of audit requirements, and the remaining portion of requirements assessed through an on-site visit.

2.11. Auditor training and qualifications

Sustainability systems should define qualifications and training requirements for auditors and other assurance personnel, along with competence assessment procedures, to ensure they have the necessary skills to deliver remote audits. This can extend to defining how auditor training can also be delivered remotely. Training content should include areas linked to at least audit preparation, planning, and execution.

For example: ASI (Aluminium) assurance providers are required to work with their auditors on calibration regarding technological and methodological good practices, and on evaluating the extent to which remote assessments are effective.

For example: ASC remote audits can be witnessed by CAB’s lead auditor as part of the requirements to keep auditors’ qualifications (ASC CAR v2.1 B18), but they cannot be considered for the sign off of new auditors.

For example: FSC Training Providers may replace classroom (in-person) training by remote trainings, based on the following specifications:

- Travel restrictions are in place for any of the registered trainees or the trainer(s).
- Trainings should offer similar opportunities as in-person trainings to conduct practical exercises and allow for interaction of trainer(s) and trainees (as far as technology allows).

2.12. Requirements for assurance providers

Sustainability systems should define any additional remote auditing requirements expected of their assurance providers, such as required communications with the scheme owner or policies for how assurance providers can update their procedures.

Some schemes issue broader responsibility to assurance providers, requiring them to have policies that address procedures for selecting the remote audit type, conducting remote audits, and/or adapting audit policies, etc.

For example: Where assurance providers assess the conditions for hybrid or fully remote audit eligibility and/or take part in audit eligibility decisions, they must do one or several of the following:

- Seek permission (RA) or inform the scheme owner of hybrid audit or audit type chosen
- Monitor and document the reasons why on-site audits are not possible
- Develop policies and/or procedures for remote audits (AWS, FSC, FTUSA, GLOBALGAP, RSPO)
- Communicate the procedures and policies with clients and scheme owners about how remote audit types can be used (FSC, FTUSA)
- Maintain lists of remotely audited operations or remotely assessed audit components, and consider whether to make these publicly available (MSC, RTRS)
- Train auditors on remote audit processes and procedures (ASC, ASI, FSC, GLOBALGAP, RSPO)

2.13. Safety preconditions for on-site audits

_Sustainability systems should define the preconditions that need to be in place in order for on-site audits to take place or to resume. These preconditions are often based on a risk assessment or can take the form of a checklist. In addition, sustainability systems should define safety precautions for on-site audits to minimise risk._

_For example:_ SAAS requires that assurance providers conduct an operational risk assessment to identify all certification risks resulting from a decision to return to on-site audits in a place, including:

- Infection risks for CB personnel, client personnel, and other personnel with whom a CB representative may come into contact (such as drivers, translators, etc.);
- CB auditors’ competence in identifying and evaluating client’s COVID-19 (SA8000) issues.

The outcome of the risk assessment specifies short-term, medium-term and long-term controls/actions (including any training and familiarization) needed to mitigate residual risks for the scope(s) of activity by country or region. CBs are required to repeat the operational risk assessment periodically, as needed, to further identify, evaluate and mitigate risks associated with changing circumstances.

_For example:_ Fair Trade USA assurance providers are required to implement heightened safety precautions when returning to onsite audits. In addition to any specific guidance provided by each programme, at a minimum this shall include the following:

a) All legal permissions/permits required to travel and conduct onsite activities are obtained;

b) Any applicable quarantine requirements are fulfilled;

c) Time spent onsite is minimized to focus on the parts of the audit that require onsite verification;

d) Logistics onsite are arranged to minimize risks, including observing social distancing, use of personal protective equipment (PPE), and minimizing time spent indoors, as well as any protocols required by the specific facility or site.
3. Audit Implementation

Where audits have relied traditionally on on-site assessments of performance, the remote audit turns this approach on its head. Every aspect of the audit process is likely to be affected. This section walks through the steps in the audit process and how these should be adapted for remote auditing.

3.1. Pre-audit planning

*Sustainability systems should define the steps that need to be taken both by the assurance provider and by the client in preparation for a remote audit.*

For example: ASI (Assurance Services International) sets out some general considerations that should be taken into account when planning a remote audit, including that a longer preparation time will be needed; that assessors need to be flexible and adaptable; that there is a greater risk for misunderstanding through the use of virtual communications tools; that concentration may be affected and can impact audit duration and need for breaks; and that there is need for a contingency plan should technology fail.

For example: FSC requires that assurance providers and certificate holders shall:

- have the technical and operational capacity to conduct audits remotely, and
- agree on a secure and confidential data transmission, and
- ensure the availability of key staff.

For example: Guidance from ISO 9001 Auditing Practices Group\(^2\) suggests planning steps specific to remote audits can include:

- assess and document feasibility and risks with the auditee;
- determine the different ICT used and how they will be used;
- define the agenda, accommodating dispositions different from an on-site audit (e.g. better definition of tasks by different team members);
- have the organization identify the people to be audited and ensure their availability at defined times;
- test the use of ICT before the audit to confirm there is a stable connection and people know how to use the technology.

3.2. Client preparation

*Sustainability systems should define a list of documents and information to be provided by the assurance provider to clients in advance of a remote audit and a list of information to be provided in advance by the client to the assurance provider.*

For example: BCI requires the following information is sent to clients prior to the audit: planned activities, documents and records to be requested, Dropbox or equivalent document pathway, Remote Audit Process document, requests that field facilitators are notified, request for the names of field facilitators, and request to confirm appropriate communications platform.

---

For example: RA requires the following information is provided to the client: list of documents to be provided by the client in advance of the audit, sampling methods, date by which information is needed (at least 5 days before audit date), sites to be assessed for groups or chain of custody multi-site operations.

3.3. Facilitators (for hybrid audits)

*Sustainability systems should consider the use of facilitators in hybrid audits to support on-site technical review of standard requirements.*

Facilitators are individuals who are not qualified as auditors in the sustainability system (but may have other auditing qualifications) and who act as the eyes and ears for the remote audit team. Remote audits are made possible in some cases only by the use of on-site facilitators to supplement the remote assessor. As a future practice, well-planned facilitator involvement may also help reduce overall audit costs compared to on-site audits.

For example: ASC requires that the facilitator shall only follow live instructions of the auditor and cannot in any case replace the auditor in conducting evaluations or reaching compliance conclusions. When using a facilitator, the communication with the remote auditor shall be synchronic (as opposed to asynchronous) at least during 80% of the audit time.

For example: Facilitators in the RSPO system are either the CB’s employee or contractor, are not qualified as an RSPO auditor or lead auditor, but support the audit team in performing the on-site audit by being the eyes and ears of the audit team on the ground. RSPO sets the following requirements for use of facilitators:

- The number of CB Audit Facilitators required for the audit shall be as appropriate to the number of auditors in the audit team.
- The audit person days of the Audit Facilitator shall not be accounted as audit person days of the CB’s audit team.
- The Audit Facilitator shall not at any point replace or take over the role of the CB’s audit team, even in case of a technology problem.
- The Audit Facilitator shall not participate in writing the CB audit report and/or the CB audit findings.

3.4. Interpreters

*Sustainability systems should define how interpreters can function in a remote audit.*

For example: IOAS suggests that on-site interpreters can simply translate the words of the interviewee. If the interpreter is on-site, ideally they can also function as the camera operator, with an earphone to be able to relay the conversation between assessor and client without disturbing the inspection.

3.5. Assessment Process

*Sustainability systems should, at minimum, define how each of the requirements in their standard is to be assessed, the methodology for doing so, and what evidence is to be provided. This delineation should include which requirements can be assessed remotely and which require on-site verification.*

With a remote audit, technically the audit process starts with the desk-based review of documentation provided by the client. Once that initial assessment has been completed, the main focus of the remote audit itself is the virtual communication with the client, workers, and stakeholders to gather additional evidence. Depending on
the type of assessment process chosen, each option can then be supported by a variety of communication and information gathering technologies.

**For example:** LEAF Marque have developed the Evidence for Remote Audits spreadsheet, which identifies what evidence is required and the alternatives available for each Control Point.

### 3.6. Audit duration

*Sustainability systems should recognise that remote audit planning is likely to take longer than regular audit planning, but that there may be efficiency gains in on-site audit duration.*

**For example:** ASI (Assurance) suggests there could be variation in the timeframe to conduct the assessment and fragmentation of activities spread over the course of a longer period of time (e.g. 4hr/day for 3 days).

### 3.7. Implications for Fees

*Sustainability systems should examine their fee structure and rationale, taking into consideration how fees are impacted by the absence of travel costs and travel time, and by increased audit planning and preparation time.*

**For example:** IOAS Remote assessments of CB offices or CB inspections will be charged without travel time and costs. In all cases however, 0.5 day is charged to allow for preparation and 1 day is charged for reporting.

### 3.8. Audit Decision-making

*Sustainability systems should define the types of decisions on compliance that can be taken as a result of a remote audit and the implications of such decisions on certification status.*

**For example:** RA allows for the following forms of decision: 1) Issue no certification decision until an on-site audit has been completed; 2) Issue a positive certification decision based on the results of the remote audit alone; 3) Issue a positive certification decision with a limitation on volume until the on-site assessment is conducted.

### 3.9. Audit reporting

*Sustainability systems should consider how the audit report format needs to change for remote audits and what additional information is required to be included.*

As the nature and format of data and information collected through the remote audit is likely to be quite different from the traditional audit process, consideration should be given to how additional information will be captured and reported, and any implications for data privacy and confidentiality (see section 4.5).

**For example:** ASI (Aluminium) includes an ‘Unable to Rate’ option that provides the opportunity for the auditor to note interim findings but temporarily hold off from a final conclusion on conformance, until such time as the full assessment can be completed during a subsequent onsite audit.

**For example:** ASC requires that the assurance provider shall record in the audit report: that the audit has been carried out (assisted) remotely; methodologies and tools used to collect evidence during the (assisted) remote audit; and which standard indicators were not evaluated.
3.10. Oversight requirements for remote auditing

*Sustainability systems should define oversight requirements for remote witness auditing of assurance providers. The witness auditing should include at least remote assessment of the assurance providers’ management systems (proxy for office audit) and remote witnessing of the assurance provider assessing clients.*

Remote oversight witness audits can be of a remote assurance audit or an on-site assurance audit (where the assurance provider has local auditors able to conduct the assessment on-site).

For example: ASI will join e.g. phone calls or web conferences between assurance provider and client, including opening and closing meetings, interviews with the client’s personnel, etc. In addition, ASI evaluates the assurance provider’s document review that happens during a remote audit, as well as other audit-related documentation - the same process as for on-site witness assessments.

3.11. Publicly available information

*Sustainability systems should require that publicly available information about an assessment includes at least information about how the audit was carried out (e.g. on-site, remote, or hybrid).*

For example: MSC requires that assurance providers shall document in the assessment announcement and the assessment/audit report the information on the restrictions or health risks which have prevented the on-site audit.
4. **Data Management and Technology**

Remote auditing practices have focused initially on how to manage for higher risks to the integrity of the audit process inherent in remote data gathering. However, it can be useful to approach remote auditing proactively as an opportunity to improve data gathering, management and analysis, and to strengthen the quality and integrity of the audit process as a result. This section focuses on considerations for how to integrate data and technology effectively into the remote audit process. Further reading on this topic can be found in this complementary ISEAL guide on Using technology and Data to enable and enhance remote audits.

4.1. **Good data management practices**

Sustainability systems that choose to integrate new sources of data into risk assessment and compliance assessment processes should ensure they have sufficiently robust data management practices and processes in place to support effective audit processes.

Elements of good data management are described in the ISEAL Assurance Code v2, and more detailed resources on good data and information management are available on the ISEAL Platform.

4.2. **Selecting technology for remote audits**

Sustainability systems should evaluate which technologies to use for different aspects of the remote audit. They should ensure their assurance providers inform the clients and their audit personnel, confirming the client’s understanding of how the chosen technologies will be used and their competence to do so.

Factors that influence the choice of technology include: up-front and running costs; the type, quality and relevance of data made available; client accessibility and comfort in using the technology; and data collection (consent), storage (personal data), and use (privacy, security) considerations.

**For example:** Any type of virtual interview will need to be supported by a choice of video conferencing software (Zoom, Skype etc.). Making the right choice of which video conferencing tool to use may depend less on your preferences and more on what works best for the client. This can depend on which platform they have access to, geographical context, bandwidth, and connectivity. There is a chance that cultural contexts and remoteness of location will also play a factor here and you should not assume that everyone will have the same comfort level being on camera. Rather than being prescriptive on which tool to use, it can be more useful to build in flexibility of options within the assurance policies, while being more prescriptive on the desired outcomes.

**For example:** The importance of selecting appropriate technology for the purposes of remote auditing is addressed in normative references such as IAF MD 4: 2018 which covers the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes.

**For example:** Global GAP requires that before the remote inspection takes place, the CB shall:

a) Determine the platform (e.g., virtual meeting app, wearable technology, telephone/video call, messaging app, drones, or other platforms, etc.) for hosting the inspection. This platform needs to be agreed upon between the CB and the producer.

b) Explain to the producer which documents, activities, facilities are expected to be inspected via video streaming (real time) and which will be evaluated based on records/recorded information, and additionally, if applicable, which people need to be interviewed.
c) Test the ICT platform compatibility between the CB and the producer prior to inspection. A trial meeting using the same media platforms agreed upon shall be conducted to ensure the scheduled inspection can be performed as planned.

d) Encourage and consider the use of webcams, cameras, etc. when physical evaluation of an event is desired or necessary.

e) If the remote inspection is impossible due to technical constraints, (e.g., no phone or internet connection on the farm, etc.) GLOBALG.A.P. Remote cannot be used as an option for inspection.

For example: ASI (Assurance) sets out the following guidelines for use of technology:

- The Assessor, in agreement with the CAB, shall decide on the conference software (e.g. Zoom, Go-To-Meeting, Skype for Business, WebEx, etc.) for hosting the audit.
- Recommends the use of webcams, cameras, etc. throughout the audit
- The auditor shall schedule a test call with the CAB prior the audit to verify if selected tech is and connections are suitable.
- All participants should dial in individually to ensure good sound quality and to allow each person to share screens and to have face-to-face interaction.

4.3. Accessing client data

Sustainability systems should set guidelines for how and under what timeframe the client should make data and information available during the audit.

For example: ASI (Assurance) suggests that during the audit, the audit team should document when the transmission of information or evidence appears to be impossible/not an option, and should focus on what can be done, moving on when limitations arise. When records or documents are reviewed during the Assessment, this should be done via screen sharing to reduce the amount of data and information that has to be transferred between the assurance provider and ASI.

For example: BCI Data access timing: While the assessment is taking place, the assessor reserves the right to request that documents are submitted within a 2-hour timeframe.

For example: GLOBALGAP requires assurance providers to make efforts to confirm what was heard, stated, and read throughout the inspection.

4.4. Data privacy and consent

Sustainability systems should comply with the EU GDPR by minimizing the collection and use of personal data (often referred to as data that could identify an individual or natural person), and should seek consent from individuals for the specific uses of information they are collecting from those individuals.

The EU’s General Data Protection Regulation (GDPR)¹ requires organisations to conduct due diligence to identify and assess the personal data they process, while only collecting personal data that is required for execution of essential activities.

¹ https://gdpr-info.eu/
For example: ASI (assurance) requires that all information sent by the assurance provider shall be securely managed in accordance with ASI’s confidentiality and data privacy policies. In the audit, all audit participants shall be identifiable with their full name and the assurance provider shall confirm who is present during the assessment.

For example: ASC requires that only the data needed for the audit process is recorded. Regarding worker interviews, data is only recorded with explicit consent of the interviewees. Afterwards the interviewees verify and sign a checklist provided by the auditor containing at least the medium of recording, date of recording, a short description, and duration of storage of all that was recorded as part of the audit.

For example: RSPO requires that recording of audit evidence shall be done in line with contractual agreements with clients and respecting the confidentiality of information / proprietary rights of client. Pictures may only be taken upon consent of the involved parties. Similarly, recording of videos or audio material can only be done upon consent of the involved parties.

For example: ISO 9001 APG states that it is good practice that when documented information is to be analysed in an asynchronous manner, it should be shared in a secure and agreed system, such as cloud-based Virtual Private Networks (VPNs) or other file-sharing systems. Once the audit is complete, the auditor should delete from its system or remove access to any documented information and records not required to be retained as objective evidence. Auditors should not take screenshots of auditees as audit evidence. Any screenshots of documents or records or other kind of evidence should be previously authorized by the audited organization.

4.5. Data security

Sustainability systems should require that anyone handling (collecting, storing, analysing) data related to the assessment process has adequate security practices in place to maintain the integrity, access permissions, and confidentiality of the data in accordance with their data governance policy.

For example: ASC assurance providers are required to collect and store all data using up-to-date security practices. These measures include access control to the data collected and encrypted transmission of data, for instance when uploading and/or emailing. Additionally, they are not to store data beyond a required timeframe. The assurance provider shall specify how long each recorded file will be kept on their servers.

For example: RA suggests that the viability of remote audits depends on assurance providers checking that full confidentiality, security and data protection is ensured for all data shared during the audit. This may require specific agreements between the Certificate holder and the assurance provider for the use of recordings, etc.

4.6. Gathering information from workers

Sustainability systems should define steps to ensure the integrity and confidentiality of remote worker interviews and to avoid compromising the safety of interviewees.

For example: Goodweave puts the following steps in place when carrying out remote worker interviews:

- Enumerators read an informed consent script that describes the research project, voluntary nature of participation, and data confidentiality protocols.
- Respondents are not interviewed if they did not provide consent.
- Enumerators are trained to speak conversationally and record personal stories or quotes that convey the respondents’ experiences.
Interviews are anonymized.

Enumerators do not record or request any personally identifying information.

Completed questionnaires and the database are kept on a secure server accessible to only two staff.

All paper files and notes are destroyed.

**For example:** The following is a list of other good practices distilled from a range of sustainability systems:

- During assurance provider interviews, the local facilitator shall ensure that the client’s representatives do not interfere, that the interviews can be performed in confidence, and that the workers’ anonymity is maintained. (RSPO)

- The technology and tools shall allow auditors to confirm interviewee identity. The client may not record the interview themselves. (ASC)

- It is important to use video to see facial expression and body language and ensure interviews can be conducted in confidence. (Preferred by Nature)

- As much as possible, the assessor should aim to use video while conducting remote interviews. Where video is not possible, voice calls can be conducted as a substitute. (BCI)

- Ensure capture of the time and geo-reference the interview location in the report. (GlobalGAP)

**4.7. Remote locations and accessibility**

*Sustainability systems should have procedures in place for how to gather information from remote locations where internet or cellular access may be limited. They should also consider whether any new system requirements limit accessibility to their programme, particularly from disadvantaged groups and indigenous peoples.*

Consideration can include:

- carefully evaluating the conditions of using remote audits (based on stakeholder group),

- evaluating entry barriers like technology accessibility and cost, and

- evaluating inherent discrimination from client risk assessments (e.g. whether risk profiles are potentially discriminating against specific countries or stakeholder groups).

FEASIBILITY AND RISK ANALYSIS FOR REMOTE AUDITS

1. Confidentiality, Security and Data Protection (CSDP)
   - Ensure agreement between auditor and auditee about CSDP issues.
   - Document any arrangements to ensure them.

2. Use of ICT
   - There is a stable connection with good online connection quality
   - The ICT allows access to relevant documented information including software, databases, records, etc.
   - It is possible to make the authentication/identification of interviewed people preferably with image
   - If observation of facilities, processes, activities, etc., is relevant to achieve audit objectives, it is possible to access them by video

3. People in the organization
   - It is possible to access and interview people relevant for the QMS

4. Operations
   - If the organization is not operating regularly, due to contingency situations, the processes/activities being performed are representative and allow fulfilment of the audit objectives

5. Complexity of the organization and Audit Type
   - In case of complex organizations, processes, or products and services and where the objectives of the audit type require full assessment of the standard and wider sampling (e.g. initial assessment or reassessment) a careful analysis of feasibility of remote audits to fully evaluate the organization conformity to all requirements should be performed.

6. Conclusions
   - The audit objectives can be attained with the remote audit - proceed to remote audit
   - The audit objectives can be achieved partially - a remote audit may be done partially and later complemented with a on-site audit
   - The audit objectives cannot be attained via remote audit

7. Validate risk analysis with audit programme manager
This work was funded by a grant to ISEAL from the Sustainable Trade Initiative (IDH)