

Performing EASA Compliant Remote Audits (Part CAO)

The Use of Information and Communication Technologies (ICT) for Performing Remote Audits

Sofema Aviation Services (SAS) www.sassofia.com considers the EASA regulatory requirements regarding the performance of remote audits specifically within an EASA Part Combined Airworthiness Organisation (Part CAO) I.A.W Amendment 1 *ED Decision 2022/011/R*

Introduction

GM1 CAO.A.100(b) and CAO.B.055 Quality system and organisational Annex VI to ED Decision 2021/009/R Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Annex Vd (Part-CAO) to Commission Regulation (EU) No 1321/2014 - Issue 1 — Amendment 1 Review *ED Decision 2022/011/R*

The Use of Information and Communication Technologies (ICT) for Performing Remote Audits (Similar provisions to those in [GM1 145.A.200\(a\)\(6\)](#) and [145.B.300](#) apply.)

ED Decision 2022/011/R - The use of information and communication technologies (ICT) for performing remote audits

This GM to support:

- competent authorities when overseeing regulated organisations;
- regulated organisations when conducting internal audits/monitoring compliance of their organisation with the relevant requirements, and when evaluating vendors, suppliers and subcontractors.

‘remote audit’ means an audit that is performed with the use of any real-time video and audio communication tools instead of the physical presence of the auditor on-site; the specificities of each type of approval need to be considered in addition to the general overview (described below) when applying the ‘remote audit’ concept;

‘auditing entity’ means the competent authority or organisation that performs the remote audit;

‘auditee’ means the entity being audited/inspected (or the entity audited/inspected by the auditing entity via a remote audit);

It is the responsibility of the auditing entity to assess whether the use of remote ICT constitutes a suitable alternative to the physical presence of an auditor on-site in accordance with the applicable requirements.

The Conduct of a Remote Audit

- Documented procedures
 - Flexible and non-prescriptive in nature to optimize the conventional audit process.

- Adequate controls are defined to avoid compromising the integrity of the audit process.
- Security and confidentiality maintained

ICT Audit May Include:

- Meetings by means of teleconference facilities, including audio, video and data sharing;
- Assessment of documents and records by means of remote access, in real time;
- Recording, in real time during the process, of evidence to document the results of the audit, including non-conformities, by means of exchange of emails or documents, instant pictures, video or/and audio recordings;
- Visual (livestream video) and audio access to facilities, stores, equipment, tools, processes, operations, etc.

Pre-Audit Agreement

- Determining the platform for hosting the audit;
- Granting security and/or profile access to the auditor(s);
- Testing platform compatibility between the auditing entity and the auditee prior to the audit;
- Considering the use of webcams, cameras, drones, etc. when the physical evaluation of an event (product, part, process, etc.) is desired or is necessary;
- Establishing an audit plan which will identify how remote ICT will be used and the extent of their use for the audit purposes to optimize their effectiveness and efficiency while maintaining the integrity of the audit process;
- Time zone acknowledgement and management to coordinate reasonable and mutually agreeable convening times;
- A documented statement of the auditee that they shall ensure full cooperation and provision of the actual and valid data as requested, including ensuring any supplier or subcontractor cooperation, if needed; and
- Data protection aspects.

The following equipment and set-up elements should be considered:

- The suitability of video resolution, fidelity, and field of view for the verification being conducted;
- The need for multiple cameras, imaging systems, or microphones, and whether the person that performs the verification can switch between them, or direct them to be switched and has the possibility to stop the process, ask a question, move the equipment, etc.;
- The controllability of viewing direction, zoom, and lighting;
- The appropriateness of audio fidelity for the evaluation being conducted; and
- Real-time and uninterrupted communication between the person(s) participating to the remote audit from both locations (on-site and remotely).

Concerning Competence

When using remote ICT, the auditing entity and the other persons involved (e.g. drone pilots, technical experts) should have the competence and ability to understand and utilize the remote ICT tools employed to achieve the desired results of the audit(s)/assessment(s).

- The auditing entity should also be aware of the risks and opportunities of the remote ICT used and the impacts they may have on the validity and objectivity of the information gathered.
- Audit reports and related records should indicate the extent to which remote ICT have been used in conducting remote audits and the effectiveness of remote ICT in achieving the audit objectives, including any item that has not been able to be completely reviewed.

Regulation (EU) 2021/1963 Competent Authority Requirements

The competent authority shall verify:

- Full with applicable requirements prior to issuing an organisation certificate;
- Continued compliance with the applicable requirements of the organisations it has certified;
- The implementation of appropriate safety measures mandated by the competent authority in accordance with points [145.B.135\(c\)](#) and [\(d\)](#).
- This verification shall:
 - Be supported by specific guidance documentation to perform their functions;
 - Provide the organisations concerned with the results of oversight activities;
 - Be based on assessments, audits and inspections and, unannounced inspections;
- Provide the competent authority with the evidence needed in case further action is required, including the measures provided for in point [145.B.350](#).
- The competent authority shall establish the scope taking into account the results of past oversight activities and the safety priorities.
- If facilities located in more than one State CA may transfer responsibility to other CA),
- Other Member States - The CA shall other CA before performing any on-site audit or inspection of the facilities.
- The competent authority shall collect and process any information deemed necessary for performing oversight activities.

Next Steps

Sofema Aviation Services www.sassofia.com & Sofema Online www.sofemaonline.com provides Classroom, Webinar & Online EASA compliant regulatory Training – for additional guidance or information please email team@sassofia.com