European Union Aviation Safety Agency

FAQ n.116561

FAQs:

Continuing airworthiness - General, Continuing Airworthiness, Regulations

Question:

How to use information and communication technologies for performing remote audits on to DOA, LoA/POA, AMO, CAMO, CAO and AMTO holders*?

Answer:

Objective of this document:

This document provides technical guidance on the use of remote information and communication technology (ICT) to support:

- the competent authorities when performing the oversight of regulated organisations and
- the industry when conducting internal audits / monitoring compliance of the organisation with the relevant requirement and when performing evaluation of suppliers and subcontractors.

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

In the context of this document, “remote audit” is understood as an audit performed with the use of any real-time video and audio communication tools in replacement of the physical presence of the auditor on-site. Specificities of each type of approval / letter of agreement need to be considered in addition to the below general overview when applying the “remote audit” concept.

1. Conduct of remote audit by a Competent Authority

Competent authorities who decide to use remote audit should describe the remote audit process in their documented procedures and should consider at least the following elements:

- Methodology for the use of ICT is sufficiently flexible and non-prescriptive in nature to optimise the conventional audit process.
- Adequate controls are defined and in place to avoid abuses that could compromise the integrity of the audit process.

- Measures to ensure that security and confidentiality are maintained throughout the audit activities (data protection and intellectual property of the organisations also need to be safeguarded).

Examples of use of ICT during audits may include but are not limited to:

- 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 (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.

An agreement between the competent authority and the organisation should be established when planning a remote audit which should include:

- determining the platform for hosting the audit (e.g. Go-To-Meeting, WebEx, Microsoft Lync, Microsoft TEAMS, etc.);
- granting security and/or profile access to the auditor;
- testing platform compatibility between the competent authority and organisation prior to the audit;
- considering the use of web-cams, cameras, drones, etc. when physical evaluation of an event (product, part, process, etc.) is desired or necessary;
- establishing an audit plan which will identify how ICT will be used and the extent of its use for the audit purposes to optimise its effectiveness and efficiency while maintaining the integrity of the audit process;
- if necessary, time zone acknowledgement and management to coordinate reasonable and mutually agreeable convening times;
- a written statement of the organisation that they 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 elements of the equipment and setup 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 performing the verification can switch between them, or direct them to be switched and has the possibility to stop the process, ask a question,

move 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.

When using ICT, the competent authority and other involved persons (e.g. drone pilots, technical experts) should have the competency and ability to understand and utilize the ICT tools employed to achieve the desired results of audit(s)/assessment(s). The competent authority should also be aware of the risks and opportunities of the ICT used and the impacts that they may have on the validity and objectivity of the information gathered.

Audit reports and related records should indicate the extent to which ICT has been used in carrying out remote audit and the effectiveness of ICT in achieving the audit objectives, including any item that was not able to be completely reviewed.

2. Internal Audits performed by approved organisation and evaluation of its suppliers and subcontractors

The considerations described in paragraph 1 may also be applied by approved organisations when conducting internal audits / monitoring compliance of the organisation with the relevant requirements and when performing evaluation of suppliers and subcontractors. The application of “remote audit” concept should be described in a documented procedure accepted / approved by the Competent Authority.

** DOA: Design Organisation Approval; LoA/POA: Letters of Approval/Production Organisation Approval; AMO: Maintenance Organisation Approval; CAMO: Continuing Airworthiness Management Organisations Approval; CAO: Combined Airworthiness Organisation Approval; and AMTO: Maintenance Training Organisation Approval*

Last updated:
19/07/2020

Link:
https://www.easa.europa.eu/it/faq/116561