

Remote audit provisions relating to the JFS-C Certification Program (Applicable to Ver. 3.0 and later)	Issue date: Nov. 10, 2020	Document number: C01P18
	Revision date:	Revision number: R00

Remote audit provisions relating to the JFS-C Certification Program

(Applicable to Ver. 3.0 and later) ¹

Preface

These provisions are based on the JFS-C Certification Program (hereinafter the “Program”) and managed by the Food Safety Management Association (hereinafter “JFSM”), which is the certification program owner (CPO), and they establish the procedures for conducting following audit activities remotely under IAF MD4:2018: office audits of certification bodies, witness on remote audits, witness for evaluation of auditor’s skills, and on-site verifications.

1. Purpose

The purpose of these provisions is to enable audits, on-site verifications, and witness for auditor skill evaluations based on this Program that are to be conducted in the event that, due to emergencies or special circumstances, on-site implementation has been determined to be difficult to undertake. These provisions are established to ensure the integrity of audits and to enable audit activities to be conducted with minimal risk to food safety under the circumstances listed below, by enabling the audits to be partially conducted remotely and combined with on-site audits to be conducted at a later date.

- 1) When there are immigration or movement restrictions by the government of the country or region where the organization to be audited is located
- 2) When there are immigration or movement restrictions by the government of the country or region when the audit activities are to be audited
- 3) When auditors raise concerns that their health or safety may be jeopardized by the movement
- 4) When the organization to be audited raises concerns that the work of the organization may be jeopardized by the entry of auditors

2. Definition of ICT-based remote audits

Information and communication technology (ICT) relates to the collection, storage, reading, processing, analysis and transfer of information by means of hardware such as smartphones, mobile devices, computers, drones, video cameras and wearable devices, and includes software such as applications and artificial intelligence that control the hardware.

When an on-site audit that originally involves the audit activity of visually confirming the on-site situation cannot be performed for any reasons listed above, ICT, as applied in these provisions, is a technology that enables the on-site confirmation to be conducted remotely. Therefore, ICT-based remote audits can be applied to all audits that originally requires on-site visual confirmation including usual on-site audits, witness-audits, verification of correction and corrective action, and witness for evaluation of auditor’s skills.

3. Requirements for remote audits

- 1) Requirements for adopting remote audits

In order to conduct a remote audit for the above reasons, the auditing party shall document the procedure to meet the following requirements and follow the prepared procedure to reach an agreement with the party to be audited regarding the necessity and implementation of the remote audit.

Remote audit provisions relating to the JFS-C Certification Program (Applicable to Ver. 3.0 and later)	Issue date: Nov. 10, 2020	Document number: C01P18
	Revision date:	Revision number: R00

- ① Both parties shall recognize that a remote audit is an auditing method that may be used when an on-site audit is not possible.
- ② Both parties shall agree that the situation requiring the remote audit may continue beyond the due date of the audit.
- ③ Both parties shall agree that as soon as the situation requiring the remote audit is resolved, it is assumed that on-site audit will be conducted.
- ④ No risk shall be anticipated by executing remote audit based on the past nonconformity history or other information.
- ⑤ Both parties shall mutually agree on the implementation and cooperation of the remote audit.
- ⑥ Both parties shall agree on measures to be taken when information transfer using ICT does not operate as expected.

2) Requirements for the use of ICT

In order to conduct visual check on the on-site practice remotely, information transfer using ICT shall meet the following requirements.

- ① Information required by the auditing party can be accurately transferred
- ② Information required by the auditing party can be adequately transferred
- ③ Information required by the auditing party can be transferred without delay
- ④ No doubt on the authenticity of the information transmitted to the auditing party.
- ⑤ No leakage or theft possible when information is transferred, stored or used.
- ⑥ Appropriate system and environment are available at both the auditing party and the audited party to support the use of ICT.

4. Scope of remote audits

The scope of remote audits is normally the same as the applicable scope of the on-site audits of certification bodies conducted by the CPO in the operation of this Program, to include witness on remote audits, on-site verifications and witness for evaluation of auditor's skills, periodic audits, on-site audits of the first initial audit, and recertification audits. However, the scope for which verification is required in the following section 5 is out of the scope of application for remote audits.

5. Scope of application that requires verification by on-site audits

The following parts of the verification of manufacturing operation in the recertification audits shall be verified by on-site audits in order to ensure the integrity and reliability of audits required by this Program.

- ① Verification of on-site practice for operations related to the critical control points (CCPs) and the occurrence of food safety hazards
- ② Verification of activities of workers who engage with operations related to the CCPs and the occurrence of food safety hazards

Remote audit provisions relating to the JFS-C Certification Program (Applicable to Ver. 3.0 and later)	Issue date: Nov. 10, 2020	Document number: C01P18
	Revision date:	Revision number: R00

6. Requirements and deadlines for measures taken after audit results

- 1) In the periodic audits, the audit can be completed remotely only when no critical or major nonconformity is identified. When a minor nonconformity is pointed out, correction or corrective action are required to be performed within 30 days, and the status of the correction or corrective action can be confirmed remotely. However, corrections or corrective actions confirmed remotely shall be re-confirmed on-site at the next audit. In addition, the facts confirmed remotely shall be clearly stated in the audit report, and the facts re-confirmed in the next on-site audit shall also be noted in that audit report as re-confirmed facts from the previous remote audit.
- 2) For recertification audits, the duration from the date of the remote audit to the completion of all audit activities when conducting the above verification by means of an on-site audit shall not exceed 30 days. If the audit cannot be completed within this 30-day deadline and needs to be extended, the risks posed by the postponement of the completion of the audit shall be evaluated and a process shall have been established to set an appropriate extension deadline according to the assumed level of risk. Even when a risk posed by the postponement of the completion of the audit is not anticipated, all audit activities shall be completed within a maximum of 90 days from the start of the audit.
- 3) When an on-site audit cannot be completed within the deadline due to unforeseen circumstances even though a recertification audit has been started remotely and the certification period has expired, the certification shall be begun again from an initial application.
- 4) Regardless of the type of audit, if a critical or major nonconformity is found during a remote audit, the same measures and response period allowed for usual on-site audit shall apply, and a re-audit or verification of correction or corrective actions shall be conducted on-site.
- 5) The audit report shall clearly state that the audit was conducted remotely, the audit report shall be prepared when the audit is completed in accordance to the level of nonconformity mentioned above, and after the audit results are proven by reviewer those information shall be entered in the database. (In the remarks column of the database, state that the audit was a remote audit.)

7. Remote audit labor-hours

- 1) When the requirements described in 2) of the above section 3 are met, the man-days for a remote audit shall be the same as for an on-site audit, and the man-days specified in the JFS-C Certification Program Document shall be followed. Even when the requirements described in 2) of the above section 3 have been confirmed, fatigue and break time shall be taken into consideration for additional workload due to handling of a large amount of information, processing time due to the communication transfer speed, the use of ICT equipment, etc., but such conditions are not included in the man-days. When it is necessary to assign a professional technician to operate the ICT equipment, this requirement can be added to the man-days. Records including the basis for the determination of the man-days shall be kept in the same way as for usual on-site audits.

Remote audit provisions relating to the JFS-C Certification Program (Applicable to Ver. 3.0 and later)	Issue date: Nov. 10, 2020	Document number: C01P18
	Revision date:	Revision number: R00

- 2) When a recertification audit has been started remotely and the certification has been expired because it took 90 days or more before the completion of the on-site audit, the certification will be revoked according to 3) in section 6. When a reapplication is begun within six months after that and the remote audit part performed before the expiration indicates conformity, the man-days of the remote audit part can be deducted from the initial audit man-days based on the reapplication. The basis for calculating the man-days shall be recorded. (Minimum audit labor-hours shall be two labor-days or more.)

8. Composition of the audit team

When special hardware or software is used for the application of ICT, assistants required to perform those operations can participate in the audit team. However, such assistants shall not be involved in conducting the audit itself.

9. Audit report

The audit report is prepared in the same way as for an on-site audit, but it shall clearly state that the audit was conducted remotely, and that each requirement item was verified remotely. The items that have been verified by an on-site audit as described in item 5 above shall also be recorded in the audit report.

10. Management of transferred information

As a general rule, all information transferred for remote audits shall be saved in storage under secure conditions in the same way as information obtained during usual on-site audits, and at a minimum, this information is to be stored until the technical review of the audit report, certification, and determination on the continuation of certification and recertification are completed. Thereafter, management and disposal of the information shall be conducted in accordance with the agreement with the certification body.

¹ Disclaimer: This translated document is provided for information purposes only. In the event of a difference of interpretation or a dispute, the original Japanese version of this document is binding.

Revision History

Version	Issue Date	Revision History
R00	November 10, 2020	First edition