FOOD SAFETY SYSTEM CERTIFICATION 22000

ANNEX 9: CB REQUIREMENTS FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

Version 5.1 | November 2020

CONTENTS

1. PURPOSE

This Annex describes the requirements for the use of Information and Communication Technology (ICT) by Certification Bodies linked to FSSC 22000 audit activities.

2. SCOPE

The scope of this document covers the following:

- Conducting FSSC 22000 audits using Information and Communication Technology (ICT)
- CB Auditor requirements and activities

ICT is the use of technology for gathering, storing, retrieving, processing, analyzing, and transmitting information. It includes software and hardware such as smartphones, handheld devices, laptop computers, desktop computers, drones, video cameras, wearable technology, artificial intelligence, and others. The use of ICT may be appropriate for auditing/assessment both locally and remotely.

As technology evolves and time constraints on businesses increase, there is a need to consider alternative methods of delivering auditing activities whilst still achieving the audit objectives and ensuring a robust audit process.

The IAF Mandatory Document (MD) 4 for the *Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes* (latest version) shall be used by CBs as a normative document in conjunction with the requirements as set out in this Annex.

3. CONDUCTING AUDITS USING ICT

The standard method for conducting FSSC 22000 audits is via full on-site audits as described in Part 3 of the Scheme. An alternative, voluntary option can now be applied where the criteria are met, by delivering the FSSC 22000 audit as a split process utilizing ICT. The ICT audit approach is voluntary and shall be mutually agreed between the CB and the certified organization prior to the audit.

The ICT audit approach consists of 2 main steps:

1) **Remote audit** consisting of a document review and interviews with key personnel using ICT.
2) **On-site audit** focusing on the implementation and verification of the FSMS (including HACCP), PRPs, the physical inspection of the production process and any remaining requirements not covered during the remote audit.

During the **remote audit**, assessment activities are performed from a location other than the physical location of the audited organization while during the **on-site audit**, assessment activities are performed at the physical location of the audited organization.

In the first instance the CB shall conduct an assessment to determine, in conjunction with the certified organization, whether the ICT audit approach is a viable option. The CB shall have documented procedures including criteria for assessing and approving the ICT Audit Approach. This assessment shall be conducted and documented prior to the audit, taking into consideration the members of the audit team and the audited organization.

The following shall be considered when conducting the assessment:

a) Maturity of the certified organization's FSMS and performance history;
b) Whether the certified organization permits and accommodates remote audit activity (i.e. availability of records in electronic format or document reader) including data protection and security measures;
c) The ICT tools to be utilized;
d) Whether the certified organization and/or the CB have the ability to provide representatives capable of communicating in the same language.
e) Whether the CB and the certified organization have the capability and ability to conduct the remote audit in the chosen medium/forum of the remote audit.
f) Impact on audit duration and audit planning e.g. where more time might be required due to the use of ICT.

3.1 GENERAL PRINCIPLES

a) If the ICT audit approach is deemed to be a viable option, ICT means to be used shall be tested with the certified organization before the planned remote audit to confirm that the ICT is appropriate, suitable, and effective. Feasibility also depends on the online connection quality. A weak bandwidth or limited hardware capability may slow the process to the point of inefficiency.
b) Suitable support/training shall be provided on the use of ICT to the auditor and any other members of the audit team, prior to the remote audit. Records of these trainings shall be kept by the CB.
c) The requirements of IAF MD4 shall be followed. This mandatory document defines the rules that certification bodies and their auditors shall follow to ensure that ICT is used to optimize the efficiency and effectiveness of the audit/assessment, while supporting and maintaining the integrity of the audit process.
d) The CB shall include the requirements of IAF MD4 in their procedures for the use of ICT and personnel competence.
e) Data security and confidentiality: to prepare for the use of ICT, all certification legal and customer requirements related to confidentiality, security and data protection should be identified and actions taken to ensure their effective implementation. This implies that both the auditor and the auditee agree to the use of ICT and with the measures taken to fulfil these requirements.
f) Both the remote audit and the on-site audit shall be conducted by a FSSC 22000 qualified auditor for the sub-category.
g) The remote audit component will typically be 0.5 - 1 day and the on-site verification audit the remainder of the total duration of the regular annual audit. The on-site audit component cannot be less than 1 day and shall at least be 50% of the total audit duration. When determining the amount of time spent on-site and remotely, the outcome of the assessment and the historical performance of the organization (including complaints and recalls) shall be taken into consideration. For example, if the assessment demonstrated that a remote audit is possible, but the historical performance of the organization has been of concern, then the proportion of time spent on-site is expected to be increased.
h) The total audit duration based on the calculation in Part 3 of the Scheme rules shall be met between the remote audit and the on-site audit. Where rounding is applied, durations shall be rounded upwards to the nearest half day taking into account that additional time

might be required to conduct the remote audit. Total audit duration does not include preparation activities or reporting, and additional time is required for these activities as defined in Part 3.

i) When compiling the audit plan for the remote audit, consideration should be given to appropriate durations and allow for more frequent breaks to enhance attention and reduce eye strain. These breaks cannot be counted towards audit time.

j) If time is consumed on issues such as network downtime, unexpected interruptions or delays, accessibility problems or other ICT challenges, this time shall not be counted as audit time. Provisions for ensuring audit time must be established.

k) It is recommended that the remote and the on-site audit take place as close together as possible, but in all cases the maximum timeline for completion of the audit (remote + on-site) shall not exceed 30 calendar days.

l) As an exception and only in the case of serious events (see Appendix 1), the timeline for completion of the audit may be extended to a maximum of 90 calendar days, based on a clear and documented concession process and risk assessment by the CB. The risk assessment shall consider the elements in section 3 of IAF Information Document (ID) 3 *Management of Extraordinary Events or Circumstances Affecting ABs, CABs, and Certified Organizations* as a minimum. The extension is only allowed where the efficiency and integrity of the audit will not be compromised. Where concessions are granted by the CB and the 90-day timeline are applied, the risk assessment shall be uploaded to the portal as part of the audit documentation.

m) In all instances where ICT utilized is not functioning properly or preventing/hampering a robust audit, the audit shall be aborted, and suitable follow-up actions determined.

3.2 APPLICABILITY

The ICT audit approach may be applied in the case of the regular, annual FSSC 22000 audits (surveillance and recertification audits) as part of the routine certification process and is additional to Part 3 of the Scheme.

It can also be applied to Stage 1 audits as described below and Head Office audits where the corporate functions are controlled separately.

In the year where an unannounced audit is due, the ICT audit approach outlined in this Annex may be used, whilst still applying the requirements of Part 3, section 5.4 of the Scheme. The prerequisite would be that the on-site part of the audit shall be conducted first, followed directly by the remote audit with a maximum period of 48 hours between the two audit components.

3.2.1 INITIAL AUDITS

The full Stage 1 audit may be conducted off-site (ISO/TS22003 clause 9.2.3.1.3) with the use of ICT. The objectives of the Stage 1 audit as per ISO17021-1 (9.3.1.2.2) shall be met and to this end, ICT (i.e. live video) shall be included to also observe the work environment and facilities. The Stage 1 audit report shall reference that the audit was completed remotely, which ICT tools were used, and the objectives achieved. The Stage 2 audit shall be conducted as a full on-site audit within 6 months of the Stage 1 or the Stage 1 shall be repeated. It is not permitted to use the ICT audit approach for the Stage 2 audit.

3.2.2 SURVEILLANCE AUDITS

Annual surveillance audits may be conducted using the ICT audit approach. The full audit (remote + on-site) shall be completed within the calendar year.

Where the ICT audit approach is applied to the first surveillance audit following an initial certification, the process shall be planned to ensure that the full audit (remote + on-site) takes place before or not later than 12 months after the date of certification decision for the initial audit.

Where the timelines as referenced above are exceeded, the full surveillance audit shall be conducted on-site and in line with the audit program or the certificate shall be suspended.

3.2.3 RE-CERTIFICATION AUDITS

The re-certification audit may be conducted using the ICT audit approach. The remote audit combined with the on-site audit constitutes a complete re-certification audit and both components shall be completed prior to the expiry of the existing certificate. The requirements in ISO/IEC 17021-1: 2015 – 9.6.3.2 apply.

3.3 AUDIT PROCESS

The audit (remote + on-site) shall be conducted by qualified FSSC 22000 auditor/s meeting the competency requirements linked to the scope of certification. In all instances the on-site audit shall be conducted by a FSSC 22000 qualified lead auditor with the sub-category and it is preferred that the same auditor is used for both the remote and the on-site audit to ensure continuity. Where different auditors are used for the remote and on-site audit components, the competency requirements as defined in the Scheme shall be met and the CB shall have a proper handover/communication process in place.

3.3.1 REMOTE AUDIT COMPONENT

The remote audit includes a document review and interviews with key personnel.

The remote audit shall at least include a review of the following key FSMS elements:

- Document/procedure reviews;
- HACCP plans and key changes since the last audit (where applicable);
- Product recalls and significant complaints;
- Status with regard to FSMS objectives and key process performance, management review and internal audits;
- Interviews with management and key personnel;

3.3.2 ON-SITE AUDIT COMPONENT

The on-site audit serves as the verification audit for Food Safety Management System (FSMS) implementation with a focus on the production processes and environment as well as the remainder of the clauses not covered as part of the remote audit.

The on-site audit shall include as a minimum inspection/physical verification of PRPs, the traceability test and implementation of the FSMS. The latter includes, but is not limited to, the HACCP system, for example the effective operation of PRPs, verification of the process flow diagram, OPRP and CCP monitoring and verification. It might be necessary to review parts of the remote audit again to ensure implementation of requirements.

All the requirements of the Scheme shall be covered between the remote audit and the on-site audit components and be clearly reflected in the audit plans, audit program and the final audit report.

3.3.3 NONCONFORMITY MANAGEMENT

Any nonconformities identified during the audit (remote and on-site) shall be addressed in line with the Scheme requirements including grading and timelines and recorded on the NC report aligned to Annex 2.

i. Where the audit (remote + on-site) is completed within 30 calendar days, one nonconformity report is completed and the timeline for nonconformity closure starts at the end of the on-site audit. Any nonconformities identified during the course of the audit shall be communicated to the organization in a timely manner. The CB may opt to provide a provisional NC report to the organization at the end of the remote audit.

ii. In the case of a serious event and where the 30 calendar days for audit completion is exceeded (refer to the exception in 3.1(l)), any nonconformities identified as part of the remote audit shall be recorded and a copy of the nonconformity report left with the certified organization at the end of the remote audit. The timeline for closure of these nonconformities starts at the end of the remote audit. The NC report produced following the on-site audit shall contain an overview of all the nonconformities raised, including the nonconformities raised at the remote audit to provide a consolidated record. The timeline for closure of NCs identified at the on-site audit starts at the end of the on-site audit.

iii. Where a critical nonconformity is identified at any time during the audit (remote or on-site), the certificate shall be suspended, and a full new on-site audit will be required to lift the suspension within 6 months.

ICT tools may be used to close out minor and/or major nonconformities, depending on the nature of the nonconformity and the reliability of the ICT. The CB needs to be able to demonstrate that the methods used are suitable for the resulting action. Critical nonconformities require an on-site follow-up audit in all instances.

3.3.4 AUDIT REPORT

One audit report is produced covering both the remote and the on-site audit components. The audit report shall clearly identify the extent to which any ICT has been used in carrying out the audit and the effectiveness of ICT in achieving the audit objectives. The audit report shall include all summarized information, findings, and nonconformity details of both the remote and on-site audit, covering all Scheme normative requirements and meeting the requirements as set out in Annex 2 of the Scheme. The report shall also reference the dates and the duration of the on-site and remote audits and the auditor/s involved in both parts. The requirements assessed during the remote audit shall be identified by placing a "R" at the beginning of the information.

The full audit pack, consisting of the remote and the on-site audit documentation shall be uploaded to the Portal within 2 months of the last day of the on-site audit. Instructions will be provided separately by the Foundation on the process and requirements for uploading audit information and nonconformities in the portal.

The certification audit is only concluded once both the remote audit and the on-site audit have been successfully completed. Following completion of the full audit (step 1 & 2) and a positive certification decision by the CB, the audit process is complete and where applicable a new certificate may be issued.

4. AUDIT TEAM

4.1 WITNESSING OF AUDITORS

Where appropriate ICT tools are available, this technology may also be utilized for the remote witnessing of existing approved FSSC 22000 auditors as part of the maintenance of competency requirement (3 yearly witness audit) and the requalification process.

The same applies to already qualified FSSC 22000 auditors moving to another CB. Where the new CB deems the remote witnessing to be sufficiently robust, the new CB may use a remote witness audit to approve the FSSC 22000 auditor. Remote witnessing is not allowed for initial auditor approval of FSSC 22000 (auditors new to FSSC 22000).

In all cases where remote ICT tools are used, the CB needs to ensure that the technology is appropriate and enables the witnessor to observe the full FSSC 22000 certification audit, including the opening meeting, document review, on-site facility audit and the closing meeting. It needs to be clearly reflected in the witness audit report that the witness was conducted remotely, and which remote technology was used. Permission will be required from the certified organization to conduct the witness audit in this manner and the normal confidentiality requirements apply. The technology needs to be tested beforehand and the witnessor and the auditor trained in the use of the technology as required in IAF MD4. In all instances where the technology utilized is not functioning properly or preventing/hampering a robust audit, the witness audit shall be aborted, and suitable follow-up actions determined by the CB.

4.2 USE OF TECHNICAL EXPERTS

Technical experts are permitted to join the audit remotely using ICT tools, if the CB has determined that ICT tools are appropriate and sufficient to meet the audit objectives and the certified organization agrees to the remote audit activity. The technology needs to be tested beforehand and the technical expert and the auditor shall be trained in the use of the technology as required by IAF MD4. In all instances where the technology utilized is not functioning properly or preventing/hampering a robust audit, the CB shall make alternative arrangements to ensure the full audit process can be completed or the audit shall be aborted.