FSSC 22000




# FSSC 22000

## FULL REMOTE AUDIT ADDENDUM

Version 2 | February 2024

# CONTENTS



# REVISION HISTORY

| Date Published | Issue | Changes |
|---|---|---|
| **October 2020** | 1 | First publication |
| **February 2024** | 2 | • Editorial changes, and updates made in line with Version 6 of the FSSC 22000 Scheme<br>• Added further detail under Section(s):<br>o 3.2 (d) – upload training records to Assurance Platform<br>o 3.2 (h) – data security and confidentiality<br>o 3.3 – exemption application for unannounced audits<br>o 3.5.2 – audit report and upload to Assurance Platform<br>o 3.5.3 – reference to be made on the certificate |

# 1. PURPOSE

This document describes the requirements for Certification Bodies (CB) when conducting FSSC 22000 audits fully remotely with the use of suitable Information and Communication Technology (ICT) when the premises of the certified organization cannot be accessed as a result of a serious event.

# 2. SCOPE

The standard method for conducting FSSC 22000 audits is either full on-site audits as described in Part 3 of the Scheme, or partial on-site audits using the ICT Audit Approach as described in Annex 5, both of which are GFSI recognized options.

The FSSC 22000 full remote option is an accredited, non-GFSI recognized, voluntary option that can only be utilized where access to the premises of the certified organization is not possible as a direct result of a serious event (refer Appendix 1 of the Scheme), supported by a risk assessment. Mutual agreement between the CB and the certified organization is required prior to conducting the full remote audit.

A full remote audit is defined as an audit that takes place entirely at a location other than that of the certified organization through the use of ICT.

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 document.

# 3. CONDUCTING FULL REMOTE AUDITS

As set out in Part 3, section 5.10 of the Scheme on the Management of serious events, the CB shall conduct a risk assessment to evaluate whether certification can be maintained and review the planned audits when on-site auditing is not possible. A full remote audit may also be considered as an option when planning the audits and where this audit methodology is supported by the feasibility and risk assessments.

## 3.1 RISK AND FEASIBILITY ASSESSMENTS

In the first instance the CB shall conduct a risk assessment to determine the impact of the serious event on the current certification status of the certified organization as set out in Part 3 of the Scheme, clause 5.10. The elements of section 3 in IAF Information Document (ID) 3 *Management of Extraordinary Events or Circumstances Affecting ABs, CABs, and Certified Organizations*, shall be considered. The full remote audit option can only be utilized when the risk of maintaining certification is determined as being low, based on the outcome of the risk assessment.

Secondly, the CB shall conduct a feasibility assessment to determine, in conjunction with the certified organization, whether a full remote audit is a viable option and to determine if the full audit objectives can be achieved through the use of ICT.

The following shall be considered when conducting the feasibility assessment:

a) Maturity of the certified organization's FSMS and performance history;
b) Whether the certified organization permits and can accommodate remote auditing (i.e. availability of records in electronic format or document reader), including relevant data protection and security measures;
c) The ICT tools to be utilized;
d) Whether the certified organization and/or the CB have representative/s 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, covering all parts of the audit, including the production audit; and
f) Impact on audit duration and audit planning e.g. where more time might be required due to the use of ICT.

## 3.2 GENERAL PRINCIPLES

a) For a full remote audit to be conducted, the site needs to be operational with production taking place. In the event that the site has closed and/or no production is taking place, the full remote audit option cannot be applied.
b) The CB shall have documented procedures including criteria for assessing and approving the full remote audit process.
c) If the full remote audit 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.
d) Suitable support and 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 and uploaded on the auditor's register on the Assurance Platform.
e) Use of remote technology shall ensure that adequate controls are in place to ensure a true representation of the site and a robust audit.
f) 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.
g) The CB shall include the requirements of IAF MD4 in their procedures for the use of ICT and personnel competence.
h) Data security and confidentiality: to prepare for the use of ICT, all certification, legal and customer requirements related to confidentiality, security, and data protection shall be identified and actions taken to ensure their effective implementation. This means that both the auditor and the auditee agree to the use of ICT and with the measures taken to fulfil these requirements.
i) The remote audit shall be conducted by an FSSC 22000 qualified auditor(s) meeting the competency requirements linked to the scope of certification as set out in the Scheme, Part 4, Section 3.5.
j) 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 in line with the audit schedule and Scheme requirements.

## 3.3 APPLICABILITY

The full remote audit option is only applicable in the following cases when linked to a serious event:

i. Where the regular, announced FSSC 22000 surveillance or recertification audits are impacted as a result of a serious event and cannot take place on-site;
ii. Transition audits – refer to Part 3, clause 5.8 of the Scheme;
iii. Where follow-up audits to close out nonconformities cannot take place – this will be dependent on the nature of the nonconformity, the suitability of the ICT and the CB shall in all instances be able to justify the effectiveness of the methods used. Critical nonconformities require an on-site follow-up audit in all instances.
iv. To conduct a special audit based on the outcome of the serious event risk assessment.

Full remote audits shall not be applied in the case of unannounced audits, except where an exemption has been applied for and approved by the Foundation. In this case, the ICT shall be tested well in advance of the audit, so as to ensure that the technology is suitable, and the audit can be delivered as unannounced.

In the year where an unannounced audit is due, the ICT audit approach (remote + onsite) outlined in Annex 5 may be used, whilst still applying the requirements of Part 3, Section 5.4 of the Scheme.

Refer to Annex 5 for details on the use of ICT for Stage 1 audits and Head Office audits.

## 3.4 AUDIT PLANNING

There is a need for effective planning for the remote audit to ensure that it achieves stated objectives and minimum audit duration. As a result, more time might be needed for the planning process. The total audit duration based on the calculation in Part 3 of the Scheme shall be met. 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 of the Scheme.

The types of issues to be considered in the planning phase are explained in ISO 19011 clause 6.2.3 Determining feasibility of the audit:

*The feasibility of the audit should be determined to provide confidence that the audit objectives can be achieved.*

*The determination of feasibility should take into consideration factors such as the availability of the following:*

*a) Sufficient and appropriate information for planning and conducting the audit;*
*b) Adequate cooperation from the auditee;*
*c) Adequate time and resources for conducting the audit*

*NOTE: Resources include access to adequate and appropriate information and communication technology.*

It is advisable to obtain supporting information from the certified organization prior to the audit to assist with the audit planning process. Examples of such information may include: a site map, flow diagrams, overview of OPRPs/CCPs, any specific shift patterns as well as any process, production or significant changes brought about as a result of the serious event.

The audit plan and the audit program shall clearly reflect that the audit was conducted fully remotely and linked to a serious event, as well as indicating the different types of ICT used during the course of the audit. 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 duration. 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 towards audit duration. Provisions for ensuring audit duration requirements are met, must be established.

## 3.5 AUDIT

Remote audit activities follow the same principles and format of the on-site audit activities and includes a full audit against the Scheme requirements. It is therefore likely that different types and combinations of ICT will be used during the same audit, that must be reviewed and agreed on as part of the feasibility and risk assessment and audit planning process. The full audit shall be completed in a set timeframe that may be sub-divided over several days for example a 2.0-day audit may be spread out over 3-4 days to allow for sufficient breaks and optimal use of the ICT.

Examples of requirements, activities and processes include:

| Audit activity | Remote interaction |
|---|---|
| <u>Auditing activities</u><br>a. Opening and closing meetings<br>b. Audit plan reviewing at different stages of the audit<br>c. Intermediate conclusions report<br>d. Audit team intermediate meetings where applicable | Video conference<br>Web meeting |
| <u>Organization's processes/activities/people</u><br>a. Interviews<br>b. Processes or activities where the audit object is mainly the review of documents and explanatory information obtained through interview such as purchasing, human resources/training, commercial processes, design, and development. Many of these activities are performed by shared services.<br>c. Infrastructure that has a wide territorial range | Video conference with screen share<br>Realtime video images obtained with drones, mobile or fixed video cameras.<br>Access to video/surveillance monitoring of sites |
| <u>Particular situations</u><br>a. Participation of technical experts | Video conference, real time images, shared screen, asynchronous document, and data review i.e. in a cloud or similar environment. |

When it is required to make adjustments to the audit plan at the opening meeting, the availability and feasibility to use ICT should also be reconfirmed. Measures to ensure confidentiality and data security should also be revised and agreed where applicable.

It is important that the ICT used is suitable to audit the on-site facilities, storage areas and manufacturing processes using streaming/live video with audio capacity through mobile or other wearable technology to allow confirmation of continued implementation of PRPs, observation of practices and processes and interviews with personnel. The site representative will need to take the camera or other video equipment (e.g. a laptop, mobile phone or tablet) into the production, storage, and other areas to enable the auditor to witness, see and question any aspects and replicate an on-site facility and process walkthrough.

When using video for watching online live images, it is important that the organization demonstrates veracity of images. When looking at images of a facility these can be compared with floor plans and flow diagrams for instance. Images of a geographical site that are observed can be compared with available satellite images or information available from Geographic Information Systems (GIS). Any video or similar technology does not require recording, but a record shall be kept of the duration of the live video and what was covered. This is to be recorded in the audit report.

The responsibility of the effective application of remote auditing methods for any given audit lies with the CB and the lead auditor (in terms of performing audit activities).

### 3.5.1 NON-CONFORMITIES

Remote audit activities follow the same principles of the on-site audit activities and where non-conformities are identified, these are documented, graded, and addressed as defined in Part 3 of the Scheme requirements.

### 3.5.2 AUDIT REPORT

The Audit report shall indicate that the audit was conducted as a full remote audit, 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, 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 full remote audit. An overview shall be included in the executive summary of the report providing details of the serious event and the extent to which ICT was used, including different methodologies applied.

The full audit pack, including the feasibility and risk assessments, shall be uploaded to the Assurance Platform within 2 months from the last day of the full remote audit.

### 3.5.3 CERTIFICATION DECISION

a) As part of the certification decision process, the CB shall review the audit program and take into consideration the need for an on-site special audit and any changes required to the audit program based on risk and the outcome of the audit.

b) It remains the responsibility of the CB to ensure a proper and robust audit process and make an informed certification decision. Where the outcome of the remote audit is to maintain (re-) certification, the certificate shall be updated to reference that a Full Remote Audit was conducted by adding the following reference “Audit delivery: Full Remote Audit due to a serious event”. Following the next regular audit (full on-site or via the ICT Audit Approach), the certificate shall be updated, and the reference to Full Remote Audit removed.

c) In the case of a full remote audit being delivered for Category FII, under normal circumstances, a reference shall be added on the certificate as follows: "Audit delivery: Full Remote Audit". In the case of a serious event, 3.5.3 (b) above shall apply.