IFS Broker version 3.2
Audit Protocol for Remote Auditing

ENGLISH

IFS BROKER VERSION 3.2:
Audit Protocol for Remote Auditing

0   Introduction

Information and Communication Technology (ICT) has made remote auditing more feasible. Referring to the document IAF MD4 : 2023, ICT is the use of technology for gathering, storing, retrieving, processing, analysing, 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 both locally and remotely.

For the purpose of auditing, the IFS Broker version 3.2 Remote Audit means that the audit is performed entirely using remote ICT whilst being conducted in compliance with IFS Broker version 3.2 Requirements.

The use of remote ICT for auditing will only be successful if the right conditions are in place. The two fundamental requirements are that the technology is available and that both auditor(s) and auditee are competent and at ease with its operation.

1   Objective

This document was created to ensure a robust audit process for renewal audits by applying remote ICT for the evaluation of IFS Broker version 3.2 Requirements by a certification body/auditor.

The remote option is voluntary and needs to be agreed well in advance between the certification body and the company subject to IFS Broker Certification.

The requirements of IAF MD4:2023 shall be followed, as it defines the rules that certification bodies and their auditors shall follow to ensure that remote ICT is used to optimise the efficiency and effectiveness of the audit, while supporting and maintaining the integrity of the audit process.

Furthermore, 2.1.1 pre-requisites for the application of remote auditing techniques need to be fully ensured.

Note 1: The remote audit option is only applicable for the announced option. It is NOT possible to complete a remote audit as part of the unannounced audit program.

2   Framework/trail

For the certification process, the general rules of IFS Broker version 3.2 apply.

The main purpose for conducting a remote IFS Broker Audit is to obtain objective evidence of the fulfilment of IFS Broker version 3.2 Requirements by using remote ICT.

In this regard, there are some additional points to consider that are related to the use of remote ICT in the certification process, which shall be taken into account.
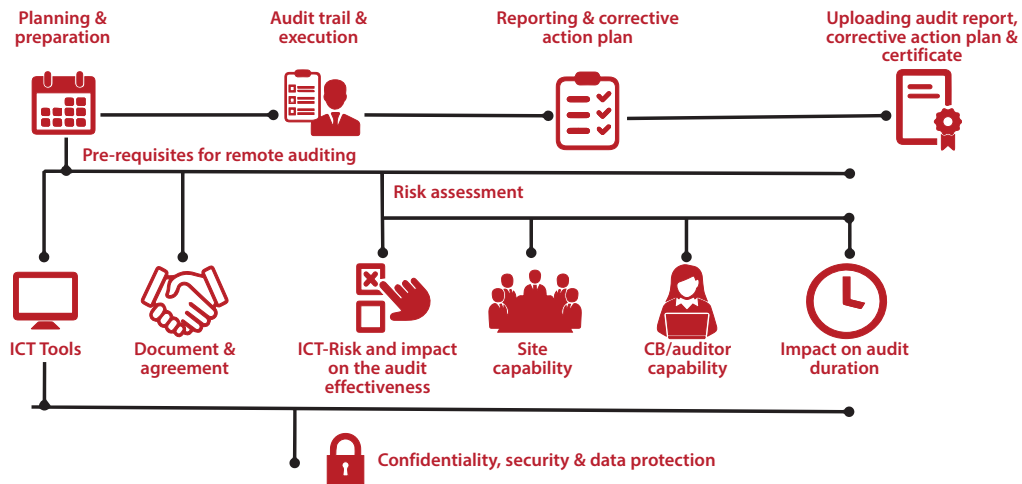
2.1   Planning and preparation

2.1.1   Pre-requisites for the application of remote auditing techniques

To be able to apply the full remote audit option, the following pre-requisites shall be fulfilled:

- The auditee is actively IFS Broker certified or subject to an initial IFS Broker Audit, an IFS Broker Follow-up Audit or Extension Audit according to IFS Broker 3.1, 3.2, 3.3, 3.4, Part 1.

- The certification body, auditor and auditee have the appropriate information technology (IT) infrastructure and environment (e.g. internet access) in place.

- The auditee has all relevant documents and records available online, or has a document scanner or similar, to enable the digitalisation of further documents or records, if necessary.

- The certification body and the auditee have signed an agreement on the use of ICT, which includes details on data security and confidentiality.

    Note1: When determining and verifying the appropriate technology/media platform (e.g. Go-To-Meeting, adobe connect, WebEx, zoom, Microsoft Teams, etc.) for hosting the audit, it shall be considered whether the platform is able to ensure data protection and the type of platform shall be agreed upon between the certification body and the auditee.

    Note 2: The certification body is obligated to sign an agreement between auditor and auditee about local and applicable data security requirement issues.

    Note 3: This agreement shall be available at the certification body on request. Evidence of agreements related to data security can be in the form of records, agreed procedures, or emails.

- The certification body shall develop a procedure covering the requirements of IAF MD4:2023 and the requirements described in this document. All activities using ICT during the certification process shall meet the mentioned requirements.

2.1.1.1 Performance of the risk assessment

Prior to audit preparation and as a pre-requisite, the certification body shall conduct a risk assessment to determine whether it is feasible to apply the remote audit option.

The risk assessment shall include, but is not limited to:

- The capability of the certification body/auditor to conduct a remote audit using remote ICT.

  Note: In case of any doubt regarding the auditor's capability, the certification body shall allocate an alternative auditor to the audit.

- A remote ICT and IT system, that the certification body and the auditee have mutually agreed on and both have access to, and the capability of the auditee to conduct a remote audit using remote ICT.

  The following factors shall be considered, but are not limited to:

  - adequate cooperation from the auditee (e.g. access to an IT system, availability and capability of the auditee to use technology such as remote ICT),

  - resources including access to sufficient, adequate and appropriate information and communication technology, including IT support for the ICT platform, if necessary

  - the limitation of the site's willingness to share the information remotely.

- Risks and impacts of the use of remote ICT in regard to confidentiality, security and data protection, including identification and documentation of risks and opportunities that may impact the audit effectiveness for each selected remote ICT, including the selection of the appropriate technologies, and how they are managed.

Note 1: The certification body shall take the local data protection and privacy laws into consideration. Since ICT such as video is used, the relevant consent between the individuals involved shall be addressed to ensure compliance with local privacy regulations, in reference to IAF MD4:2023, clauses 4.1.3 and 4.1.4.

Note 2: In the case of non-agreement regarding information security and data protection measures, the certification body shall not apply the remote audit option for the audit/company.

- Risk and impact of the effectiveness of remote ITC on the audit, including possible risk of IT failure (e.g. loss of internet connection).

- Impact on audit duration and audit planning e.g. when more time might be required due to the use of remote ICT.

- Continuity of the auditee being certified with the same certification body.

- Number of employees at the company (on-site and/or mobile/home office), and participants necessary for conducting the audit.

- Results and nature of raised deviations and/or non-conformities from last audit, including certification status.

- Number of recalls/withdrawals/other incidents (e.g. food fraud) initiated by the auditee during the ongoing/last certification cycle.

This risk assessment shall be conducted and documented in advance for each audit. It is expected that all identified risks are addressed and mitigation measures are defined, as necessary. As per IAF MD4:2023, clause 4.2.1, where the application of remote technologies and methodologies are not a feasible possibility, the alternative of an on-site audit shall be proposed to the auditee.

If the risk assessment results in a positive outcome, the risk assessment findings shall be addressed in the audit preparation.

2.1.2 Audit preparation

The general rules of IFS Broker version 3.2 apply.

In addition to the regular audit preparation, as laid down in the standard, and provided that the risk assessment has had a positive outcome, the following requirements apply:

The certification body is obliged to communicate and arrange the following with the auditee:

- Allocation of resources necessary to perform the audit remotely, both for the certification body/auditor and the auditee.
- Allocation of a contact person at the certified site who will facilitate, manage and coordinate the arrangements of the audit together with the certification body on behalf of the company subject to the IFS Broker Audit.
- Availability of applicable files, procedure(s), documents and records for the broker services/ process(es) being assessed. Some further information, such as information on products, risk management system, etc., may need to be sent to the auditor for review prior to the remote audit.
- Time zone acknowledgement and management, to be able to coordinate reasonable and mutually agreeable meeting hours, preferably during the working hours of the broker subject to certification.
- A trial meeting, using the same technology/media platforms agreed upon, should be conducted to ensure the scheduled audit can be performed as planned and without interruptions.
- Set up/technical check of devices/tools, set up recording devices, internet connection (to preview a test on the use of ICT before the audit) to confirm that there is a stable connection and that the individuals involved can confidently use the technology.

Note: The remote audit plan shall identify how remote ICT will be utilised and the extent to which ICT will be used for audit purposes, to optimize audit effectiveness and efficiency while maintaining the integrity of the audit process.

2.1.3 Audit duration

The general rules of IFS Broker version 3.2 apply.

The certification body needs to consider that in certain cases more time is needed to conduct the audit remotely. Possible factors could be, but are not limited to:

- Determination of the different remote ICT to be used and how it will be used.
- Presentation of documents using remote ICT (e.g. switching of pages, returning to previous documents for cross checks, executing the traceability test while auditing other requirements, internet connection).

Note 1: For example, an audit duration of eight (8) hours can be split into a maximum of two (2) consecutive working days.

Note 2: The time needed for audit preparation including performing a risk assessment in regards to ICT, cannot be counted towards the audit duration.

2.1.4 Auditor Competency

The general rules of IFS Broker version 3.2 apply.

Auditors are required to pass the "IFS Broker Remote Audit e-learning" e-learning prior to conducting his/her first IFS Broker Remote Audit.

Moreover, auditors need to have sufficient knowledge and understanding on the application of the remote technology and platform used.

The auditor shall also be aware of the risks, their mitigation measures and necessary corrective actions, of possible malfunctions of the information and communication technologies used and the impact that they may have on the validity and objectivity of the information gathered.

Furthermore, with regard to the above, an auditor shall review the determined risk in light of a remote audit and its objectives and may propose changes to the determined ICT technology used, if necessary.

Note: Certification bodies shall also train and monitor IFS Auditors on the performance of the remote Broker audit in line with IFS principles and IAF MD4 : 2023 requirements. Documentation of both shall be available on request.

3 Audit trail and execution

The general rules of IFS Broker version 3.2 apply.

Before starting the audit (i.e. opening meeting), it needs to be ensured that the ICT platform and necessary features function properly and that all relevant audit participants have accessed the platform successfully.

In addition to the general rules, the auditor is obliged to explain the remote audit process during the opening meeting (including the traceability test, if the audit is conducted over consecutive days) and to explain how ICT is applied for the purpose of collecting objective evidence.

Measures to ensure confidentiality and security shall be confirmed by the auditor during the opening meeting.

The remote audit will be conducted using a combination of features such as documentation and record review via screen-sharing, taking screenshots or sending of documents including remote interviews. Interviews include, as usual, appropriately sampled representatives of management and operational personnel involved in the process.

Note: Interviews with staff are carried out in the same way as during an on-site audit at the physical Broker office.

Only records and documents presented to the auditor during the ongoing remote audit, or documents (e.g. procedures, organisation chart, risk assessment documentation) submitted prior to the remote audit and verified during the ongoing remote audit can be considered as audit evidence.

In case the audit is split over different days, the actual sampled product(s) for the traceability test need to be announced and comprehensively exercised within one (1) day.

Example: total audit duration of eight (8) hours, split over two (2) days of four (4) hours:

1. Day: auditing of general requirements.

2. Day: announcement of sample(s) and execution of the traceability exercise.

The closing meeting has to be followed as in the on-site audit process.

Note: The auditor shall delete and remove access to any documented information and records not required as objective evidence from its system after completing the audit.

4 Reporting and corrective action plan

The general rules of IFS Broker version 3.2 apply.

The cover page of the audit report shall clearly state that the audit was conducted remotely. Furthermore, it should be indicated under "audit details" what kind of remote ICT has been used.

Note: The audit plan and certificate shall indicate that the audit was carried out fully remotely.

5 Uploading audit report, corrective action plan and certificate

The general rules of IFS Broker version 3.2 apply.

Furthermore, by uploading the relevant documents, the certification body is required to mark the tick-box "remote audit".

6 Technical guidance

The certification body/auditor conducting the audit shall ensure compliance with the essential requirements below:

- No unauthorised voice or video recording is allowed.

- No unauthorised screenshots from documents as audit evidence are allowed. Any screenshots of documents or records or other kind of evidence shall be previously authorised by the audited organization.

- All reviewed information (voice and/or video) will only be used as evidence to support audit findings and conclusions.

- The certification body shall ensure that the ICT used allows the recording of the session as objective evidence. The identification of participants by name needs to be clearly stated/ understood and recorded as part of the session.

- In cases where the auditor identifies during the remote audit that the audit cannot be finalised using ICT, the auditor has to make contact with the site again remotely within the 14 day timeframe to finalise the audit. Otherwise the audit will be deemed as failed and a certificate cannot be granted.

- The certification body is obliged to record these sessions and store the data according to the IFS Standard Rules.

Note: Clarifications regarding "recording": IFS considers recording a screenshot at the start/ end of a session, where the participants and the duration of the session can be identified as sufficient. Furthermore, the log-file of the ICT used shall be stored and available on request.

7 Other applicable documents

- IFS Broker version 3.2, February 2024

- IFS Broker Doctrine

- IAF MD 4:2023 for the use of information and communication technology (ICT for auditing/ assessment purpose

IFS publishes information, opinions and bulletins to its best knowledge, but cannot take any responsibility for any mistakes, omissions or possibly misleading information in its publications, especially in this document.