Remote Audits

1. Aim and Purpose

This instruction contains regulations on the use of information and communication technology (ICT) in the context of audits, particularly for remote audits. The aim is to ensure that the results of remote audits are comparable to those of on-site audits.

The version takes into account the requirements of IAF MD 4:2022.

2. Scope

Unless certain services are explicitly excluded in point 8, this instruction applies to all audits within the scope of ISO/IEC 17021, ISO/IEC 17065, ISO 14065 as well as to audits according to EfbV, provided that the use of remote audit techniques is provided for in these audits.

3. Responsibilities

The responsibility for defining general regulations on the use of ICT lies with the management of the certification body.

The respective project manager is responsible for the correct consideration of possible remote audits as part of the preparation of the offer and initial audit programme.

The respective lead auditor is responsible for the effective implementation of the regulations described here in the audit as well as the documentation of the audit process and results in accordance with requirements.

4. Description

Remote audits are intended to replace on-site audits, using technical tools to gather information, interview an audited organisation, etc., when face-to-face methods are not possible or not desired. The audit time of remote audits always counts as on-site time.

Remote audits can be conducted from the auditor's office (or another suitable location) or from a location of the audited organisation.

In principle, this regulation also includes the use of ICT in cases where this is operated by the customer and made available for assessment purposes (e.g. existing video surveillance in warehouses). In these cases, the lead auditor is responsible for the specific implementation in the audit. If doubts arise regarding the effectiveness for audit purposes, the management of the certification body must be informed, who will then decide on the further procedure.

4.1. Risk assessment

A general risk assessment for the use of remote audit techniques is prepared for each management system by the head of department. As a result, it is determined to what extent remote audit techniques are permitted for auditing each location without a separate individual risk assessment.

If the lead auditor wishes to utilise a higher proportion of remote audit time, an individual risk assessment with FL162EN is required. The topics and aspects listed in the general risk assessment with an increased risk potential are assessed in particular.

For this purpose, the lead auditor fills out the FL162EN, and the assessment is then carried out by the respective head of department.

4.1. Offer preparation

As part of the preparation of the offer, the possibility of remote audits by the certification body is discussed in principle with the applicant. If the applicant is interested in using remote audit techniques and there are no major obstacles (e.g. confidentiality requirements, lack of technical requirements), the possibility of remote audits is mentioned in the offer and taken into account in the further procedure.

4.2. Application review

With application FL052, the customer indicates whether they agree to the use of remote audit technologies. To this end, he must state whether the prerequisites for their use are met:

- o Sufficient Internet connection at the respective locations/facilities
- o Availability of the necessary hardware (video conferencing system)
- o Availability of the necessary software and its acceptance with regard to confidentiality requirements

If the client proposes video conferencing systems or other technology that is not available as standard at GUTcert, a statement from internal IT must be obtained when the application is reviewed.

The result of the application review regarding the use of remote audit techniques is documented, communicated to the client and taken into account in the planning of the audit programme.

4.3. Audit planning and implementation

After the application has been reviewed, the certification body appoints an appropriately qualified audit team. The auditors/assessors and other persons involved (e.g. drone pilots, technical experts) must have the competence and ability to understand and utilise the information and communication technologies used in order to achieve the desired results of the audit(s)/assessment(s).

The responsible lead auditor then plans the further audit activities on the basis of the audit programme. By collecting further detailed information about the customer, it may be necessary to reassess the risks and opportunities of the planned use of remote audit techniques in the audit. It may also be necessary to adjust the planned audit programme; this is done in close consultation with the certification body and the customer and must be documented appropriately. The risks associated with the transfer of any sensitive data in individual agenda items during remote audits must also be taken into account.

As part of the concrete planning of the audit by the lead auditor and customer, it must be ensured that the existing technology is compatible on both sides and enables remote audits to be carried out without disruption. If necessary, this must be tested before the audit in order to recognise and rectify technical problems.

The planned use of ICT must be documented in the audit plan for each agenda item with details of the respective technology.

The audit results must be documented in the usual way. The lead auditor must refer to the use of ICT in the audit report and make a statement on the effectiveness of its use.

5. General information for remote audits

5.1. Risk assessment for the use of ICT, especially for remote audits

The following are possible applications for the use of ICT in the context of remote audits and their general risk level:

a) Very good applicability, low risk:
Interviews or meetings that usually take place in a meeting room and in which presentations are presented and documents are reviewed.

b) Very good applicability, low risk:
Inspection of data from databases or similar, also with selection and review of random samples within the IT tools.

c) Moderate applicability, low risk:
Inspection of existing paper documents using a camera or scanner (with subsequent transmission).

d) Moderate to poor applicability, medium risk:
Tours with video transmission, inspection of the layout of systems/parts and other facilities.

- e) Poor applicability, medium to high risk:
Inspection of products in production with random sampling.

f) Poor applicability, high risk:
Interviews with production workers (who are not used to using video conferencing).

5.2. For which audit parts are remote audits generally not suitable?

a) Interviews with employees where the observation of non-verbal signals is important.

b) Audits in which other senses besides sight and hearing are addressed (e.g. sense of temperature, draught, sense of touch for roughness) or in which distortions can easily occur due to the transmission (assessment of lighting, colours, etc.).

c) If confidentiality requirements cannot be met by remote techniques.

5.3. To what extent can remote techniques be used in audits?

a) The possible remote share that can be planned without an individual risk assessment is specified in the annex by the respective head of department.

b) If this is to be exceeded in individual cases, an individual risk assessment is required in accordance with 4.1.

c) Cases are conceivable in which up to 100% of the audit time is carried out remotely, e.g. for organisations without physical locations (i.e. only virtual according to IAF MD 1). However, these would be absolute exceptions.

d) Remote audits are a good means of reducing travelling expenses and thus also reducing the environmental impact of the audit.

e) They are also suitable for gaining audiovisual access to very remote or dangerous locations.

5.4. In which procedures are there restrictions or special regulations for remote audits?

a) All procedures for which official requirements have other specifications.

b) In the context of ISO 50001 certifications, only locations with low energy relevance (e.g. small office locations, sales offices) are generally considered for a remote audit. In addition, no effective personnel should be permanently employed at these locations with regard to the management system.

c) For audits in accordance with ISO 45001, the use of ICT is generally not suitable for auditing process and risk control. (This includes, among other things, the observation and control of compliance with regulations, procedures, rules and operating instructions that ensure operational safety. As well as the identification, assessment and mitigation of specific hazards to reduce the risk of accidents). Conversations with ordinary workers or other 'non-functional staff' in particular often provide different results via ICT than 'at the machine' and only allow limited conclusions to be drawn from body language. Remote audits can therefore generally not replace on-site inspections and, in some cases, on-site interviews only to a limited extent. Especially for initial certifications and when sites are audited for the first time, it can be assumed that an on-site visit is necessary to obtain the required information. If the company doctor can only be interviewed remotely, the reasons must be documented. Remote audits in accordance with ISO 14001 are only permitted for sites with low or limited risk classes.

d) Remote audits are excluded for audits in accordance with EfbV as soon as there is an on-site facility requiring authorisation or waste management activities are carried out. Remote audits are only permitted under certain conditions, e.g. offices with scheduling activities.

e) As part of an RSPO audit, remote audits should only be carried out after consultation with the RSPO, as these are not explicitly provided for by the standard.

f) For audits in the context of emissions trading, the provisions of Art. 31 of the Accreditation and Verification Ordinance and EU Guideline Chapter 3 apply.

g) AZAV: The question of whether remote audits can replace an on-site audit is always a case-by-case decision. In addition to the criteria listed in this overview, the following aspects are included in the assessment:

o Has another body (e.g. state authorities in the context of school accreditation, other TCS, etc.) already inspected the premises?

o Have the premises already been inspected by GUTcert on site in previous audits?

o Has the provider of training centres (e.g. meeting rooms in hotels) already documented o Does the provider of training facilities (e.g. conference rooms in hotels) have documented minimum standards for seminar rooms and can it therefore be assumed that the premises are standardised at different locations?

o Can the documentation of the measures carried out on site be viewed using remote techniques?

6. Necessary competences for auditors

If ICT is to be used in audits, the designated auditors must have the necessary competence to

a) plan the use of ICT in the audit, taking existing risks into account,

b) develop audit findings with the help of ICT and

c) fulfil the general requirements of the audit (especially with regard to confidentiality), even when using ICT.

Auditors who have an appointment for ISO 9001 EAC 31/2 or 33 or ISO 20000-1 or ISO/IEC 27001 do not require separate proof of their competence.

For the use of ICT provided by the customer, the appointment as an auditor is sufficient as proof of competence for a) and b).

Completion of the corresponding e-learning course serves as proof of competence for c)

General risk assessment regarding remote audits

This overview provides a general assessment of the risks that can arise when using remote audit techniques to audit management systems. This is based on the use of video conferencing technology (e.g. Teams or Zoom) in remote audits.

In this list, the audit methods usually used are recorded for each individual standard element

- o records the audit methods normally used,
- o assesses the risk associated with the audit methods when using remote audit techniques,
- o documents aspects and topics where there is an increased risk to the effectiveness of the audit when using remote audit techniques.
- o An overall assessment is then made of the extent to which remote audit techniques can be included in the audit for each location without the need for a separate individual risk assessment.

Audit methods:

1. review of documents
2. interview/interrogation of persons
3. observation of activities
4. visual inspection of operating facilities
5. random sampling
6. technical inspections

Risk assessment:

low: The efficiency and effectiveness of the audit is very little influenced by the use of remote audit techniques;
it is not to be expected that the audit result will be influenced by the use of remote audit techniques.

medium: The efficiency and effectiveness of the audit can be influenced to a manageable extent by the use of remote audit techniques;
the achievement of the audit objective can be influenced to a manageable extent by the use of remote audit techniques.

high: The efficiency and effectiveness of the audit can be significantly influenced by the use of remote audit techniques;
the achievement of the audit objective can be strongly influenced by the use of remote audit techniques.

Management systems according to DIN EN ISO 9001

Standard element	Audit methods	Risk assessment with regard to remote audits	Aspects/topics with increased risk potential with regard to remote audits
Context and MS	1, 2	low	
Top management, policy	1, 2	low	
Responsibilities and authorities	1, 2	low	
Risks and opportunities	1, 2	low	
Quality objectives	1, 2	low	
Changes	1, 2	low	
Resources, infrastructure	1, 2, 4	medium	- Infrastructure, facilities
Monitoring and measuring resources	1, 2, 3, 4, 5	High	- Resources for measurements and tests - Status of test and operating equipment
Personnel, Organizational knowledge	1, 2, 3, 5	medium	- Knowledge of the management system by employees and, if applicable, external parties
Communication	1, 2	low	
Documented information	1, 2, 4	medium	- Availability of documented information at the workplace
Planning	1, 2	low	
Product requirements	1, 2, 5	low	
Development	1, 2, 5	low	
Procurement	1, 2, 3, 4, 5	high	- Incoming goods inspection for external deliveries - Control of outsourced services
Production	1, 2, 3, 4, 5, 6	high	- Process control - Labelling the status of products including traceability - Handling of customer property - Handling of (intermediate) products (handling, storage, transport)
Release, Control of nonconforming outputs	1, 2, 3, 4, 5, 6	high	- Dealing with non-compliant products
Data analysis and evaluation	1, 2	low	
Internal audit	1, 2	low	
Management review	1, 2	low	
Improvement	1, 2	low	

Overall assessment:

The inclusion of remote audit techniques in the auditing of sites in accordance with DIN EN ISO 9001 is possible up to a share of 50% of the respective audit time without a separate individual risk assessment.

Management systems according to DIN EN ISO 27001

Standard element	Audit methods	Risk assessment with regard to remote audits	Aspects/topics with increased risk potential with regard to remote audits
Context and MS	1, 2	low	
Top management, policy	1, 2	low	
Responsibilities and authorities	1, 2	low	
A.I organization			
Risks and opportunities	1, 2	low	
Information security Risk assessment	1, 2, 4, 5	High	- Assessment of existing risks
Information security risk treatment	1, 2, 4, 5	medium	- Evaluation of the effectiveness of implemented measures
Network structure plan	1, 2	low	
ISMS goals	1, 2	low	
MS changes	1, 2	low	
Resources	1, 2, 4, 5	Medium	- Infrastructure, facilities
A.II Management of values	1, 2, 4, 5	High *)	- Completeness of value inventory
personnel	1, 2, 4, 5	Medium	- Knowledge of the management system by employees and, if applicable, external parties
A.III Personnel security	1, 2, 3, 5	Medium	- Compliance with specified regulations
Communication	1, 2	Low	
Documented information	1, 2, 4	Medium	- Availability of documented information at the workplace
A.IV physical security	1, 2, 3, 4, 5, 6	high	- Implementation of technical requirements (access, monitoring, protection against phys. threats, protection of transmission paths)

Standard element	Audit methods	Risk assessment with regard to remote audits	Aspects/topics with increased risk potential with regard to remote audits
Operational planning and control	1, 2	low	
A.V access control	1, 2, 3, 4, 5, 6	High *)	- Implementation of technical requirements (access, authentication)
A.VI Operational security	1, 2, 3, 4, 5, 6	High *)	- Implementation of technical requirements (protection against malware, handling storage media, backup)
A.VII network security	1, 2, 3, 4, 5, 6	High *)	- Implementation of technical requirements (network devices, network infrastructure)
A.VIII development of systems	1, 2, 3, 5	low	
A.IX Supplier relationships	1, 2, 3, 4, 5, 6	medium	- Implementation of technical requirements (external access for service providers) - Incoming goods inspection for external hardware deliveries
A.X Business Continuity Management	1, 2	low	
Data analysis and evaluation	1, 2	low	
Internal audit	1, 2	low	
Management review	1, 2	low	
A.XI Compliance	1, 2	low	
Improvement	1, 2	low	
A.XII Information security incidents	1, 2	low	

*) for systems of a non-physical nature (e.g. software, cloud) for which remote access to these systems is possible, the risk is reduced to low

Overall assessment:

The inclusion of remote audit techniques in the auditing of sites in accordance with DIN EN ISO/IEC 27001 is possible up to a scope of 50% of the respective audit time without a separate individual risk assessment.
For locations where physical assets only play a minor role, it is possible to increase the remote share to 70%.
(At present, GUTcert is still accredited in accordance with DIN EN ISO/IEC 27006:2021, after which the remote share of 30% can only be exceeded with the approval of DAkkS).

Date: 15.01.2025 signed. Head of QM: Andreas Lemke

Management systems according to DIN EN ISO 45001

Standard element	Audit methods	Risk assessment with regard to remote audits	Aspects/topics with increased risk potential with regard to remote audits
Context and MS	1, 2	low	
Top management, policy, worker participation	1, 2	low	
Responsibilities and authorities and worker consultation	1, 2	high	- Consultation of workers (also at lower hierarchical levels)
Risks and opportunities, hazard identification	1, 2, 3, 4, 5	high	- Identification of workplace hazards and assessment of their severity and probability.
OHS goals	1, 2	low	
MS changes	1, 2	low	
Resources, Infrastructure	1, 2, 4	high	- Infrastructure, facilities - Safety and emergency equipment can only be correctly reviewed on site
Personnel	1, 2, 3, 5	high	- Workers at lower hierarchical levels - Knowledge of the management system by workers and, if applicable, external parties
Communication	1, 2, 3, 5	medium	
Documented Information	1, 2	low	
Operational control and planning	1, 2, 3, 4, 5	high	- Availability of documented information at the workplace - Checking compliance with safety guidelines/operating instructions - Permits to work - Maintenance records - Observation of work practices - Monitoring of safety documentation - Use of PPE - Inspection of physical security measures
Procurement	1, 2, 3	medium	- Incoming goods inspection for external deliveries - Control of outsourced services - Observation of external personnel
Emergency preparedness, hazard prevention	1, 2, 4, 5	high	- Inspection of monitoring and alarm systems, escape routes - Security and emergency equipment can only be correctly reviewed on site
Data analysis, evaluation; compliance	1, 2, 5	high	- „practiced“ Compliance
internal Audit	1, 2	low	
Management review	1, 2	low	
Improvement	1, 2, 4	medium	- Effectiveness test also of (near) accidents with involvement of workers, transfer to similar workplaces if necessary

Overall assessment:
The inclusion of remote audit techniques in the auditing of sites in accordance with DIN EN ISO 45001 is possible up to a share of 35% of the respective audit time without a separate individual risk assessment.

Date: 04.04.2025 signed. Head of OHS: Seán Oppermann

-