Remote-Audits

GUT Certifizierungsgesellschaft
für Managementsysteme mbH
Umweltgutachter
Chief Executive Officer:
Prof. Dr.-Ing. Jan Uwe Lieback
AFNOR Group

Eichenstraße 3b
12435 Berlin
Tel.: +49 30 2332021 - 0
Fax: +49 30 2332021 - 39
info@gut-cert.de
www.gut-cert.de

Limited liability company, registered
office in Berlin
Commercial Register:
Amtsgericht Charlottenburg
HRB 64544
VAT ID no. DE 190888348

GLS BANK:
IBAN DE04 4306 0967 1316 1823 00
BIC GENODEM1GLS
Postbank Berlin:
IBAN DE62 1001 0010 0496 3301 03
BIC PBNKDEFF

Content

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 remote audits yield results comparable to those of on-site audits.

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

2 Scope

Unless specific services are explicitly excluded within this document, this instruction applies to all audits conducted within the scope ISO/IEC 17021, ISO/IEC 17065 and ISO 14065, as well as to audits under the EfbV, provided that the use of remote audit techniques is envisaged in these audits.

3 Responsibilities

Responsibility for establishing general regulations on the use of ICT lies with the management of the certification body.

The respective project manager is responsible for ensuring that potential remote audits are properly considered during the preparation of offers and the initial audit programme.

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

4 Description

Remote audits are intended to replace on-site audits, using technical aids to gather information, conduct interviews with the audited organisation etc., where face-to-face methods are not possible or not desired. The audit time for remote audits always counts as on-site time.

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

In principle, this regulation also covers the use of ICT in cases where this is operated by the client themselves and made available for assessment purposes (e.g. existing video surveillance in warehouses). In such cases, the lead auditor is responsible for the practical implementation during the audit. Should any doubts arise regarding the effectiveness for audit purposes, the management of the certification body must be informed, which will then decide on the further course of action.

4.1 Risk assessment

For each management system, the department head carries out a general risk assessment regarding the use of remote audit techniques. The outcome determines the extent to which remote audit

techniques are permissible during the audit at each site without the need for a separate individual risk assessment.

If the audit leader wishes to utilise a higher proportion of remote audit time, an individual risk assessment using the FL162 form is required. In particular, the topics and aspects listed in the general risk assessment as having an increased risk potential are evaluated. Once the lead audit has completed the FL162 form, the assessment is carried out by the respective department head.

4.2 Offer preparation

As part of the preparation of the offer, the certification body discusses the general feasibility of remote audits with the client. If the client is interested in using remote audit techniques and there are no significant obstacles (e.g. confidentiality requirements, lack of technical prerequisites), the possibility of remote audits is mentioned in the offer and considered in the subsequent process.

4.3 Application review

In the FL052 application, the client indicates whether they agree to the use of remote audit techniques. To this end, they must state whether the prerequisites for their use are in place:

- Adequate internet connection at the respective sites/facilities
- Availability of the necessary hardware (video conferencing system)
- Availability of the necessary software and its compliance with confidentiality requirements

If the client proposes video conferencing systems or other technologies not standardly available at GUTcert, a statement from internal IT must be obtained during the application review.

The outcome of the application review regarding the use of remote audit techniques is documented, communicated to the client and considered in the planning of the audit programme.

4.4 Audit planning and conduct

Following the application review, the certification body appoints a suitably qualified audit team. The auditors/verifiers and other persons involved (e.g. drone pilots, technical experts) must possess the competence and ability to understand and use the information and communication technologies employed to achieve the desired results of the audit(s)/assessment(s).

The responsible lead auditor then plans the further audit activities based on the audit programme. The collection of further detailed information about the client may make it necessary to reassess the risks and opportunities associated with the planned use of remote audit techniques during the audit. If necessary, the planned audit programme must then also be adapted. This is done in close consultation with the certification body and the client and must be appropriately documented. The risks associated with the transmission of potentially sensitive data during individual audit items as part of remote audits must also be taken into account.

When the lead auditor and the client are planning the audit in detail, they must ensure that the existing technology is compatible on both sides and that remote audits can be carried out without

disruption. If necessary, the technology must be tested prior to the audit in order to identify and resolve any technical issues.

The planned use of ICT must be documented in the audit plan for each agenda item, specifying the relevant technology.

The audit results are documented in the usual manner. The lead auditor must refer to the use of ICT in the audit report and provide a statement on the effectiveness of its use.

5 General information for remote audits

5.1 Risk assessment regarding the use of ICT, specifically for remote audits

The following lists 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 during which presentations are given and documents are reviewed

b) **Very good applicability, low risk:**

Inspection of data from databases or similar, including thr selection and review of samples within 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**:

Site inspections with video transmission, inspection of the layout of plants/ plant parts and other facilities

e) **Poor applicability, medium to high risk:**

Inspection of products in production with sampling

f) **Poor applicability, high risk:**

Interviews with production workers (who are not accustomed to video conferencing)

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

a) Interviews with employees where the observation of non-verbal cues is important
b) Audits in which senses other than sight and hearing are engaged (e.g. temperature perception, draughts, sense of touch for roughness) or in which distortions may easily occur due to the transmission (assessment of lighting, colours, etc.)
c) Where confidentiality requirements cannot be met by remote techniques

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

a) The proportion of the audit that can be conducted remotely without an individual risk assessment is specified in the annex by the relevant department head.
b) Should this proportion be exceeded in individual cases, an individual risk assessment is required in accordance with 4.1.
c) There may be cases where up to 100 % of the audit time is carried out remotely, e.g. for organisations without physical sites (i.e. exclusively virtual sites according to IAF MD 1). However, these are absolute exceptions.
d) Remote audits are a good means of reducing travel expenses and thus also minimising 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 do restrictions or special rules apply?

a) All procedures for which official requirements have other specifications
b) In the context of ISO 50001 certifications, generally only sites with low energy relevance (e.g. small office locations, sales offices) are eligible for a remote audit. In addition, no effective personnel involved in the management system should be permanently stationed at these sites
c) For audits in accordance with ISO 45001, the use of ICT is generally not suitable for auditing process and risk control. Process and risk management includes, among other things, monitoring and ensuring compliance with regulations, procedures, rules and operating instructions, which ensure operational safety, and the identification, assessment and mitigation of specific hazards to reduce the risk of accidents. In particular, discussions with production staff or other employees without managerial roles often yield different results via ICT than those conducted 'at the machine' and allow only limited conclusions to be drawn regarding body language. Remote audits can therefore generally not replace an on-site audit and, in some cases, can only partially replace on-site interviews. Particularly in the case of initial certifications or when sites are being audited for the first time, it must be assumed that an on-site audit is necessary to obtain the required information. If the company doctor can only be interviewed remotely, the justification must be documented
d) For audits under the EfbV, remote audits are excluded as soon as there is a facility on site requiring a permit or waste management activities are carried out. Remote audits are only permitted under certain conditions, e.g. for offices carrying out planning activities
e) In the context 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 within the framework of emissions trading, the provisions of Article 31 of the Accreditation and Verification Ordinance and Chapter 3 of the EU Guideline apply

g) In the case of AZAV, the question of whether remote audits can replace an on-site audit is always decided on a case-by-case basis. In addition to the criteria listed in this overview, the following aspects are taken into account in the assessment:
   - Has another body (e.g. state authorities in the context of school accreditation, other TCS etc.) already inspected the premises?
   - Have the premises already been inspected by GUTcert on-site in previous audits?
   - Does the provider of training venues (e.g. conference rooms in hotels) have documented minimum standards for seminar rooms, and can it therefore be assumed that the premises are consistent across different locations?
   - Is the documentation of the measures carried out on-site available for viewing via remote technology?
   - Locations where no group activities are carried out (e.g. administrative sites), or premises for individual activities or job placement services, are suitable for remote audits regardless of the criteria mentioned above

6 Required competences for auditors

If ICT is to be used during 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) draw up audit findings with the help of ICT, and
c) meet the general requirements for the audit (particularly confidentiality) even when using ICT.

Auditors who hold 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 client, the auditor's appointment is sufficient proof of competence for a) and b). Completion of the relevant GUTcert e-learning course serves as proof of competence for c).

7 General risk assessment regarding remote audits

The following overviews provide a general assessment of the risks that may arise when applying remote audit techniques during the auditing of management systems. This assumes the use of video conferencing technology (e.g. Teams or Zoom) in remote audits.

In each list, for every individual standard element

- the audit methods typically used are recorded,
- the risk associated with these audit methods when using remote audit techniques is assessed, and
- aspects and topics are documented where there is an increased risk to the effectiveness of the audit when using remote audit techniques.

An overall assessment is then made of the extent to which remote audit techniques can be included in the audit for each site without the need for a separate individual risk assessment.

Audit methods

1. Document review
2. Interviews/questionnaires with individuals
3. Observation of activities
4. Inspection of operational facilities
5. Sampling
6. Technical inspections

Risk assessment of the use of remote audit techniques

low	• The efficiency and effectiveness of the audit are only very slightly affected • The audit result is not expected to be influenced
medium	• The efficiency and effectiveness of the audit may be influenced to a manageable extent • The achievement of the audit objective may be influenced to a manageable extent
high	• The efficiency and effectiveness of the audit may be significantly influenced • The achievement of the audit objective may be strongly influenced

7.1 Management systems in accordance with DIN EN ISO 9001

Standard element	Audit methods	Risk assessment	Increased risk potential
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, organisational knowledge	1, 2, 3, 5	medium	• Knowledge of the management system among staff and, where applicable, external parties
Communication	1, 2	low	
Documented information	1, 2, 4	medium	• Availability of documented information in 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 inspection for external supplies • Control of outsourced services
Production	1, 2, 3, 4, 5, 6	high	• Process control • Identification of product status, including traceability • Handling of costumer property • Handling of (intermediate) products (handling, storage, transport)
Release, control of nonconforming outputs	1, 2, 3, 4, 5, 6	high	• Handling of non-compliant products
Data analysis and evaluation	1, 2	low	
Internal audits	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.

Date: 15.01.2025

signed Andreas Lemke
Head of QM

7.2 Management systems in accordance with DIN EN ISO/IEC 27001

Standard element	Audit methods	Risk assessment	Increased risk potential
Context and MS	1, 2	low	
Top management, policy	1, 2	low	
Responsibilities and authorities	1, 2	low	
A.I organisation	1, 2	low	
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, hardware
A.II Management of values	1, 2, 4, 5	high*	• Completeness of value inventory
Personnel	1, 2, 3, 5	medium	• Knowledge of the management system among staff and, where 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 in the workplace
A.IV Physical security	1, 2, 3, 4, 5, 6	high	• Implementation of technical requirements (access, monitoring, protection against physical threats, protection of transmission paths)
Operational planning and control	1, 2	low	
A.V Access control	1, 2, 3, 4, 5, 6	high*	• Implementation of technical requirements (access, authentication)

Standard element	Audit methods	Risk assessment	Increased risk potential
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 supplies
A.X Business Continuity Management	1, 2	low	
Data analysis and evaluation	1, 2	low	
Internal audits	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 non-physical systems (e.g. software, cloud) to which remote access 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 share of 50 % of the respective audit time without a separate individual risk assessment.

For locations where physical assets play only a minor role, the remote component may be increased to 70 %.

GUTcert is currently accredited to DIN EN ISO/IEC 27006:2021; under this standard, exceeding the 30 % remote proportion is only possible with the consent of DAkkS.

Date: 15.01.2025

signed Andreas Lemke
Head of IT

7.3 Management systems in accordance with DIN EN ISO 45001

Standard element	Audit methods	Risk assessment	Increased risk potential
Context and MS	1, 2	low	
Top management, policy, worker participation	1, 2	low	
Responsibilities and authorities and worker consultation	1, 2	high	• Consultation with employees (also those 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 likelihood
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	• Staff at lower hierarchical level • Knowledge of the management system among staff and, where 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 in the workplace • Verification of compliance with safety guidelines/operating instructions • Work permits • Maintenance records • Observation of working practices • Monitoring of safety documentation • Use of PPE • Inspection of physical security measures
Procurement	1, 2, 3	medium	• Incoming inspection of external supplies • 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 • Safety 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	

Standard element	Audit methods	Risk assessment	Increased risk potential
Improvement	1, 2, 4	medium	• Effectiveness test including (near-) accidents with involvement of employees; 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: 04.04.2024

signed Seán Oppermann
Head of OHS

7.4 Management systems according to DIN EN ISO 50001

Standard element	Audit method	Risk assessment	Increased risk potential
Context and MS	1, 2	low	
Top management, policy. worker participation	1, 2	low	
Responsibilities and authorities and worker consultation	1, 2	low	
Risks and opportunities, hazard identification	1, 2	low	
Energy targets	1, 2	low	
Energy assessment	1, 2	low	
Energy performance indicators (EnPI)	1, 2	low	
Energy baseline	1, 2	low	
Energy data collection	1, 2, 3, 4, 5	medium	
MS changes	1, 2	low	
Competence and resources	1, 2, 3, 5	medium	
Awareness	1, 2, 3, 5	medium	• Knowledge of SEU through effective personnel
Communication	1, 2	low	
Documented information	1, 2, 4, 5	low	• Control documents, EnPI tracking, action tracking
Operational control and planning	1, 2, 3, 4, 5	medium	• Identification of SEU, energy assessment, EnPI, influencing factors, plausibility check of results

Standard element	Audit method	Risk assessment	Increased risk potential
Procurement	1, 2, 5	low	
Monitoring, measurement, analysis and evaluation of energy performance and the EnMS	2, 3, 4, 5	high	• Including inspection of technical systems and facilities, functionality/accuracy of measurement technology
Internal audit	1, 2	low	
Management review	1, 2	low	
Improvement	1, 2	low	
Compliance	1, 2, 4, 5	high	• Permitting planning/requirements, contracts, management of recurring audit obligations
Design	1, 2, 4, 5	medium	• Requirements/contracts, energy efficiency

Overall assessment
The incorporation of remote audit techniques in the auditing of sites in accordance with DIN EN ISO 50001 is possible for up to 50 % of the respective audit time without a separate individual risk assessment.

In cases involving complex measurement technology, SEUs with high consumption or operating sites with low digital visibility, an individual assessment is required.

Sales offices can be audited 100 % remotely if there are no energy-effective personnel on site and energy consumption is well below 5 % of total energy consumption (according to DIN EN ISO 50001). Consumption/collection points (= energy consumption points outside sites with their own meters but without permanent staff) must be included in the audit documentation.

Date: 18.09.2025

signed Jochen Buser
Head of EnMS

7.5 Management systems in accordance with DIN EN ISO 14001

Standard element	Audit methods	Risk assessment	Increased risk potential
Context and MS	1, 2	low	
Top management, policy	1, 2	low	
Responsibilities and authorities and worker consultation	1, 2	low	
Risks and opportunities, hazard identification	1, 2	low	
Environmental aspects	1, 2, 3, 4	medium	

Standard element	Audit methods	Risk assessment	Increased risk potential
Compliance	1, 2, 4, 5	high	• Planning of permits/requirements, contracts, controlling of recurring obligations
Environmental objectives and measures, indicators, environmental performance evaluation	1, 2, 3, 4, 5	medium	• Including inspection of technical facilities
Environmental data collection	1, 2, 3, 4, 5	medium	
MS changes	1, 2	low	
Competence and resources	1, 2, 3, 5	medium	
Awareness, employee participation	1, 2, 3, 5	medium	• Including on-site interviews
Communication	1, 2	low	
Documented information	1, 2, 4, 5	medium	• Control documents, EMS tracking, monitoring of measures
Operational planning and control	1, 2, 3, 4, 5	medium	• Process planning, application of life cycle analysis
Emergency preparedness and response	1, 2, 3, 4, 5	high	• Control of environmentally relevant activities, emergency scenarios
Procurement	1, 2, 5	low	
Monitoring, measurement, analysis and evaluation of environmental performance and the EMS, infrastructure and maintenance	2, 3, 4, 5	high	• Including inspection of technical equipment, functionality/accuracy of measurement technology
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 14001 is possible for up to 50 % of the respective audit time without a separate individual risk assessment. This is particularly possible if the environmental aspects at the site are classified as relatively simple, such as low emissions, no relevant use of hazardous substances and no site in ecologically sensitive areas (FFH, Natura 2000, etc.). For sites with a comparable structure and a centrally controlled management system, an increased proportion of remote auditing is often uncritical (e.g. sales offices) and may be applied for where appropriate.

Conversely, the proportion of remote auditing should be reduced or switched entirely to on-site auditing if complex or permit-relevant environmental aspects are present, such as in the case of IED facilities or sites with complex permits and conditions. The same applies in the event of environmental incidents, complaints, high-profile sites, or if significant changes have occurred since the last

audit. New or restructured sites, as well as independent subsidiaries with environmental responsibilities, generally require an individual risk assessment.

A clear justification for the proportion of remote work included in the audit plan or report is required in all cases, particularly in borderline cases.

Date: 18.09.2025

signed Yulia Felker
Head of EMS