Technical Specification

ISO/IEC TS 17012

First edition
2024-07

Conformity assessment — Guidelines for the use of remote auditing methods in auditing management systems

Reference number
ISO/IEC TS 17012:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the ISO Committee on Conformity Assessment (CASCO).

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document was developed in response to rapidly developing technology and changes in working practices based upon a variety of experiences, including those from the coronavirus pandemic. Applying remote auditing methods can bring a variety of benefits for all parties involved in the audit. This document provides guidance on how an audit can be effectively conducted and how audit objectives can be achieved when remote auditing methods are used.

Remote auditing methods can improve the efficiency of an audit by reducing travel-time and expense and achieving an improvement in the overall carbon footprint, as well as avoiding travel risk, enabling virtual access to more sites. A further benefit is facilitating diversity of participation in the audit and the increased involvement of technical experts within the audit. This includes cross-border activities that can improve the overall efficiency of the audit, whilst maintaining business continuity, especially in challenging situations and conditions.

The objective of this document is to provide assurance that remote auditing methods represent an additional sustainable and flexible way to conduct audits of management systems and provide confidence to customers, regulators, scheme owners and other interested parties.

This document includes guidance on a risk-based approach to be followed for planning and implementing the remote auditing methods that can apply to all types and sizes of organizations. Table 1 and Table 2 provide examples of risks and opportunities.

This document can be used to support an on-site, a remote or a hybrid approach to auditing management systems.

NOTE ISO 19011:2018, Table 1 gives examples of different types of audits.

This document can also be used to support other conformity assessment activities, such as accreditation assessment, product certification or peer assessment.

This document supports the continued integrity of first-party, second-party and third-party audits, including management system certification audits, to facilitate their conduct in a competent, thorough and transparent manner when remote auditing methods are used. This document can also be used to support other conformity assessment activities, such as accreditation, product certification or peer assessment. This document provides additional guidance to the implementation of ISO 19011:2018 and ISO/IEC 17021-1.

This document highlights the importance of ensuring that the output of any audit process fulfils the objectives of the audit programme. This document does not take precedence over any requirements of other standards/schemes.

This document follows the same structure as ISO 19011:2018 in order to facilitate use of the two documents together.

Conformity assessment — Guidelines for the use of remote auditing methods in auditing management systems

1 Scope

This document provides guidance on the use of remote auditing methods in auditing management systems. It is applicable to all organizations that plan and conduct all kinds of internal or external audits (i.e. first-party, second-party and third-party audits) of management systems.

This document supports the general principles of auditing given in ISO 19011:2018 and provides further guidance on specific conditions, possibilities and limitations for implementing remote auditing methods.

This document is intended to strengthen confidence in the use of remote auditing methods for auditing management systems among customers, regulators, accreditation bodies, certification bodies, scheme owners, industry, employees, consumers, suppliers and other interested parties.

The use of remote auditing methods for auditing management systems is not intended to replace on-site audit methods. Instead, remote auditing methods are intended to serve as a tool to effectively and efficiently conduct the audit.

NOTE This document can be used for other types of audits and assessments.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17000, *Conformity assessment — Vocabulary and general principles*

ISO 19011:2018, *Guidelines for auditing management systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 19011:2018 and ISO/IEC 17000 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
remote auditing method
method used for conducting audit activities from any place other than the location of the auditee

Note 1 to entry: Remote auditing methods can be used in combination with on-site methods to achieve a full and effective audit.

Note 2 to entry: Remote auditing methods can be used for virtual locations, i.e. where an organization performs work or provides a service using an online environment, enabling individuals to execute processes irrespective of physical locations.

Note 3 to entry: Remote auditing methods can be used by the auditor at one site of the auditee to audit another site.

4 Principles of auditing

The principles of auditing are given ISO 19011:2018, Clause 4.

5 Managing an audit programme

5.1 General

5.1.1 General guidance is given in ISO 19011:2018, 5.1.

5.1.2 When preparing the audit programme, the organization should consider the following in relation to the use of remote auditing methods:

a) the principles mentioned in Clause 4;

b) risks related to the effectiveness of the audit programme (see 5.3) and the countermeasures;

c) opportunities related to the audit programme (see 5.3);

d) information security, confidentiality and privacy issues related to remote auditing methods;

e) the availability of information required to make judgment on their applicability;

f) the acceptability for and limitations of scheme owners, regulators and other specifiers;

g) the ability to use them.

5.2 Establishing audit programme objectives

5.2.1 General guidance is given in ISO 19011:2018, 5.2.

5.2.2 The organization carrying out the management system audit can use remote auditing methods under, but not limited to, the following conditions:

a) the remote auditing methods do not prevent the achievement of audit programme objectives;

b) the use of remote auditing methods is appropriate and accepted by the relevant interested parties;

c) the technologies have been selected and their management has been defined;

d) the information required for using remote auditing methods is sufficient;

e) the scope of the use of remote auditing methods (audit criteria and boundary) has been determined in the audit programme;

f) the ability of both parties (i.e. the audit team and the auditee) to use remote auditing methods has been confirmed, including personnel competence, technical abilities and physical abilities;

g) the organization carrying out the management system audit and the auditee have resolved any differences in the understanding of remote auditing methods;

h) there is an agreement in place to alter the remote auditing method when necessary.

NOTE Alteration of remote auditing methods can include other remote or on-site auditing methods.

5.2.3 When appropriate, the organization carrying out the management system audit should prepare and implement a process to investigate the auditee's ability to use remote auditing methods.

The organization carrying out the management system audit should review the obtained information related to remote auditing methods and communicate with the auditee to:

a) review whether the auditee meets the conditions for the application of remote auditing methods, as determined by the assessment of risk associated with their use (see 5.3);

b) confirm the following:

   1) the feasibility of achieving the audit objectives within the defined audit scope when remote auditing methods are used;

   2) the support conditions for using remote auditing methods, including technological support to resolve any issue;

   3) any specific or additional requirements for the agreed remote auditing methods including competencies.

5.3 Determining and evaluating audit programme risks and opportunities

5.3.1 General guidance is given in ISO 19011:2018, 5.3.

5.3.2 The organization carrying out the management system audit should consider risk and opportunities on the audit programme, taking account of the knowledge of the auditee and any previous experience to determine whether remote auditing methods are feasible. Remote auditing methods should not be permitted when the assessment of risk identifies an unacceptable threat to the effectiveness of the audit process. Subsequent planning should:

— prevent or reduce risks associated with the remote auditing methods;

— leverage opportunities identified from the use of remote auditing methods;

— cover the evaluation of the effectiveness of actions taken to address the risks and opportunities;

— ensure that the expected results of the audit will be achieved.

5.3.3 Examples of risks and opportunities related to an audit programme and their potential impacts are given in Table 1 and Table 2.

Table 1 — Risks related to audit programmes and potential impact due to use of remote auditing methods

Risks	Potential impact
Processes requiring observation not adequately addressed in the audit programme	The processes would not be effectively audited.
Inability to use remote auditing methods due to the nature of the process	The processes would not be effectively audited.
Limitations in the application of random sampling	The processes would not be effectively audited.
Unknown capability of auditee to contribute to application of remote auditing methods	The necessary technical equipment is not adequate and thus prevents a trouble-free audit process.
Insufficient overall competence of the audit team to conduct audits effectively, using remote auditing methods	The audit objectives would be compromised.
Time loss due to insufficient digitization	Necessary information needs first to be digitized. The loss of time can prevent all information from being reviewed.

Table 1 *(continued)*

Risks	Potential impact
Limited competence or experience in the use of remote auditing technologies	Ineffective or incorrect use of the technologies can limit the process and the quality of the implementation of the audit plan.
No provision for an alternative plan in case remote auditing methods fail	Audit objectives can be compromised.
The specific requirements for data protection and information security when digital information is exchanged are not considered	There is a potential breach of data protection legislation.
Inadequate or unreliable technology (e.g. that related to stability and quality of internet)	The audit cannot be performed, or it is performed in an ineffective manner.
Inability to provide adequate sensory information	Poor quality of visual and audio communications, as well as a lack of any perception of odour, vibration, temperature and relative humidity, can limit the potential to obtain reliable audit evidence.
Integrity of audit evidence can be compromised via the use of remote auditing methods (e.g. reduced legibility of documented information, poor video resolution, lack of visibility of parts of the process)	Possibly wrong or decreased reliability of audit conclusions.

Table 2 — Opportunities related to audit programmes and potential impact due to use of remote auditing methods

Opportunities	Potential benefit
Travel time is reduced or eliminated	The reduction in travel time leads to cost savings, productivity, continuity in the audit and reduction in carbon emissions from travel.
Optimized audit time	Can eliminate or reduce the time for site induction and transfer between audit locations or processes; uses technology to view wide areas.
Short reaction time	The recording of opportunities and risks takes place in a timely manner, especially for locations requiring long journeys. Consequently, the audit programme and audit plan can be adjusted quickly.
Easier scheduling and effective participation despite interested parties being at different locations	The scheduling of audits, especially for participants and observers at different locations where travel is difficult to schedule or organize, is simplified because the location is not a deterrent.
Easy involvement of external parties	Temporary involvement of external parties (e.g. technical experts) is easy to plan and implement when necessary for only a short time.
Auditability of processes across locations	Cross-location processes and their interfaces can be easily planned and audited in unison, and do not have to be divided.
Ad hoc and short notice assessments for acute topics	In the event of sudden deviations, a defined group of participants can schedule and conduct an audit at short notice to clarify the issues.

Table 2 *(continued)*

Opportunities	Potential benefit
Easier documentation and reporting	Since much evidence is available electronically, the effort for managing documentation and reporting can be reduced.
Direct access to data	The availability of audit evidence in electronic applications, so that large data files do not need to be transferred and electronic security is properly managed.
Health and safety of the audit team	No exposure to potentially hazardous conditions (e.g. conflict, civil unrest, health risks, radiation, transport risks).

5.4 Establishing the audit programme

5.4.1 General guidance is given in ISO 19011:2018, 5.4.

5.4.2 When preparing the audit programme, the organization carrying out the management system audit should:

a) ensure that the use of remote auditing methods does not contradict the principles stated in Clause 4;

b) consider, but not be limited to, the relevant aspects in 5.4.3.

5.4.3 The organization carrying out the management system audit should communicate with the auditee on the implementation of remote auditing methods, confirm and reach an agreement with the auditee on the following relevant aspects:

a) the competences and responsibilities of the organization carrying out the management system audit (including personnel), the auditee and external providers [e.g. suppliers of information and communication technology (ICT) services being used for remote auditing methods, such as third-party software platforms];

b) information security risks and control measures;

c) the scope and boundary of remote auditing methods;

d) resources (including the remote auditing software platform), approaches and methods for using remote auditing methods;

e) actions including, if relevant, alternative communication related to any disruption issues;

f) the evaluation of audit results and the effectiveness of remote auditing methods in meeting the audit objectives;

g) information security and risks related to the protection of intellectual property rights.

NOTE Legal requirements can apply.

5.5 Implementation of audit programme

5.5.1 General guidance is given in ISO 19011:2018, 5.5.

5.5.2 The organization carrying out the management system audit should designate an audit team with the ability to use remote auditing methods and communicate the relevant requirements from the audit programme with the audit team leader.

5.5.3 Remote access to documented information pertaining to the audit should be retained at least until the auditor presents the report.

NOTE Remote access to documented information can be granted if needed for audit follow-up activities.

5.6 Monitoring the audit programme

5.6.1 General guidance is given in ISO 19011:2018, 5.6.

5.6.2 When monitoring the audit programme, the organization carrying out the management system audit should monitor the use of remote auditing methods to ensure the effectiveness of the audit programme.

a) The organization carrying out the management system audit should determine the content of the audit programme to be monitored, including, but not limited to:

   1) the adequacy and suitability of audit resources, including personnel competency and remote auditing method performance;

   2) (when applicable) the suitability of actions including alternative communication related to any disruption;

   3) the effectiveness of information confidentiality and security control measures.

b) The organization carrying out the management system audit should determine the monitoring frequency based on the results of risk identification and evaluation. Monitoring methods include, but are not limited to, using technology appropriate to remote auditing methods to observe the audit activities of the audit team.

c) When the outcome of the monitoring shows that the audit process is not implemented in accordance with the audit programme or fails to meet the audit objectives, supplementary audit, alternative site-based or remote auditing methods or other remedial measures should be implemented. Appropriate documented information should be retained as evidence for monitoring.

5.7 Reviewing and improving audit programme

5.7.1 General guidance is given in ISO 19011:2018, 5.7.

5.7.2 When reviewing the audit programme, the organization carrying out the management system audit should evaluate the suitability and adequacy of the audit programme when remote auditing methods are used.

5.7.3 In order to improve the audit programme, consideration should be given to the audit results and to the feedback on the use of remote auditing methods, including:

a) whether the audit objectives have been achieved stating changes that need to be made;

b) efficiencies or other benefits, or difficulties encountered;

c) other relevant feedback (e.g. regarding the suitability of remote auditing methods for specific processes, sites or functions, or regarding new needs in terms of competence);

d) lessons learned from the application of remote auditing methods.

5.7.4 Based on considerations in 5.7.3, amendments and improvements of the audit programme can be implemented for the existing audit programme for subsequent audits and future audit programmes.

6 Conducting an audit using remote auditing methods

6.1 General

6.1.1 General guidance is given in ISO 19011:2018, 6.1.

6.1.2 The selection of the remote auditing methods to be used for an audit depends on the audit type, the audit objective(s) and the scope of the audit being conducted.

NOTE Guidance on application of remote auditing methods is provided in Annex A.

6.1.3 The audit participants should collaborate to ensure the remote auditing methods are used effectively.

6.1.4 It is the auditor's responsibility (see 5.5) to conform to applicable information security requirements while conducting an audit using remote auditing methods.

6.2 Initiating audit

6.2.1 General guidance is given in ISO 19011:2018, 6.2.

6.2.2 The audit team leader should establish contact with the auditee to:

a) confirm the authority to conduct the audit using the remote auditing methods identified for the audit;

b) provide information to the auditee regarding the specific remote auditing methods to be used;

c) receive information from the auditee regarding details on the remote auditing methods being provided (e.g. the communications platform);

d) request remote access to relevant information for the planning and conducting of the audit;

e) establish the extent to which electronic documented information and objective evidence is available, to enable an audit using remote auditing methods;

f) where applicable, obtain appropriate consent (e.g. transcription, recordings, images);

g) confirm data security and confidentiality requirements for the remote auditing methods identified for the audit;

h) confirm any other risks that can limit or require on-site activities (e.g. health and safety, restricted access, electronic Faraday cage);

i) confirm the competence of the auditee to use the remote auditing methods planned;

j) consider any opportunities that can reduce risk (e.g. to the safety of auditors) due to remote auditing methods.

6.2.3 The risks and opportunities should be considered to determine whether modification of effort and/or resources is needed to ensure the audit objectives are achieved. The review can result in a change in the auditing methods being applied (e.g. a combination of methods can be used instead of entirely remote auditing methods).

6.3 Preparing audit activities

6.3.1 Performing review of documented information

General guidance is given in ISO 19011:2018, 6.3.1.

6.3.2 Audit planning

6.3.2.1 General guidance is given in ISO 19011:2018, 6.3.2.

6.3.2.2 The risks and opportunities related to the use of remote auditing methods should be considered in audit planning.

6.3.2.3 When preparing for the audit activities that involve the use of remote auditing methods, the following should be considered and, as appropriate, agreed with the auditee:

a) when reviewing the audit plan, confirm the duration of audit for each day taking, into account the time zones;

b) agree on alternative means of communication in case the main tool becomes unavailable;

c) confirm protocols to manage the use of ICT, such as audio and video platforms;

d) ensure the functionality of the technology for the remote auditing methods, where applicable, including:

   1) accessibility to the platform particularly to accommodate special needs (e.g. transcription availability, if necessary);

   2) confirmation of availability of the documented information via electronic means;

   3) use of file-sharing services;

   4) the quality of the audio and video platform;

   5) translation channels or additional platforms;

   6) the arrangement for remote breakout sessions;

e) conclude agreements on confidentiality, privacy, data security and access requirements;

f) confirm any information that the auditee needs to make available in advance (e.g. including a list of typical documented information, objective evidence and roles and responsibilities);

g) agree on the translation tools and methods (including translation and transcription technologies) to be used before and during the audit;

h) consider the need to secure technical support for any technology to be used for the remote auditing method chosen for the audit, including assigning the roles for platform support (camera, audio), safety and access (see 6.4.2);

i) consider data protection, record retention, intellectual property, security clearance and other data use and access controls;

   NOTE 1 Legal requirements regarding data protection can apply.

j) consider the use of means such as recordings, transcripts, photos and drones;

   NOTE 2 Legal requirements can apply.

k) confirm responsibilities for providing access to the platform to the audit participants, including audit team members, auditee's representatives, interpreters, observers and support personnel;

l) when a combination of remote and on-site auditing methods is used, ensure that the plan is clear as to which part of the audit will be remote, which auditor(s) will be remote, which auditor(s) are to be on-site and which methods are to be used by which auditor(s).

6.4 Conducting audit activities

6.4.1 General

6.4.1.1 General guidance is given in ISO 19011:2018, 6.4.1.

6.4.1.2 When remote auditing methods are used, specific consideration should be given to the risks and opportunities that can be encountered during the conduct of the audit, including techniques that are not used in face-to-face activities. Annex A provides some examples.

6.4.2 Assigning roles and responsibilities of support personnel and observers

6.4.2.1 General guidance is given in ISO 19011:2018, 6.4.2.

6.4.2.2 When using remote auditing methods, support personnel, observers and surrogate auditors (see A.3.3) should be included in the communications and planning processes, as appropriate.

6.4.2.3 Support personnel

For remote auditing methods, the roles and responsibilities of the support personnel will be similar to those for on-site audits and can be performed by the auditee or the organization performing the audit. Support personnel can include a number of different personnel including, but not limited to, interpreters, information technology (IT) technical staff and guides.

Support personnel can help to:

a) facilitate the set-up (e.g. camera, audio and visual), communication and operation of remote auditing methods (e.g. opening/closing meeting, interviews, observing the processes);

b) arrange access of the audit team and, as appropriate, support personnel to the auditee's documented information by remote auditing methods;

c) ensure the audit team and support personnel are using agreed remote access protocols, including requested devices and software;

d) conduct technical checks on the remote auditing tools ahead of the audit to resolve technical issues, such as background noise disruptions and interruptions;

e) ensure contingency plans are available and communicated to all audit participants (e.g. interruption of access, use of alternative technology);

f) ensure confidentiality and privacy during the use of remote auditing methods (e.g. by muting microphones and pausing cameras).

6.4.2.4 Observers

Remote observers should follow the same guidance as observers on-site. Observers should have access to the same remote auditing methods used.

If any documented information is shared with the auditors (e.g. via email or other data-sharing methods), arrangements should be made for observer(s) to access the documents as necessary.

6.4.3 Conducting the opening meeting

6.4.3.1 General guidance is given in ISO 19011:2018, 6.4.3.

6.4.3.2 The content of an opening meeting does not change with the use of remote auditing methods. When using remote auditing methods, the following additional considerations can improve the effectiveness of the audit.

a) The audit team leader should confirm and record who attends the opening meeting, ensuring that if participants are remote, they are identified along with the other pertinent information. Pertinent information can include the roles of the participants in the organization, the roles of the participants in the audit, the platform or technology being used and time zones.

b) Remote attendance can be used to provide for additional attendees to encourage organizational representation and/or educational opportunities provided that the meeting size is manageable.

c) Attendees should be able to contribute to the meeting (e.g. by asking questions or seeking clarification).

d) The audit team leader sets the expectations for the conduct and contributions and confirms the functionality and information that will be provided and/or used, as well as encouraging participants to engage in the audit activities. The audit team leader/support personnel ensures that information presented in the opening meeting is made available to remote participants and observers (e.g. the audit plan should be displayed for all participants).

e) Any changes in the audit schedule, remote auditing methods or access are confirmed.

f) The audio should be provided for attendees to hear the meeting and for the participants to be able to use the technology platform and communication.

g) The audit team leader should explain any need for modifications in the conduct of the audit in order to accommodate the use of remote auditing methods (e.g. to record the audit results which can cause short breaks).

6.4.4 Communicating during the audit

6.4.4.1 General guidance is given in ISO 19011:2018, 6.4.4.

6.4.4.2 Additional communication needs should be considered for audits using remote auditing methods, including but not limited to:

a) additional private communication channel(s) (e.g. a private room for the audit team, communication applications);

b) a backup method or support method to ensure continuation of communication if the main platform is unstable or lost during the audit activity;

c) an option to communicate with the support personnel/guide during the audit activities;

d) technical support when multiple remote auditing methods are used;

e) defining the rules for asynchronous communications (time-insensitive data transmission where the timing of the data generating and consuming can be different, e.g. emails, chat, recorded videos, self-paced training/induction modules).

6.4.5 Audit information availability and access

General guidance is given in ISO 19011:2018, 6.4.5.

6.4.6 Reviewing documented information while conducting the audit

6.4.6.1 General guidance is given in ISO 19011:2018, 6.4.6.

6.4.6.2 The use of remote auditing methods can introduce additional risks and opportunities related to the review of documented information. Auditors should be mindful of the information integrity and authenticity risks as well as opportunities to enhance sample size and data access in auditing.

6.4.7 Collecting and verifying information

6.4.7.1 General guidance is given in ISO 19011:2018, 6.4.7.

6.4.7.2 When using remote auditing methods, additional consideration can be needed for the verification of information. For example, artificial intelligence (AI) or simulations can require additional review of inputs prior to being used by the audit team.

6.4.7.3 When using remote auditing methods for collecting information, the following should be considered:

a) the limitations of the application of the remote auditing methods to obtain objective evidence on aspects such as the areas, locations, processes and equipment;

b) when using asynchronous tools (e.g. messaging applications, connections to remote servers or external provider's systems), additional steps are needed to verify the information (e.g. agreement of response time, awareness of system maintenance);

c) risk where objectivity of audit evidence is compromised (e.g. integrity of software and data, integrity of presented information);

d) risk from limitations on access to audit evidence;

e) recognition of the opportunities to increase the effectiveness of the audit (e.g. by means of increasing the sample, access to different type of audit evidence, covering more sites, faster collection process);

f) sampling of information can be more effective for data and records, but can pose additional risks in areas such as interviews and observations;

g) provision of flexibility regarding the timing and location of the interviews;

h) the absence of sensory data such as smell;

i) risks of abuse/deception.

NOTE Annex B provides further guidance on useful practices.

6.4.8 Generating audit findings

General guidance is given in ISO 19011:2018, 6.4.8.

6.4.9 Determining audit conclusions

General guidance is given in ISO 19011:2018, 6.4.9.

6.4.10 Conducting the closing meeting

6.4.10.1 General guidance is given in ISO 19011:2018, 6.4.10.

6.4.10.2 The content of a closing meeting does not change with the use of remote auditing methods. See 6.4.3 for additional considerations to improve the effectiveness of the audit.

6.5 Preparing and distributing audit report

6.5.1 General guidance is given in ISO 19011:2018, 6.5.

6.5.2 The audit report should record the remote auditing methods used, their extent and effectiveness, including any benefits or limitations. Declarations and attestations related to the audit report should demonstrate the principles of confidentiality and due professional care (e.g. the extent of AI use in report generation). Audit reports and related records should indicate the extent to which ICT has been used in carrying out the audit.

6.6 Completing audit

General guidance is given in ISO 19011:2018, 6.6.

6.7 Conducting audit follow-up

6.7.1 General guidance is given in ISO 19011:2018, 6.7.

6.7.2 Consideration should be given to the suitability, effectiveness, risks and opportunities of remote auditing methods for conducting follow-up activities.

7 Competence and evaluation of auditors

7.1 General

General guidance is given in ISO 19011:2018, 7.1.

7.2 Determining auditor competence

General guidance is given in ISO 19011:2018, 7.2.

7.2.1 General

In determining the necessary competence for an audit, an auditor's knowledge and skills related to the following should be considered:

a) the methods of auditing, including on-site, remote or a combination of both;

NOTE ISO 19011:2018, Table A.1 provides examples of audit methods that can be used, singly or in combination, in order to achieve the audit objectives.

b) the uncertainty in achieving audit objectives, noting that for remote auditing methods the following can contribute to the uncertainties in achieving audit objectives:

- internet connectivity;
- software compatibility;
- hardware availability;
- data integrity;
- information security and confidentiality;
- the reliability of the objective evidence shared by the auditee during the remote audit;

c) other requirements impacting remote auditing methods and techniques.

7.2.2 Personal behaviour

General guidance is given in ISO 19011:2018, 7.2.2. However, desired personal behaviour can be exhibited differently when remote auditing methods are used. Following complementary guidance on personal behaviour can also be beneficial.

Examples of personal behaviour pertinent to remote auditing methods can include:

a) willingness to work remotely;

b) observant, i.e. actively observing how and where activities occur, and being comfortable with technology to allow for effective observation;

c) open to improvement, i.e. familiarization with emerging technologies;

d) patience, i.e. with audit participants, records retrievals and questions, as well as dealing with issues with technology such as internet connectivity;

e) confidence in the use of remote auditing technology;

f) resilience to stress;

g) sensitivity to digital data privacy;

h) adaptability, i.e. dealing with emergencies.

7.2.3 Knowledge and skills

7.2.3.1 General

Auditors should possess the knowledge and skills necessary to achieve the intended results of the remote audits they are expected to perform (e.g. computer skills, knowledge of information security and confidentiality management, handling of online meeting platforms and the use of information and communication technology necessary for effective audit).

NOTE Legal requirements can apply.

7.2.3.2 Generic knowledge and skills of management system auditors

Auditors should understand the risks and opportunities of remote auditing methods and have the knowledge and skills as outlined below:

a) understand the increased risks associated inherently with such audits, including the potential confidentiality and information security risks from the remote auditing methods;

b) understand the increased planning and organization needed for the remote auditing method, including the communication with the auditee;

c) understand the impact of using remote auditing methods in relation to audit time, the audit programme and related audit plan;

d) ensure that the records examined remotely are what the auditors have asked for, rather than what the auditee makes available or wants the auditors to see;

e) make the additional necessary effort to establish audit findings and conclusions when using remote auditing methods (e.g. multiple electronic sources or embedded electronic files need to be reviewed);

f) establish the integrity of the data being reviewed remotely;

g) use different technologies to conduct the audit and effectively interact with other team members and the auditee, including when faced with unexpected issues with respect to infrastructure and operational environment (e.g. poor network connection);

h) have the ability to mitigate disruptive behaviour at the remote location (i.e. lateness, inattentiveness, and argumentative behaviour);

i) have a basic understanding of databases and AI where used as part of remote auditing methods.

7.2.3.3 Discipline and sector-specific competence of auditors

Auditors should demonstrate the following competencies:

a) the ability to evaluate the suitability and risks of remote auditing methods to the audited industry sector and management system discipline;

b) an understanding of management system standards and other relevant requirements, including scheme owner requirements related to remote auditing methods (e.g. restrictions impacting the use of remote audits).

7.2.3.4 Generic competence of audit team leader

The audit team leader should demonstrate the following competencies:

a) provide support and address issues faced by the audit team in the use of remote auditing methods;

b) ensure coherence among team members in the use of remote auditing methods, including a combination of on-site and remote collaboration methods.

7.2.3.5 Knowledge and skills for auditing multiple disciplines

When auditing multiple discipline management systems, the audit team should have an understanding of any risks and opportunities imposed by remote auditing methods in auditing different management systems.

7.2.4 Achieving auditor competence

Auditor competence can be achieved through training, mentoring and gaining experience in using remote auditing methods and techniques.

7.2.5 Achieving audit team leader competence

General guidance is given in ISO 19011:2018, 7.2.5.

7.3 Establishing auditor evaluation criteria

General guidance is given in ISO 19011:2018, 7.3.

7.4 Selecting the appropriate auditor evaluation methods

7.4.1 General guidance is given in ISO 19011:2018, 7.4.

7.4.2 In selecting auditor evaluation methods, consideration should be given to the accessibility and effectiveness of the technology to observe, interview and test the auditor in the use of remote auditing methods.

7.4.3 General guidance is given in ISO 19011:2018, Table 2.

Additional examples related to auditor evaluation using remote auditing methods can include:

a) reviewing video recordings of auditor performance;

b) testing of auditor competence in applying remote auditing methods;

c) using live transcriptions/translations.

7.5 Conducting auditor evaluation

7.5.1 General guidance is given in ISO 19011:2018, 7.5.

7.5.2 In conducting auditor evaluation, consideration should be given to:

a) the feasibility and effectiveness of the technology to observe, interview and test the auditor in the application of remote auditing methods;

b) the competence of the evaluator in the evaluation methods selected, the technologies used for the evaluation and the application of the remote auditing methods.

For observation requiring different methods other than the ones used for the audit, care should be taken to not influence or interrupt the audit.

7.6 Maintaining and improving auditor competence

7.6.1 General guidance is given in ISO 19011:2018, 7.6.

7.6.2 Consideration should be given to specific knowledge and skills, such as the ability to use new or change remote auditing methods, software and electronic equipment, taking into account the pace of change of technologies.

Annex A
(informative)

Remote auditing methods

A.1 Types of audits using remote auditing methods

A.1.1 Audits using entirely remote auditing methods

In an audit using entirely remote auditing methods, no on-site activity is planned with any auditor. The feasibility of using remote auditing methods can be determined through an assessment of the risks related to the nature of the organization's products and/or services, remote access to relevant processes, locations and the organization's management system documentation, time zones of auditor and auditee, etc.

A.1.2 Audits using a combination of methods

An audit where a combination of methods is used, and where at least one part is conducted on-site, can be referred to as a "hybrid" or a "blended" audit. For example, one auditor conducts specific parts of the audit on-site, such as production and service, while another auditor conducts document review remotely using ICT (in some cases this can be fully remote, reviewing the document without interaction with the entity until after the document review). Use cases can include when using on-site auditors with partial qualification or conducting audits over an extended period.

NOTE It is important to consider the assessment of risk related to the tools used to determine the best approach. For example, hosting of servers to store and transfer documents can be an issue if multi-national auditors or audit teams are used.

A.2 Technological considerations

A.2.1 When implementing remote auditing methods, the following technological considerations should be covered.

a) The use of shared folders, drop boxes, file transfer protocol (FTP) servers, email, encrypting technology ["end-to-end" (e2e)], and video conferencing software should be verified to be accessible/visible and to have audio/video that can be heard/watched by all participants without interference.

b) Communication protocols should be communicated before the audit (e.g. agreement on when a participant can interrupt a speaker, or the use of raised hand or other indication for interventions or inputs).

c) Data integrity and traceability should be assured by using technologies such as digital signature.

d) Connections that have high dropout rates should be avoided.

e) Backup should be provided when mobile phones are used. At the beginning of the audit, it should be clarified how to contact the auditee in case of a technical difficulty.

f) It should be ensured that IT support can be accessed at the auditee location if the auditee is hosting/providing the platform.

A.2.2 The following examples can be provided by the auditee or by the organization carrying out the management system audit:

a) use of the video stabilizing feature of mobile phones, stable phone holders (e.g. attached to the neck, chest or a pole) and noise cancelling features;

b) use of drones for areas that are not easily accessible (permission to use; the operator should be qualified to fly the drone; all information should be provided prior to the audit);

c) different channels for the use of auditors, including breakout rooms and different team members channels;

d) a method for the audit team to communicate to each other confidentially.

A.3 Examples of implementation of methods

A.3.1 Auditing documented information:

Handling documented information when using remote auditing methods can be implemented using the following methods.

a) Use of screenshots and screensharing should be clarified and agreed. Screenshots can be a method of grabbing specific information that is to be translated into the audit records. Using screen-sharing software, auditors can view the desktop of an employee or an interested party to observe specific processes or systems.

b) Secure file sharing platforms: Prior to the audit, agreement should be reached on the information to be provided, on the length of time the information is to be made available (held by each party or the exchange platform), on when the documents provided will be deleted, and on how confidential information will be exchanged (e.g. that it is only provided during the audit and not in an exchange platform).

c) Remote data access: With appropriate security measures, auditors can access an organization's systems and databases remotely to analyse data and perform tests.

d) Remote inventory tools: Physical inventories can be implemented remotely using Internet of Things (IoT) devices, Radio Frequency Identification (RFID) technology or video feeds, to validate inventory counts.

e) Data analytics: Auditors can use data analytics tools to analyse large datasets remotely and identify trends, anomalies or potential risks.

f) Remote process mapping: Auditors can use virtual process mapping techniques to understand and assess an organization's workflows and procedures.

A checklist can be used to include relevant items to be agreed upon as part of audit planning. This document can be retained as a supporting document that can become part of the audit report.

When using this approach, it can be beneficial to include a statement in the audit report that the methods and ICT were agreed upon prior to the audit.

A.3.2 Auditing the organization's digital twin

An organization's digital twin is a virtual representation or digital replica of its physical assets, processes, systems, and operations. It can integrate real-time data from sensors, devices and other sources to create a dynamic and interactive simulation. Digital twins can be used in auditing a management system when the accuracy of the digital twin can be verified. Auditing a digital twin can introduce additional risks and opportunities.

A.3.3 Use of surrogate auditors

A surrogate auditor is a person who attends the audit in-person and acts as the eyes and ears of the audit team. The use of surrogate auditors should be agreed during the planning of the audit programme. The audit team leader should plan how the surrogate auditor is to be used during the audit. Surrogate auditors should have competence in the surrogate audit process. Surrogate auditors are not responsible for asking questions, unless guided by the responsible auditor to do so. The responsibility for the audit documentation remains with the audit team leader.

Surrogate auditors should meet the same impartiality requirements as auditors and should have adequate skills, including language skills in the languages of both the auditee and the auditor, if needed.

NOTE Surrogate auditors are not expected to have the same technical competence as the auditors themselves.

An audit where a surrogate auditor is used can require multiple ICT tools. The auditor working remotely should have a means of guiding the surrogate auditor and communicating directly with the surrogate auditor and the auditee, which can be separate from each other.

The use of such interactive means of communication enables the following:

a) conducting interviews;

b) observing work performed with remote guidance;

c) completing checklists and questionnaires;

d) conducting document review with auditee participation.

A.3.4 Document reviews

When conducting document reviews with auditee participation, auditors can request electronic copies of relevant documents for examination, such as financial records, policies, procedures and compliance documentation. The following methods can be used:

a) real-time reading of documents (records, bench sheets) via ICT;

b) electronic submittals [standard operating procedures (SOPs), quality manuals, internal audit and management review reports);

c) remote access to computers and data;

d) software to analyse, translate, search and categorize the documents received remotely during the audit;

e) pre-recorded answers to interview questions.

A.3.5 Personnel interviews

Interviewing personnel remotely can be implemented using the following methods:

a) an in-person web-based visual communication platform that follows the guidance given in this document;

b) a chat-room (or e-mail exchanges);

c) automatic or AI supported translation;

d) web-based questionnaires: auditors may send online questionnaires to the auditee's personnel and management to collect information.

A.3.6 Witnessing of activities

In cases where physical processes need to be audited, remote cameras or live streams can be set up for auditors to observe the operations. Remote witnessing activities can be conducted using the following methods:

a) real-time observation using ICT;

b) a compilation of recorded sequential activities (an activity that occurs over time through sequential steps);

c) interior facility: tour by video camera;

d) exterior facility: conducted using drones;

e) recorded performance of activities to be audited remotely.