International Organization for Standardization
Web: www.iso.org

International Accreditation Forum
Web : www.iaf.nu

Edition 1
Date: 2020-04-16

ISO 9001 Auditing Practices Group

Guidance on:

REMOTE AUDITS

INTRODUCTION

Remote auditing is one of the audit methods described in ISO 19011:2018 Annex A1. The value of this audit method resides in its potential to provide flexibility to achieving the audit objectives. In order to realize the benefits of this audit method, all interested parties should be aware of their role in the process, inputs, expected outputs, and risks and opportunities that will provide the basis to achieve the audit and audit program objectives.

There are a variety of reasons that an auditor may not be present due to safety constraints, pandemics or travel restrictions. The voluntary or mandatory confinement due to the current COVID19 pandemic, commissioning of windmill assembly of scaffold, explosive testing and other scenarios are all examples where auditing remotely is beneficial.

New information and communication technologies (ICT) have made remote auditing more feasible. As access to ICT has increased, remote auditing has become more commonly used. This allows the auditor to communicate with people globally, accessing a wide range of information and data.

These techniques transform the way we work. These ICT open the opportunity to audit sites and people remotely, shortening distances, travel time and costs, reducing the environmental impact associated with audit travel, adapting audits to different organizational models. ICT can help to increase the size or quality of sampling in the audit process, when prepared, validated and used properly. This is the case, for example, when using video cameras, smart phones, tablets, drones or satellite image to verify physical settings such as pipe identification in the petroleum industry, machinery settings, storage areas, production processes or forest or agricultural sites.

Use of ICT also allows for the inclusion of expertise in an audit that otherwise might not be possible due to financial or logistical constraints. For example, the participation of a technical expert may only be needed to analyse a specific project for only two hours. With ICT available the technical expert may be able to analyse the process remotely, thereby reducing time and costs associated with travel.

On the other side, however, we must consider the limitations and risks posed by ICT in the fulfilment of audit objectives. These include information security, data protection and confidentiality issues, veracity and quality of the objective evidence collected, amongst others.

The following are questions that may arise.

- When watching images, are we looking at real time images or are we looking at video records?
- Can we capture everything about the remote site or are we being guided by selected images?
- When planning for a remote interview, will there be a stable internet connection and the person to be interviewed knows how to use it?
- Can the processes and sites to be audited be realistically audited offsite?
- Can you have a good overview of the facilities, equipment, operations, controls? Can you access all the relevant information?

Many of these questions can only be answered after a visit to the site.

To use ICT in the audit process, the audit program manager and the audit team need to identify the risks and opportunities and define decision criteria to accept or not accept its use, where and in which conditions.

In this paper we approach remote auditing from the establishment of the audit program, moving to audit planning and audit realization. We point out to some good and bad practices in its use and we share some examples. We present a generic risk and opportunity analysis for the use of some ICT, that can serve as a basis for the decision-making process.

BACKGROUND INFORMATION ON ISO 19011:2018 AND IAF MD 4

According to ISO 19011:2018, the feasibility of a remote audit using ICT should be considered when establishing the audit program. It is important to verify the adequacy of resources required to ensure an effective audit outcome. In its annex A.1, ISO 19011 gives several examples for the application of remote audit methods in combination with on-site methods.

“Remote audits refer to the use of ICT to gather information, interview an auditee, etc., when “face-to-face” methods are not possible or desired. (ISO 19011)

IAF MD 4 is a mandatory document for the use of ICT for audit/assessment purposes. It defines the rules that certification bodies and their auditors shall follow to ensure that ICT are used to optimize the efficiency and effectiveness of the audit/assessment, while supporting and maintaining the integrity of the audit process.

Both ISO 19011 and IAF MD 4 should be known and considered by the auditors.

An important clarification made in ISO 19011, A.16 is between remote audits and auditing virtual locations. “Auditing of a virtual location is sometimes referred to as virtual auditing.”

Virtual audit is a set of audit activities on a virtual environment. A virtual environment may be composed by digital and/or non-digital activities using technological assets (software, hardware, sensors, PLCs, automated devices) taking some or all decision(s) in the process(es). As an example, a manufacturing plant may have robots doing some production processes but also people doing traditional production processes. The decisions on the production processes made by robots or people are equally important. Those of the robots certainly come from people who make their code, establish their assumptions, decision making criteria and other features.

GENERAL RECOMMENDATIONS FOR REMOTE AUDITS

AUDIT PROGRAM

Considerations for the use of remote auditing techniques

IAF documents, accreditation bodies, and certification bodies’ requirements provide the framework to determine eligibility for the use of remote auditing technics. For second- and first-

party audits, it is the customer or audited organization's purview to determine convenience of remote auditing according to audit objectives.

Feasibility

The use of ICT for remote auditing will only be successful if the right conditions are in place. The fundamental ones are that technology is available and that both auditors and auditees are competent and at ease with its operation. This should be assessed prior to the decision to use remote techniques. This preparation contributes to optimizing the audit process.

There are two general scenarios:

- On-site remote auditing: the auditor is at the organization sites and is auditing people, activities or processes that are offsite;
- Off-site remote auditing: the auditor is not at the organization and people and processes are located either at the clients facility or at another location (such as an off-site installation).

The first step to ensure feasibility is determining what technology may be used, if auditors and auditees have competencies and that resources are available.

Feasibility also depends on the online connection quality. A weak bandwidth or limited hardware capability may slow the process to the point of inefficiency. The audit process may be affected by the speed at which the auditee access and shows evidence by video, or through a tablet or computer.

Confidentiality, Security and Data Protection (CSDP)

Critical to the use if ICT are confidentiality and security issues, as well as data protection. The CB and the organization should take into consideration legislation and regulations, which may require additional agreements from both sides (e.g. there will be no recording of sound and images, or authorizations to using people's images), and possibly from the auditee itself. Where applicable by National law, the DPO (data protection officer) of both organizations should be involved in assessing these issues. In some situations' security requirements will not allow for the use of ICT.

To prepare for the use of ICT, all certification legal and customer requirements related to confidentiality, security and data protection should be identified and actions taken to ensure their effective implementation. This implies that both the auditor and the auditee agree with the use of ICT and with the measures taken to fulfil these requirements.

Evidence of agreements related to CSDP should be available. This evidence could be records, agreed procedures, or emails. The importance resides in having these CSDP criteria acknowledged by all participants.

Measures to ensure confidentiality and security should be confirmed during the opening meeting.

The audit team should prevent the access and retention of more documented information than it would in a normal face to face audit. It is probable that the audit team will want to have access to more information to prepare for the audit, or to have the ability to analyse documented information in an asynchronous way. However, it is important to reinforce trust in the audit process.

It is a good practice that when documented information is to be analysed in an asynchronous manner, it should be shared in a secure and agreed system, such as cloud based, Virtual Private Network or other file-sharing systems, utilizing CSDP guidelines. Once the audit is complete, the auditor should delete from its system or remove access to any documented information and records not required to be retained as objective evidence.

Auditors shoud not take screenshots of auditees as audit evidence. Any screenshots of documents or records or other kind of evidence should be previously authorized by the audited organization.

Risk assessment

The risks for achieving the audit objectives are identified, assessed and managed.

Another important issue is to understand what processes, activities or sites of the organization may be audited remotely with which ICT tool available.

IAF MD 4 makes clear that this decision should be based in the documented identification of the risks and opportunities that may impact the audit/assessment, for each ICT considered.

The table below lists the main issues to assess feasibility and risk analysis for a remote audit. This assessement should be done and documented for each audit involving all members of the audit team and the audited organization representative.

Any specific arrangements should be documented and communicated between relevant interested parties.

	FEASIBILITY AND RISK ANALYSIS FOR REMOTE AUDITS
1.	**Confidentiality, Security and Data Protection (CSDP)**
	Ensure agreement between auditor and auditee about CSDP issues. Document any arrangements to ensure them.
2.	**Use of ICT**
	There is a stable connection with good online connection quality
	The ICT allows access to relevant documented information including software, databases, records, etc.
	It is possible to make the authentication/identification of interviewed people preferably with image
	If observation of facilities, processes, activities, etc, is relevant to achieve audit objectives, it is possible to access them by video
3.	**People in the organization**
	It is possible to access and interview people relevant for the QMS
4.	**Operations**
	If the organization is not operating regularly, due to contingency situations, the processes/activities being performed are representative and allow fulfilment of the audit objectives
5	**Complexity of the organization and Audit Type**
	In case of complex organizations, processes, or products and services and where the objectives of the audit type require full assessment of the standard and wider sampling (e.g. initial assessment or reassessment) a careful analysis of feasibility of remote audits to fully evaluate the organization conformity to all requirements should be performed.
6	**Conclusions**
	The audit objectives can be attained with the remote audit - proceed to remote audit
	The audit objectives can be achieved partially - a remote audit may be done partially and later complemented with a on site audit
	The audit objectives cannot be attained via remote audit

Finally, when analysing feasibility, the digital quality of the data to be reviewed should also be considered. This is more relevant when the organization still retains information on paper that needs to be scanned for remote review.

The Annex in this paper provides a generic identification of potential risks and opportunities by type of communication technology and it can be used as starting point to the determination of R&O for the decision-making process. In any case the determination, should be made or revised for each situation. It is also important to remember that the intent is not to design a complex, formal and quantified approach to risk and opportunity determination. The intent is to have the ability to identify the opportunities and the risks, and to determine if the risks can be mitigated or accepted and in order to take a substantiated decision whether to proceed with the application of remote methods or not.

Determine the use of ICT for the third-party audit cycle

All the information needed to gain an understanding about the organization to assess the application of ICT will not be available before initial audit. One of the main questions, before assessing feasibility is the willingness of the client organization to consent to the application of remote auditing. Remote auditing may only be introduced and confirmed in the audit program after the initial assessment, unless it is determined to be a special case based on established criteria.

In an audit program for an initial certification audit cycle, where there is limited knowledge of the organization, it may be acceptable to conduct some parts of the audits of that cycle remotely, if there are site locations where the processes are repeated from other sites and are not too complex or demanding.

A compelling argument of a special case for a remote audit frequently involves a stage 1 initial audit of a small or medium organization. The audit duration is short, travel time is long and timing for the audit makes it inconvenient to go onsite for 2 separate visits. A stage 1 audit in an ISO 9001 management system has a focus on the system readiness and is usually focused on the documented information. The risks, in this case are also stronger for the organization. As the auditor may lose information for not visiting the premises and the off-site audit may not interact with the main people involved in the system, the risk that the state of preparedness is not well assessed at stage 1 is higher. The organization should be made aware that a remote stage 1 audit will have these risks and that they might lose the full benefits of a stage 1, that is the ability to identify deficiencies in the management system that can be solved before stage 2. For the auditor, stage 2 will allow to mitigate any deficiencies at stage 1. A stage 1 initial audit on site, is also a good opportunity to assess the use of ICT in subsequent audits.

Knowledge of the organization is gained by the audit program manager, during the several audits of the audit cycle regarding its processes, activities, degree of digitalization, ICT available for use, criticality of sites, results of internal audits, remote activities and people. The auditor should determine and communicate on the maturity of the management system and what records and evidence can be assessed remotely and which need to be observed on site. The audit program may be revised to adjust the use of ICT with the focus to optimize the audit process. For a continuously updated audit program the auditor should give feedback on the use of these techniques at the end of the audit stating changes that need to be made, such as new

processes, sites or functions to be included or withdrawn. Information on the best and/or available techniques, should be communicated.

The audit program should identify what processes, sites or ISO 9001 requirements will be remotely audited.

When allowing for remote auditing to sites, the audit program may switch between on-site and off-site audits ensuring the adequate balance between on-site and remote audits in a certification cycle. The use of remote methods is included in audit time.

AUDIT PLANNING

Audit planning will, at least in the first audits, take longer for the following reasons:

- to assess and document feasibility and risks with the auditee;
- to determine the different ICT used and how they will be used,
- to define the agenda that may need to accommodate dispositions different from an on site audit (e.g. better definition of tasks by different team members to ensure auditors audit separately and make best use of time, more detailed definition of themes to be handled in different time slots which will require a better and previous understanding of the processes of the organization, etc.);
- to allow the organization to identify the people to be audited and ensure their availability at defined time;
- to preview a test on the use of ICT before the audit to confirm that there is a stable connection and people know how to use the technology.

The conclusions, after analysing risks and opportunities, provide the basis for defining what processes to be audited under what ICT.

The auditor should confirm with the organization the feasibility of the remote audit method proposed at the program, based on the required ICT and his knowledge of the organization. This includes the verification that the people involved will know how to use the tool. The auditor reviews the risk and opportunities determined in light of this specific audit and its objectives and may propose changes to the determined use of ICT. In case a high-risk situation is detected the audit should be on-site. All other potential situations should be addressed by appropriate measures to be reflected as needed in the audit plan. Despite using remote auditing methods, the confidence that the desired audit objectives will be reached must be kept.

The plan should clearly identify what, when and how the audit will be conducted.

Examples of requirements, activities and process that are likely to be remote audited:

Audit activities	Remote Interaction
1. Auditing activities a. Opening and closing meetings with people from different sites b. Audit plan reviewing at different stages of the audit c. Intermediate conclusions report d. Audit team intermediate meetings	Phone call, videoconference Web meeting

2. Organization's processes/activities/people a. People working from home or off-site b. Processes or activities where the audit object is mainly the review of documents and explanatory information obtained through interview such as purchasing, human resources/training, commercial processes, design and development. Many of these activities are performed by shared services. c. Infrastructure that has a wide territorial range such as water or energy transportation	Video conference with screen share Realtime video images obtained with drones, mobile or fixed video cameras. Access to video monitoring of sites
3. Particular situations a. Participation of experts	Video conference, real time images, shared screen, asynchronous document and data review

AUDIT REALIZATION

When revising the audit plan at opening meeting the availability and feasibility to use ICT should be confirmed. Measures to ensure confidentiality and security should also be revised and agreed. If the auditor intends to take screen shots copies of documents or other kind of records he should ask for permission, either at opening meeting or when using ICT.

When using ICT to interview individuals the audit team should record the name and function of the interviewed people and tell them what information is being retained. When conducting interviews remotely, the auditor will need to verify statements of fact against other evidence. These need to be asked and analysed by the auditor. If they are sent via email, the auditor should ensure the level of confidentiality required for those documents.

It is also important to ensure that there is no noise disturbing the communication. If the auditor is auditing remotely off site, it should ensure there are no interruptions nor disturbance. Similarly, when there are breaks, ensure the sound is mute and image switched off to ensure privacy.

When using video for watching online live images of remote sites it is important that the organization demonstrates veracity of images. If looking at images of a facility these can be compared with floor plans. Images of a geographical site that are observed can be compared with available satellite images or information available from Geographic Information Systems (GIS).The evidence and the way it was collected should be recorded.

In a remote audit it is important to allow for small breaks, typical of those that usually occur in an unplanned manner in an onsite audit. Being seated and using the screen continuously can be tiresome. To allow small intervals for stretching legs and reducing eye strains helps to enhance attention when receiving feedback.

It is also acceptable for the auditor to inform the auditee when an interruption is required to read and analysize information that has been provided. This allows for increased understanding of the documentation and evidence that has been presented and for determination of additional questions prior to reconvening the interview.

If time is consumed on issues such as network downtime, unexpected interruptions or delays, accesibility problems or other ICT challenges, this time should not be counted as audit time. Provisions for ensuring audit time must be established.

AUDIT CONCLUSION

Audit report should clearly state the extent of use of ICT as well as the effectiveness of its use in achieving audit objectives. The report should indicate those processes that could not be audited and should have been audited on-site. This information is important for the decision process and subsequent audits.

Feedback from the audit team regarding the use of ICT should be given to the audit program manager (see program review).The audit program manager should use this feedback to update the risks and opportunities previously identified.

Annex: Example of identification of Risks and Opportunities for using remote audit techniques

Information and Communication Technology (ICT)	Potential Use	Risks	Opportunities
Video call (synchronous) (e.g.: Skype, WebEx, ZOOM, Hangouts)	Conducting Interviews Guided site tours	Security and confidentiality violations; Differences in time zones; Authentication of the person; Low Quality of communication; The possibility to observe the organization in a more autonomous and free way is weakned as the auditor does not command the camera The possibility to observe reactions from several auditess to communication may be weaker	Interview with relevant personnel working remotely, e.g. home office, project teams in design and development; Opening closing meeting in multisite audits; Remote site/activities where physical observation is not critical; Travel time/costs reduction and associated environmental impacts; Greater geographical range
	Documentary review with auditee participation	Security and confidentiality violations; Potential difficulty in responding to documentation requests; Increased time required (potentially time-consuming process); Potential data manipulation; Interaction with auditees may be weakened Diminished quality of information collected	Document reviews where site travel is not feasible, e.g. first stage audits where site visit is not critical to the achievement of objectives and time/travel constraints exist; Multi-site - good for remote sites where site visit can be skipped or where annual visits within the audit program are not necessary, but some follow up is needed; Travel time/costs reduction and associated environmental impacts
Surveys, Applications	Filling out checklists and questionnaires	Guarantee of authenticity; Need to pre-develop checklist and possibly prepare respondent to answer them, which increases costs	Better knowledge of the organization, applicable at preparation stage of the audit; Allows to prepare audit work, which needs to be verified during the audit by gathering other evidence; Allows the organization to prepare to the onsite visit

Information and Communication Technology (ICT)	Potential Use	Risks	Opportunities
Document and data review (asynchronous) (e.g.: web document review)	Viewing records, procedures, workflows, monitors, etc.	Security and confidentiality; Procedural difficulty in document viewing (e.g. accessing remotely and navigating in the organization website); Increased time required (potentially time consuming process); Potential data manipulation; Lack of interaction with the auditees does not allow clarification of issues; Transparency - Auditee loses perception of what is being audited and the sample	Eases organization and allows for a more flexible use of time by the audit team; Allows for better, more independent from the auditee and deeper exploration of information; Possibility of integrating expertise that would not be able to travel to the site; Provides good basis for understanding the organization's QMS, and potentially provides audit trails that the auditor may utilize during interviews.
Video (synchronous) (e.g.: drone, live stream)	Monitoring of remote or high risk work; Guided site visit; Ability to view high risk processes or operations Witnessing running processes	Risks inherent in the use and presence of equipment; e.g. drone drop, use of equipment, unfavourable weather conditions; Quality of image; Full appreciation of the site, equipment and conditions Veracity of the data	Easy monitoring of high risk tasks; Increased sampling; Ideal for auditing activities where the safety requirements do not allow the presence of the audit team, or to observe places and facilities where the ratio travel time versus audit time is high; Good for complementing field visits in outdoor activities (e.g. forest and agricultural sites, mining)
Video (asynchronous) (e.g.: surveillance camera, video recordings purposely taken for audit)	Monitoring of activities that are not ongoing at the time of the audit; Process videos; Call center voice recordings. Recorded training webinars	Security and confidentiality; Quality of image; Full appreciation of the site, equipment and conditions Veracity of the data	Higher profitability (possibility of selecting only the moments of interest of the video); Possibility of observing places, hard to reach facilities and improving sampling If the electronic record contains sensitive data that CSDP criteria considers not elegible for remote auditing, the auditor should consider reassigning that record review for onsite audit.

For further information on the ISO 9001 Auditing Practices Group, please refer to the paper: Introduction to the ISO 9001 Auditing Practices Group.
Feedback from users will be used by the ISO 9001 Auditing Practices Group to determine whether additional guidance documents should be developed, or if these current ones should be revised.
Comments on the papers or presentations can be sent to the following email address: charles.corrie@bsigoup.com.
The other ISO 9001 Auditing Practices Group papers and presentations may be downloaded from the web sites:

www.iaf.nu
https://committee.iso.org/home/tc176/iso-9001-auditing-practices-group.html

Disclaimer

This paper has not been subject to an endorsement process by the International Organization for Standardization (ISO), ISO Technical Committee 176, or the International Accreditation Forum (IAF). The information contained within it is available for educational and communication purposes. The ISO 9001 Auditing Practices Group does not take responsibility for any errors, omissions or other liabilities that may arise from the provision or subsequent use of such information.