

DOWNPASS-Standard Annex 4 – Remote audit implementation template

- preliminary version -

Introduction:

Remote auditing (audits from a distance) is one of the audit methods described in ISO 19011:2018, Annex A1. The advantage of remote auditing lies in its potential to achieve audit objectives through maximum flexibility. To take advantage of this audit method, all interested parties need to be aware of their role in the process, what their input is, what the expected output is, and which risks and opportunities need to be considered in order to achieve the audit objectives.

There are a variety of reasons why an auditor may not be present for an on-site audit, for example, due to security restrictions (access restrictions), travel restrictions, pandemics, etc.

New information and communication technologies (ICT) have made remote auditing possible. As access to ICT has improved, remote auditing is becoming more common. This enables the auditor to communicate with people around the world and access a wide range of information and data.

These technologies are changing the way work is done. ICT opens up the possibility of auditing sites and people remotely, reducing distances, travel times and costs, reducing the environmental impact associated with audit travel, facilitating adaptation to customer needs, and improving the quality of products.

ICT can help increase the scope or quality of sampling in the audit process if properly prepared, validated and used. This is the case, for example, when video cameras, smartphones, tablets, drones and satellite images can be used to verify physical conditions such as production processes or forestry and agricultural areas.

The use of ICT also enables the inclusion of expertise in an audit that would otherwise not be possible due to financial or logistical constraints. For example, the participation of a technical expert for the analysis of a specific project can be scheduled for short periods of time (for example, two hours). With ICT available, the technical expert can analyze the process remotely, reducing time and costs and improving the quality of the results.

On the other hand, the limitations and risks in meeting audit objectives must also be considered when using ICT. These include questions of information security, data protection, confidentiality, and the truth and quality of the objective evidence collected.

For example, questions may arise regarding video quality, the stability of the network connection, the auditors' expertise in using ICT, the quality of the images, etc.

To make the decision to use ICT in the audit process, auditors must work with the audit team and the client to identify the risks and opportunities associated with the use of ICT and define decision criteria to approve the use of ICT for a remote audit.

General recommendations for remote audits:

- Audit program

1. *Basic considerations*

ICT may only be used for remote auditing if the right conditions are met. This means that the technology must be available and both the auditor and the auditee must be familiar with the use of the technology. If these prerequisites are not present, a remote audit may not be performed. In order to use the technology in the audit process, there must be a consistently high quality online connection. Weak bandwidth or hardware will make the process inefficient. An audit process that is already underway must be stopped if such circumstances exist and cannot be carried out until the technical requirements have been adjusted accordingly.

2. *Confidentiality, security and data protection (CSDP)*

Crucial to the use of ICT are questions of confidentiality, security and data protection. The auditor and the company to be audited must take into account the laws and regulations and possibly make additional agreements to take account of the confidentiality, security and data protection requirements. The data protection officer (DPO) on both sides should be involved in assessing these questions. To prepare for the use of ICT, both customer requirements and auditor requirements for confidentiality, security and data protection should be addressed and reviewed. ICT may only be used if all measures have been taken and both parties confirm that the confidentiality, security and data protection requirements are met, and both parties agree to the use of ICT. Evidence of this agreement shall be provided in writing and attached to the audit documentation. This evidence must also be attached to the audit report.

The audit team must be given access to both documented information and to the business premises, farms, warehouses, rearing areas, barns, etc. when conducting a remote audit. These records (documented information) should be shared in a secure system, such as a cloud or virtual private network or other file sharing system. The data must be stored securely. Auditors should not take screenshots of audited persons as audit evidence; screenshots of persons should be made unrecognisable or removed. Screenshots of documents or records or other evidence shall be kept securely for documentation purposes.

3. *Risk assessment*

The risks taken to achieve the audit objectives must be analyzed, identified and evaluated by the auditor.

- Feasibility and risk analysis for remote audits:

1. Confidentiality, security and data protection	
All parties must ensure that there is agreement between the auditor and the auditee on the questions of confidentiality, security and data protection. Precautions must be taken to ensure compliance with these criteria.	
2. Use of ICT	

There is a stable connection with good online connection quality.	
ICT enables access to relevant documented information including software, databases, records.	
It is possible to authenticate / identify the interviewees, preferably with a picture.	
If observation of facilities, processes, activities, etc. is relevant to achieving audit objectives, also review them via video.	
Changes to the process from the past (for example, application of a Corrective Action Plan) can be reviewed via video.	
3. People in the organization	
It is possible to access and question the people relevant to the quality management system.	
4. Operation	
If the company is not in regular operation due to emergency situations, the processes / activities checked by means of the remote audit are representative and allow the audit objectives to be met.	
5. Complexity of the company and the type of audit	
In case of complex company structures, processes or products and services, the auditor must carefully check whether the remote audit tool is suitable for complete evaluation of the company and its compliance with all requirements of the DOWNPASS-Standard.	
6. Conclusions	
<p>If the audit objectives can be achieved with a remote audit: → Proceed with the remote audit.</p> <p>If the audit objectives can be partially achieved with a remote audit: → A remote audit can be partially carried out and later supplemented by an on-site audit.</p> <p>If the audit objectives cannot be achieved with a remote audit: → An on-site audit must be performed instead of the remote audit.</p>	

- Criteria for assessing the quality of the remote audit:

All information needed to gain an understanding of the company, its processes and operations should be provided to the auditor in writing prior to the use of ICT so that the auditor can determine whether such an audit is appropriate to achieve the audit objectives. The auditor must be provided with all information regarding the size of the company, the operational procedures and processes. The auditor's questions must be answered. If both parties decide in favor of a remote audit and the use of ICT, the auditor must be granted remote access to the operational (production) facilities, processes and documents so that the audit objectives can be achieved. The persons to be audited must also be identified and it must be ensured that these persons are available during the remote audit. Before conducting the remote audit, it is advisable to conduct a test on the use of ICT to confirm that a stable Internet connection exists

and that the employees in the company have been briefed on what technology is used and how it is used.

- Audit planning

The auditor has the option of conducting opening and closing meetings with people at various locations via remote audit. Furthermore, he has the possibility to organize interim meetings with the audit team via telephone call, video conference or web meeting.

The review of operational processes, operating equipment and production processes must be carried out by video images in real time, or alternatively by using drones, mobile or fixed video cameras. This must be taken into account during audit planning.

- Audit implementation

When conducting the audit, an opening meeting must be held. During this meeting, the availability and feasibility of the use of ICT should be confirmed. Measures to ensure confidentiality and security should also be presented and agreed upon. If the auditor intends to take screen shots, copies of documents, and other types of recordings, permission should be requested, either at the opening meeting or when ICT is used. When using ICT to interview people, the audit team should record the name and functions of the people interviewed and inform the people interviewed what information will be retained by the auditor. When conducting interviews remotely, the auditor must verify factual assertions using other evidence. These must be requested and analyzed by the auditor. If sent by email, the auditor should ensure the necessary confidentiality for these documents.

While conducting the audit, care should be taken to ensure that communication is not disturbed by noise. When auditing remotely, the auditor should ensure that there are no interruptions or disruptions. Similarly, if there are breaks. During breaks, the sound must be muted and the image turned off to ensure privacy.

When using video to view live online images from such remote locations, it is important that the enterprise demonstrate the veracity of the images. For example, the date of a current day's newspaper can be superimposed on the transmission of live images to demonstrate that these images are actually being taken on that date. When viewing images of a (production) facility, they can also be compared to floor plans. When viewing images of a geographical location, these can be compared with available satellite images or information from geographical information systems. All evidence, as well as the manner in which evidence is preserved, must be recorded.

In a remote audit, it is important to schedule small breaks, just as they are usually scheduled in an on-site audit. The auditors and the employees of the company being audited must be given breaks.

An auditor may interrupt the audit, for example, to read current information or analyze information provided. After such a short interruption, the audit can continue. Both sides must ensure that all relevant contacts are available during the estimated audit time and that the operating sites are accessible.

- Audit report

The audit report should describe the extent to which ICT has been used and the effectiveness of its use in achieving the audit objectives. The report should identify the processes that could not be audited but must be audited on site. This is important for the decision-making process and subsequent audits. The audit team's feedback on the use of ICT must be given to the audit manager, who uses it to update the risks and opportunities previously identified. The audit program manager must decide whether the audit objectives could be achieved with the remote audit, whether follow-up work is necessary, or whether the remote audit must be supplemented by an on-site audit

- Audit validity

The validity of a remote audit is one year. A remote audit must be followed by an on-site audit.

Annex: Example of identification of Risks and Opportunities for using remote audit techniques¹

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 weakened as the auditor does not command the camera The possibility to observe reactions from several auditees 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

¹ © ISO & IAF 2020 – All rights reserved
[www.iaf.nu; https://committee.iso.org/home/tc176/iso-9001-auditing-practices-group.html](https://committee.iso.org/home/tc176/iso-9001-auditing-practices-group.html)
 Ed10n1 2020-04-16

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 eligible for remote auditing, the auditor should consider reassigning that record review for onsite audit.