Digital audits and inspections

Working Together for Safety Recommendation 046E/2021

SfS
Samarbeid for Sikkerhet

Prepared by the Working Together for Safety Working Group: **March 2021**	Version: **Rev 00**	Working Together for Safety Project Manager: Hugo Halvorsen Hugo Halvorsen (signature on file)
Applies from: **1 June 2021**		Approved by the Working Together for Safety Board, Chairman: Hedyeh Malkamy Hedyeh Malkamy (signature on file)

Contents

1. Introduction

Due to the Covid 19 pandemic, significant changes to the way we work were introduced in the spring of 2020. Among other things, this included far more digital audits and inspections than usual. This ensured that necessary audits and inspections could be carried out despite the significant limitations placed on travel and being physically present on site.

On the basis of new experience relating to conducting audits digitally, Working Together for Safety appointed a working group to collate this experience.

2. Purpose

The purpose of this recommendation is to contribute to the effective and proper execution of digital audits. At the same time, Working Together for Safety wishes to share information about the opportunities provided by digital audits and inspections, as well as their limitations.

In this context, the term ‘digital audits’ covers all digital audits, inspections and similar activities that are carried out without the auditor being physically present on site. The recommendation does not cover general audit principles or competence requirements. For this information, please see ISO 19011[1].

3. Target group

The target group for this recommendation is everyone who plans, leads or participates in digital audits.

4. Limitations and opportunities

According to ISO 19011[1], the use of digital audits should be considered when the audit programme is established. Digital audits give companies the opportunity to undertake the necessary audits and adhere to regulations when physical presence at the relevant site is not possible. Experiences with digital audits have for the most part been positive, but it is also evident that there are some associated limitations and challenges. A combination of digital and physical audits may therefore be a good practical solution going forward.

The challenges associated with digital audits may include the following:

- The planning phase takes longer, and must be completed more thoroughly and in more detail

- There is little room for unplanned changes (it is only possible to review the points that have been planned)
- Unplanned/informal communication is also lost, which usually provides added value / additional information. Non-verbal communication (body language, etc.) cannot be observed to the same extent during a digital audit
- There is an increased risk of ending up in a situation where an individual may find it difficult/demanding to answer questions because there are many participants present in the digital meeting room
- Verifications and inspections at the facility / in the field may be conducted digitally using photos and video footage, but such solutions will always have limitations compared to being physically present on site. This is especially true in instances where verifications in the field usually constitute a large part of the audit
- In a digital audit the scope of work often has to be limited if the audit will require large numbers of videos and images to be organised and submitted prior to or during the audit.

Digital audits may also offer advantages and opportunities, such as:

- Improved access to technical expertise
- Easier access to high-risk areas or those with challenging accessibility
- Opportunity to perform simultaneous audits at several locations
- More efficient use of time, especially in cases where extensive travel would usually be involved
- The opportunity to combine digital and physical solutions, e.g. digital opening and closing meetings provide the opportunity for people to participate from several physical locations in combination with physical verification

ISO 9001 Auditing Practices Group, Guidance on Remote Audits[2] offers a good overview of the limitations, risk and opportunities associated with digital audits.

5. Risk assessment

Before deciding to perform a digital audit, a risk assessment emphasising the limitations and risk this may pose to the quality of the audit should be performed. The opportunities provided by digital/external execution of the audit should also be reviewed. The result of the assessment should be used as the basis for the acceptance/non-acceptance of a digital audit as an alternative.

The risks associated with achieving the audit goals must be identified, assessed and managed. Cyber risk must be handled in the same way as other risks. The assessment shall be performed and documented for every planned audit, and involve members of the audit team and the party being audited. Any specific arrangements should be documented and communicated between the relevant parties before the audit is started.

The risk assessment should follow the same norms (categories/colours) as other risk matrices used internally within the company. Be aware that there is a risk that the individual being interviewed may obtain information/help from others during the interview (via chat, text message, email, etc.), and that photographs and video may be from other locations than those requested.

When planning visual inspections (inspection of welds, coatings, etc.) using a camera, these must always be risk-assessed and relevant measures implemented. Risks associated with the use and presence of other equipment such as drones, requirements for Ex-certified equipment, unfavourable weather conditions, image quality requirements, etc. must be thoroughly considered.

6. Planning and execution

Notice of digital audit:

Normal practice is that an audit starts with an audit notice. If the audit will be performed digitally, this should be agreed well in advance – preferably when the notice is provided. The necessary prerequisites for performing the audit, such as a hand-held camera for use during inspection rounds, must also be clarified and agreed upon.

If the audit team is not familiar with the location to be audited, it may be beneficial for them to request videos and photographs of the relevant areas/objects prior to the pre-audit meeting in order to facilitate better planning.

Digital pre-audit meeting:

- Which digital aids/devices will be used?
- How will digital security be ensured?
- How will images and video be shared? (digital solutions)?
- Who will participate, and when? (detailed agenda)
- Meeting rules for digital meetings, etc.
- Who takes ownership of the documentation after the audit?
- What shall be audited, and what documentation shall be submitted?
- Clarify roles, e.g. observer, need for meeting facilitator, etc.
- Clarify submittal of photo/film prior to the revision
- Clarify any GDPR challenges (e.g. with regard to sound recording, filming and storage of files)

The pre-audit meeting is a good opportunity for the involved parties to connect to and test the video-conferencing equipment and sharing platforms, and ensure that everything functions adequately. If this is not possible at the pre-audit meeting, it must be done before the audit is begun.

Note that videos and photographs shared temporarily on cloud solutions are not regarded as formally submitted, and it is therefore not possible to use the material in other contexts unless otherwise agreed. Nor is it possible to access and view information shared with the authorities via cloud solutions.

Review of submitted material:

- Check that all requested documentation has been received and is of good quality (especially photographs and videos)
- Ensure that you have material that covers the ‘full picture’, e.g. overview videos in addition to close-up images of an area.
- Ensure that any missing material is submitted in good time – it is often difficult to acquire this during the course of a brief digital meeting

Digital opening meeting and interviews:

- Verify that individuals with the necessary technical expertise are participating on both sides
- Verify that the digital competence is as clarified at the pre-audit meeting
- Plan breaks in the event of long interviews (remember to mute the microphone)
- Use suitable premises (without disruptive noise)
- Agree upon meeting rules, e.g. phones should be put on silent and the audit team and the person(s) being interviewed must have their cameras on
- Many digital collaboration tools have access control functions, through which it is possible to control who is able to access the meeting. This is useful in digital audits/inspections, as it gives the audit leader the ability to control who participates in the meeting. It also provides the audit team with the opportunity to take breaks / have internal discussions

Digital closing meeting:

- Ensure good participation in order to obtain all feedback on current observations
- Audit reports, etc., shall be written and handled in the same way as for physical audits
- The use of a digital audit should be documented in the final report, along with an assessment of the quality of the audit

7. Technical aspects

In order to ensure that the digital audit can be performed with good results, the following is recommended:

- Sufficient network coverage (cable or wireless) in relevant areas, so that it is possible to conduct video conferences and if possible the live sharing of photos and video footage. A portable access point can be used in areas with insufficient coverage.
- Cameras and equipment that shall be used in classified areas must have the necessary Ex-classification, and the user must have received training in the use of the equipment / operation of the camera.

- Screenshots from control systems and other relevant systems on board should be available for live streaming to remote locations. Relevant systems may be accessible at the office premises of the company being audited, or equipment can be used that enables the sharing of screenshots from the system (screen grabber). The sharing of such information must be performed on a separate network (i.e. not on the same network as the control system).
- Ensure sufficient bandwidth, so that relevant activities (e.g. filming, sharing of documents, images, etc.) may be undertaken in an effective way.
- Efforts should be made to use standard solutions such as Microsoft Teams, but the company being audited should be permitted to choose to use the organisation's own digital solutions. The solution should feature recording support.
- Digital solutions should include the possibility to use an electronic whiteboard, which makes it possible to draw and write while all participants are able to view the same board.
- Solutions for sharing and transmitting documents, photographs, film recordings, etc. must also be ensured. Such solutions may be cloud solutions such as MS Teams.
- Photographs and videos should feature timestamps. Alternatively, the request may be detailed and the film include sequences that present these details (signage, entrances, tag numbers, etc.) in such a way that it is clear that the recording was made recently and shows the relevant requested area.
- The video solution that is used must feature secure transmission, so that no third parties are able to access the material.
- When using phones / hand-held devices featuring cameras, use of an external microphone is preferable to enable several persons to participate in the conversation. Consider whether the device shall be used in a quiet or noisy environment when choosing a microphone solution.

8. Special conditions for vessels

The scope of this chapter is internal ISM and ISPS audits, other internal shipowner inspections and digital audits performed by clients or third parties aboard vessels[5-15]. The scope does not cover digital audits performed by or on behalf of public authorities. This guidance presumes that the flag state has accepted the use of digital audits for ISM and ISPS audits, and that any guidelines from the flag state for such audits are followed.

- When planning and performing digital audits aboard vessels, special consideration shall be paid to the staffing and duty rota system so that the provisions regarding rest are adhered to.
- Any time difference between the vessel and the remote inspector must also be taken into consideration.
- The crew must be given training in the tasks they shall perform and the tools they shall use in connection with digital audits.
- Tasks and operations that the crew shall perform in connection with digital audits shall be risk-assessed and the appropriate safety measures introduced.

- Instructions and procedures for digital audits shall be incorporated into the shipowner's safety management system.
- Prior to a digital audit, the shipowner must perform a risk assessment to assess whether such an audit is appropriate and possible to carry out.
- Shipowners must handle cyber risk in the same way as other risks on board.

9. References and links

1) NS-EN ISO 19011 Guidelines for auditing management systems
2) ISO 9001 Auditing Practices Group, Guidance on Remote Audits
3) IAF MD 4 Mandatory document for the use of Information and Communication Technology (ICT) for auditing/assessment purposes
4) Regulations concerning the performance of work, use of work equipment and related technical requirements FOR-2011-12-06-1357
5) Regulations regarding organisation, management and employee participation FOR-2011-12-06-1355 (Includes GDRP)
6) Act regarding the processing of personal data (Personal Data Act) LOV-2018-06-15-38
7) DNV-GL Remote surveys for fleet in service
8) DNVGL-CP-0484 – Approval of service supplier scheme: Drone surveys by DNV GL
9) STCW Regulation I/2 Certificates and endorsements
10) STCW Regulation I/14 Responsibilities of companies
11) STCW Regulation VIII/1 Watchkeeping
12) SOLAS Chapter XI Management for the safe operation of ships
13) ISM Code Chapter 6 Resources and Personnel (MSC.353(92))
14) MLC 2006 Regulation 2.4 Entitlement to leave
15) MLC 2006 Regulation 2.7 Manning levels
16) MLC 2006 Regulation 2.3 – Hours of work and hours of rest
17) ISM code Resolution MSC.428(98) Cyber Risk Management