COS-1-10

GUIDANCE FOR REMOTE AUDITS

FIRST EDITION | MAY 2023

SEMS AUDIT & CERTIFICATES

DATA COLLECTION, ANALYSIS & REPORTING

GOOD PRACTICE DEVELOPMENT

SHARING INDUSTRY KNOWLEDGE

CENTER FOR OFFSHORE SAFETY

SPECIAL NOTES

Center for Offshore Safety (COS) and American Petroleum Institute (API) publications necessarily address topics of a general nature. Local, state, and federal laws and regulations should be reviewed to address particular circumstances.

COS, API, and their respective employees, members, subcontractors, consultants, committees, or other assignees make no warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. COS, API, and their respective employees, members, subcontractors, consultants, or other assignees do not represent that use of this publication would not infringe upon privately owned rights.

COS publications may be used by anyone desiring to do so. Every effort has been made to assure the accuracy and reliability of the data contained in them; however, the COS and API make no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaim any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

COS publications are published to facilitate the broad availability of offshore safety information and good practices. These publications are not intended to obviate the need for applying sound judgment regarding when and where these publications should be utilized. The formulation and publication of COS publications is not intended in any way to inhibit anyone from using any other practices. Questions or requests for clarification regarding this document may be directed to the Center for Offshore Safety/API, 15377 Memorial Drive, Suite 250, Houston, TX 77079 and Global Industry Services Department, American Petroleum Institute, 200 Massachusetts Ave N.W., Suite 1100, Washington, DC 20001.

Questions concerning the interpretation of the content of API RP 75 or comments and questions concerning the procedures under which API Recommended Practice 75 was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 200 Massachusetts Ave N.W., Suite 1100, Washington, DC 20001.

Requests for permission to use in other published works or translate all or any part of the material published herein should be addressed to Global Industry Services Department, American Petroleum Institute, 200 Massachusetts Ave N.W., Suite 1100, Washington, DC 20001.

TABLE OF CONTENTS

1. INTRODUCTION

The Center for Offshore Safety (COS) developed guidance and suggested considerations when planning for remote auditing of a Safety and Environmental Management System (SEMS).

This guidance is provided to address considerations specific to conducting a remote audit and may be used in conjunction with other COS Guidance documents[1] and those of involved stakeholders.

The fundamental objective of a SEMS audit is to validate the establishment, implementation, and maintenance of a Company's SEMS performance driving continual improvements. Conducting an audit remotely presents both potential opportunities and challenges. The Auditor and Auditee should evaluate the overarching safety, environmental, and economic benefits and risks to achieve the audit objectives. The Auditor and Auditee should also consider the expectations of stakeholders and the effective use of resources. Remote audit activities should be planned accordingly, and any limitations should be clearly documented.

This guidance can be used for any SEMS audit where the Auditor and Auditee agree that all or part of a planned audit can be conducted remotely.

2. DEFINITIONS

- **Asset** - The equipment (individual items or integrated systems) or software used offshore.

- **Auditee** - Company being audited.

- **Auditor** - Person qualified to meet the objectives of the audit.[2]

- **Company** - An operator, contractor or partnership engaged in offshore operations.

3. ACRONYMS

- **API** - American Petroleum Institute

- **COS** - Center for Offshore Safety

- **ICT** - Information and Communication Technologies

- **SEMS** - Safety and Environmental Management Systems

[1]COS-1-06 Guidance for Developing a SEMS Audit Plan; COS-1-09 Guidance for Conducting SEMS Audits (both API RP 75 3rd and 4th editions); COS-1-01 COS SEMS II Audit Protocol- Checklist; COS-1-08 SEMS Audit Report Format and Guidance; APR RP 75 Development of a Safety and Environmental Management Program for Offshore Operations and Facilities, 3rd Edition; API RP 75 Safety and Environmental Management System for Offshore Operations and Assets, 4th edition; and COS-2-03 Requirements for Third-Party SEMS Auditing, 1st and 2nd editions; COS-3-06 Guidance for Developing and Managing Procedures.

[2]Auditors participating in audits for which the Company intends to obtain a COS SEMS Certificate must meet the requirements defined in COS-2-01 Qualification and Competence Requirements for Audit Teams and Auditors Performing Third-Party Audits of Deepwater Operations.

4. GUIDANCE

4.1 RISK ASSESSMENT WHEN DECIDING TO ADD OR MOVE TO REMOTE OPTIONS

Expectations should be communicated and agreed upon between the Auditor and the Auditee. Depending on the objectives of the audit, not all situations may be appropriate for remote auditing.

Before deciding to conduct some, or all, of a SEMS audit remotely, Auditees should evaluate the benefits and risks of remote auditing to verify they can still achieve their SEMS audit objectives. Risks can often be mitigated or eliminated through planning and preparation. There may be scenarios where the benefits do not outweigh the risks of conducting the audit virtually despite mitigations. Where it is not feasible to achieve the objectives, consider alternatives to remote auditing.

For purposes of this Guidance, "Remote Auditing" refers to gathering information when assisted by Information and Communications Technology (ICT). ICT encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. Advances in ICT are making examples like these more commonplace:

- Interviewing personnel by voice and visual systems (e.g., videoconferencing);

- Virtually exchanging or allowing access to documents from multiple locations;

- Monitoring real-time data from multiple locations; and

- Recording and/or transmitting pictures from fixed or mobile cameras (e.g., wearable technology), drones, and satellites.

Possible benefits from the use of ICT for remote auditing include:

- Enabling "access" to facilities, personnel, and/or processes by auditors:

  - not authorized to visit (e.g., high-risk area);

  - not able to visit due to scheduling, distance, cost, or persons on board (POB) limitations;

  - during times of travel restrictions.

- Enabling safe observation by trainees and other interested parties.

Auditees should consult with affected personnel to assist with identifying potential drawbacks and risks to achieving audit objectives through the use of ICT and identifying risk mitigation steps or alternative approaches. It is helpful to document the drawbacks, risks, and mitigation steps and then verify they are in place before initiating the audit. Drawbacks and risks can be organized by audit activity (e.g., interviewing, document review, observation of activities) or by grouping the information by people, equipment, and process. Examples of both approaches are contained in the following tables.

AUDIT ACTIVITY – DOCUMENT REVIEW/INTERVIEWS/INSPECTION AND INVESTIGATION

DRAWBACK OR RISK	POSSIBLE MITIGATION
Document-sharing platforms could be slower than in-person exchanges	• Consider what documentation can be supplied and reviewed in advance • Plan sufficient time for exchange and review
Document is not available remotely (e.g., not digitized or its size exceeds capability of the transfer platform)	• Consider what documentation can be supplied and reviewed in advance, and split into multiple files to accommodate limited transfer capability • Establish a backup process for access, review, and follow-up
Communication systems breakdowns or limitations	• Arrange alternative times or methods
Equipment limitations or breakdowns	• Assure access to power • Assure batteries are fully charged or proper fuel is available • Arrange alternative times or methods
All involved do not have an understanding of or are not comfortable with the communications platform	• Offer training in use of the platform • Address questions and concerns
Limitations of the camera may restrict the ability to understand activity outside the field of view	• Arrange alternative equipment with different functions (e.g., noise canceling features, tilt and zoom, greater resolution) • Consider if still photos can suffice instead of video • Stop occasionally and change the view of the camera to view the surroundings • Consider having audit team member(s) on location with additional personnel monitoring remotely
Subject Matter Experts (SME) and auditors not being physically present	• Assure two-way communication between on-site and remote personnel to address questions and redirect on-site activities • Consider having 1 or more SME and auditor(s) on location with other personnel monitoring remotely
Odors, walking surface conditions, noise levels, and vibration will not be directly observable	• Consider whether such information is necessary to achieve objectives • Consider having some audit team member(s) on location with additional personnel monitoring remotely • Utilize technology (robot) with sensors or sensory capability (e.g., accelerometer, air samplers)
Camera, robot, or drone present safety concerns to facility	• Assure intrinsically safe equipment is used in restricted areas • Arrange for audit activity to occur in a different location • Establish an agreed-upon route of access • Implement controls to allow use of the equipment
Wearable camera or other ICT presents safety concern to personnel	• Limit interviews to fixed locations and fixed cameras • Assure user has an assistant or "minder" to help them with walking, repositioning, and other situational awareness • Determine in advance whether certain areas cannot or should not be accessed • Assure controller of the robot, drone, or mobile camera has prior training and is comfortable with its use
Interviewee is uncomfortable around cameras	• Involve personnel in the discussion of use of ICT ahead of time • Consider selection of qualified interviewees • Interview personnel as part of a group • Offer training ahead of time to reduce discomfort • Coordinate camera views • Assure privacy measures are in place
Remote invterview process fatigues those involved	• Plan accordingly for breaks, understanding that remote processes can be more tedious than in-person • Limit interviews to planned subjects and postpone new ideas or audit trails for another time
Limited opportunity to foster openness through introductory conversations	• Provide an opportunity for pre-audit interaction
Limited opportunity for follow-up conversation between auditor and auditee to rationalize points, discuss potential omissions, or present documented field updates	• Plan accordingly for sufficient time and follow-up

EQUIPMENT/PROCESS/PEOPLE	
DRAWBACKS AND CONCERNS	**POSSIBLE MITIGATION**
Ability of ICT equipment to meet performance objectives	• Consider alternative ICT equipment • Consider obtaining some of the information with ICT and some in person
Logistics issues of getting equipment and people to the location when needed	• Consider alternative modes of transportation • Plan to assure equipment, power (e.g., batteries, fuel), and people arrive in time considering mode of transport, permits, and customs issues • Consider applicable regulations and transportation restrictions
Availability of qualified personnel to operate the equipment	• Consider having audit team member(s) on location with additional personnel monitoring remotely • Plan for backup or schedule alternative times when personnel are available • Provide familiarization and training in advance
Cost to purchase, maintain, and transport to locations is prohibitive	• Consider alternative equipment • Consider renting instead of purchasing • Rent from a local provider to reduce transport cost
Safety of using the equipment where desired	• Assure intrinsically safe equipment is used in restricted areas • Establish an agreed-upon route of access • Implement controls to allow use of the equipment • Arrange for audit activity to occur in a different location
Management of digital information	• Consider applicable cyber security policies and guidance regarding equipment and data • Have a pre-defined protocol for managing sensitive data • Use secure and agreed-upon technology for information transfer
Ability of ICT to handle the digital data volume	• Consider alternative or interim data storage mechanisms • Consider capacity when selecting ICT
Ability of ICT to communicate in real-time in the intended location	• Consider connectivity and bandwidth availability of the ICT in the intended location • Consider alternative equipment or delayed transfer of information • Schedule audit activities to ensure availability of bandwidth
Lack of knowledge and skills of the ICT user	• Involve personnel in the discussion of use of ICT ahead of time • Supply trained users for the ICT or provide familiarization and training • Schedule and conduct test-runs
Willingness of auditee personnel on-site to use or participate in the ICT process	• Involve personnel in the discussion of use of ICT ahead of time • Train site personnel in use of the ICT • Supply trained users for the ICT instead of training site personnel • Demonstrate function of ICT and supply awareness level training • Schedule and conduct test-runs • Coordinate camera views • Assure privacy measures are in place
Possibility that workers will be "camera shy" or act differently on camera	• Involve personnel in the discussion of use of ICT ahead of time • Consider selection of qualified interviewees • Interview personnel as part of a group • Offer training ahead of time to reduce discomfort • Coordinate camera views • Assure privacy measures are in place
Is user encumbered by the technology (e.g., able to see, hear and react, potential trip hazard)	• Assure user of the robot, drone, or mobile camera has prior training and is comfortable with its use • Limit interviews to fixed locations and fixed cameras • Assure user has an assistant or "minder" to help them with walking, repositioning, and other situational awareness • Determine in advance whether certain areas cannot or should not be accessed

EQUIPMENT/PROCESS/PEOPLE	
DRAWBACKS AND CONCERNS	**POSSIBLE MITIGATION**
Will the equipment be used in a location where other activities may distract or disrupt the intended purpose	• Determine in advance whether certain areas cannot or should not be accessed with ICT • Coordinate schedule with different activities
Consideration of meeting/camera fatigue	• Plan accordingly for breaks
Lack of communication about use of the ICT to all personnel on the asset causes confusion or concerns	• Provide advance communication of the audit plan and ICT use to all personnel and contractors who might become involved
Need for the Pre-approval of routes, viewing/recording locations, and interviewees may impact independence of the Auditor and ability to conduct random sampling	• Create a process for managing changes to the approved audit plan and use of ICT • Consider ability of Auditor to gather information in person without ICT

4.2 LEGAL AND SECURITY CONSIDERATIONS

This element describes the methods and/or components used to evaluate, and if necessary, remediate, the SEMS audits with remote audit components have similar legal and security exposure as in-person and on-site audits.   This section identifies some potential additional legal and security considerations of remote audits. Areas to consider during the audit planning process include, but are not limited to:

1.   Documentation. Documents generated as part of remote audits, including physical and digital media such as video and voice recording, need to be managed in accordance with the Company's existing document retention procedures. The use, retention, and distribution of digital media, such as video and voice recording, drone fly-over videos, and satellite imagery should be determined ahead of time.

2.   Licensing and Approval to Use Technology. Ensure appropriate user licensing and required approvals are obtained by the Company being audited and/or the Auditor. Typical technology requiring licenses and/or approvals include, but are not limited to:

   a.   Video conference and collaboration tools

   b.   Wearable hardware and its associated software

   c.   Use of drones

      i.   coordination of controlled airspace and helicopter flight paths

      ii.   drone pilot training/certification, if required

3.   Privacy and confidentiality considerations for people and processes. Remote auditing poses concerns beyond in-person auditing as recordings and images can be shared with limited context and allow for individual interpretations. Matters to be considered include but are not limited to:

   a.   Ensure non-disclosure agreements between Company and Auditors on materials are on file for remote audits, if necessary.

   b.   Ensure required permissions are obtained from those on location in advance of the on-site recording of materials and images.

   c.   Drone flight plan should be developed to cover areas to be reviewed and/or excluded.

4.3 SETTING THE AUDIT SCOPE AND OBJECTIVES

The process for developing audit scope and objectives should not differ due to the ICT aspects of a remote audit. Planners should refer to the Audit Objectives and Audit Scope sections of COS-1-06 *Guidance for Developing a SEMS Audit Plan* for additional guidance.

The scope and objectives should be communicated and agreed upon between the Auditor and the Auditee. Once the audit is underway, changes in the scope and objectives of the audit, including changes in the remote aspects, should go through an appropriate management of change process as outlined by the Auditee:

4.4 POST AUDIT CONSIDERATIONS

The audit report should include a discussion of the use of ICT during the audit. For additional guidance, auditors should refer to COS-1-08 *SEMS Audit Report Format and Guidance*. Auditors and the Auditee should conduct an after-action review to consider the application of remote techniques in the future and possible improvement opportunities.

CENTER FOR OFFSHORE SAFETY