

Draft White Paper on SEMS Audit Methodology

Introduction

BSEE requires an operator's safety and environmental management system (SEMS) be audited at least once every 3 years to evaluate compliance with the requirements of CFR 250 Subpart S which incorporates API RP 75. The first cycle of audits has been completed with variations in audit approach and audit report content. The variability may be due in part to differences in the level of detail expected by different stakeholders, interpretation of the protocols established by the Center for Offshore Safety and [the](#) experience of individual auditors. Audits varied from management system audits (system audits) to compliance audits.

System audits are intended to be a holistic assessment of the system and its elements. Compliance audits are intended to assess performance to specific requirements. This white paper proposes how these two types of audits should be used in conjunction to reduce risk and to increase confidence that the management system and its compliance programs are operating as designed and meet the requirements.

Problem Definition

Basic questions have arisen regarding a SEMS audit: what is its purpose, how it should be performed, and what should be reported to stakeholders. The results of the first cycle of BSEE SEMS audits were a 'mixed bag' according to BSEE in reference to quality and completeness. Auditor qualifications and approach are different depending on the type and scope of an audit, as well as what and how results are reported. Auditing management systems and compliance simultaneously is difficult and inefficient. Without clear definition in terms of purpose, performance and reporting of a system audit, stakeholders will not be able to consistently measure and benchmark the effectiveness of SEMS.

Solution

Audits can be divided into two main types which cover different scopes: systems driven and compliance driven. A company's management system should include both system and compliance audits within its [verification audit](#) program(s). Conducting system and compliance audits separately assures focus on a defined audit scope and allows for appropriate audit team staffing.

A system audit is an [independent](#) internal or external evaluation of the implementation, maintenance and performance of the management system. It evaluates the effectiveness of the overall system and its elements in delivering the expected [safety and environmental](#) performance. These audits seek to identify system gaps, are performance-based and are

Formatted: Space After: 0 pt

generally conducted every 3-5 years ([for SEMS audits](#), 30 CFR 250.1920 requires an audit frequency not to exceed 3 years). The audit report includes conclusions which are subjective assessments of the state of the design and implementation of the management system based on the identified conformities and deficiencies supported by observations. The audit report may also identify strengths. A system audit should focus on the following questions which address system components within each of the elements:

- What components have been established to meet or exceed the requirements?
- How are the component implemented and maintained?
- [Who is accountable and responsible? What skills and knowledge are required for those with the accountability and responsibility? Verify, through sampling, that those accountable and responsible have the identified skills and knowledge. How are accountability and responsibility for the various components and elements determined and assigned?](#)
- [How does the company review that the components are suitable, adequate and effective and act on the results?](#)

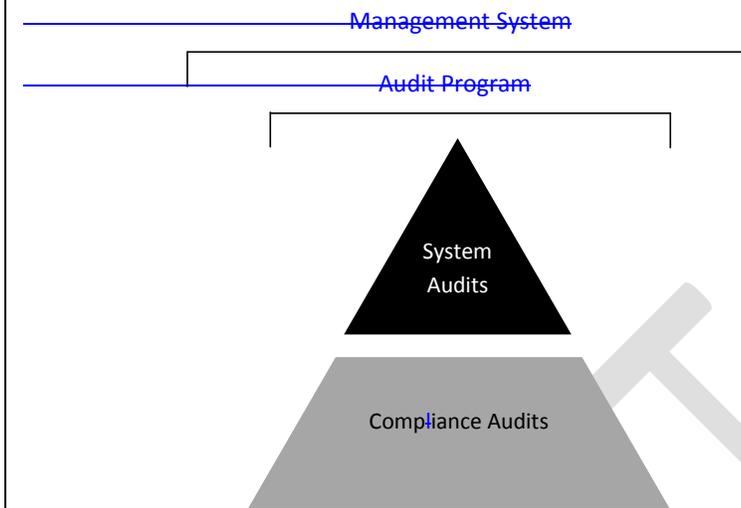
Formatted: Indent: Left: 0.25"

The results should drive changes, if needed, to the management system. A system audit should have a defined scope and should not:

- Extend beyond the defined scope,
- Be a compliance audit or inspection,
- Include criteria beyond those already set by regulations and the auditee's management system ([i.e. the requirements of 30 CFR 250, Subpart S in the case of a SEMS audit](#)),
- Limit judgment on the management system, its implementation and its effectiveness to just the knowledge and experience of the auditor.

Compliance audits [and verifications](#) should occur more frequently than system audits. Compliance audits evaluate adherence to [specific sets of](#) regulatory and/or internal requirements, and can result in [changes to the continual improvement of](#) compliance programs and the management system. The scope and results of compliance audits should be reviewed as part of the system audit and can serve as further evidence of system conformity or deficiency.

Formatted: Left, Space Before: 12 pt



Formatted: Tab stops: 0", Left

As the SEMS regulations are meant to promote the use of a holistic approach to safety and environmental management, the system audit approach is more appropriate to meet the SEMS audit requirements of 30 CFR 250.1920 and its reference to Element 12 of API RP 75.

The results of the system audit ~~should~~will include the following:

Formatted: Space After: 0 pt

- Conformities,
- Deficiencies, if applicable, which are provided as either Finding Level 1 or Finding Level 2.
- Observations which serve as evidence of both conformities and/or deficiencies
- Conclusions.

All four results – conformities, deficiencies, observations and conclusions ~~should~~will be included in the audit report. It may also include strengths ~~if agreed as agreed~~ to by the auditee.

Under the SEMS requirements, A Corrective Action Plan (CAP) is required by the auditee for each deficiency (both Finding Level 1 and Finding Level 2). The intent of the CAP and its closure is to prevent the recurrence of deficiencies.

Risk of Adopting Solution

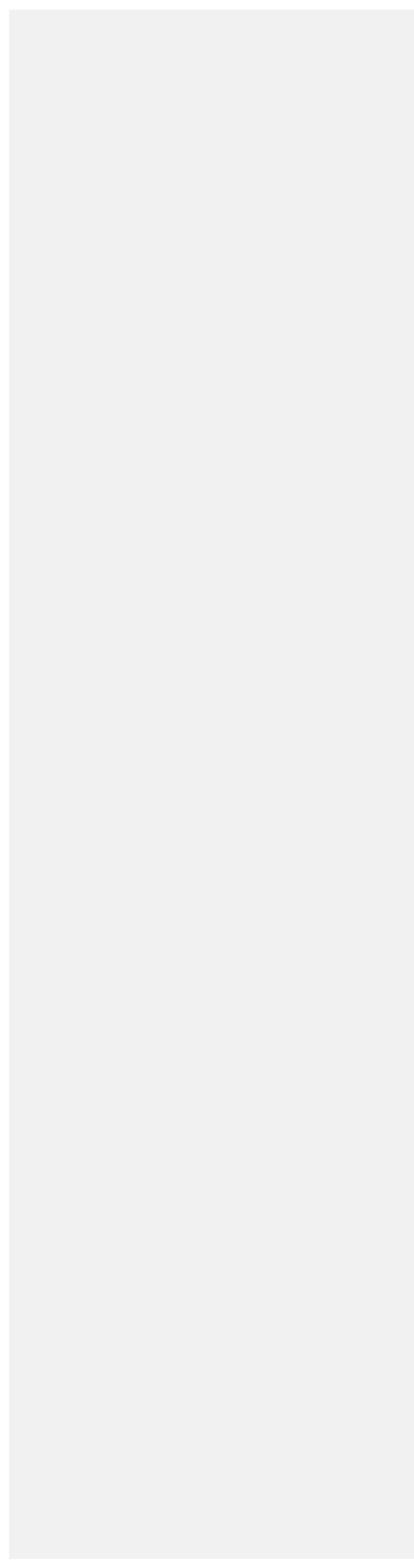
1. Will set a precedent that industry demonstrates that they have established, implemented and maintained an audit program that consists of both system and compliance audits.
2. Compliance audits become regulatory requirements.

3. Compliance audit results are required to be submitted to BSEE thus subject to Freedom of Information Act.

Call to Action

This proposal should be vetted through COS SEMS Work Groups, Single Points of Contact Committee and then presented to the COS Governing Board and API Legal. Upon approval by Governing Board and API Legal, it should be shared with BSEE to reach concurrence for future SEMS audits. If concurrence is reached, COS-2-03 will require revision and communication to industry and the Audit Service Providers.

DRAFT



Annex 1: Definitions

Compliance – act or process of meeting or exceeding regulatory and/or internal requirements.

Component – a policy, standard, practice, process, procedure or control.

Conclusion - a subjective assessment of the state of the design and implementation of the management system based on identified conformities and deficiencies.

Conformity – meets or exceeds the management system element and/or its components.

Corrective Action Plan – a scheduled plan to correct deficiencies identified in a systems audit. A corrective action plan includes the name and job title of the personnel responsible for correcting identified deficiencies, as well as the date on which the corrective action is expected to be closed.

Deficiency – either a Finding Level 1 or Finding Level 2.

Finding Level 1 – the design or implementation of an entire management system element or a significant component within the element is not conforming with requirements. The maximum number of Findings Level 1 on a single SEMS audit cannot exceed the number of SEMS elements, one for each element.

Finding Level 2 – a component within the management system element is not conforming with requirements [that is indicative of a systemic issue](#). There may be multiple Finding Level 2's within a single management system element.

Observation – evidence that supports a conformity or a deficiency.

Results - conformities, deficiencies, observations, and conclusions.

Strength – a component that has been identified by the ASP as exceeding SEMS requirements or recommended practice which could benefit industry by being shared.

Annex 2: Examples of the differences between a System and Compliance/Conformance Audit

System Audit Questions	Compliance Audit Questions
Is there an inspection program in place, is it being implemented and is it effective?	Was a particular inspection completed?
Is there a testing program in place, is it implemented and is it effective?	Was a particular valve tested?
Is there a PPE program in place, is it being	Is a particular individual wearing the proper

implemented and is it effective?	PPE?
Is there a program for air monitoring, is it being implemented and is it effective?	Was air monitoring being performed every hour?
Is there a JSA process in place, is it being implemented and is it effective?	Has this JSA been authorized by the ultimate work authority?

System Audit Report Deficiency	Compliance Audit Report Deficiency
Mechanical integrity element not fully implemented as evidenced by 25% of sampled tests were not being performed as required.	A list of specific tests not performed.
Training element not fully implemented as evidenced by: <ul style="list-style-type: none"> • 20% of sampled individual training records indicated not all training was completed as required • 20% of annual training requirements were not provided within 12 months of the last training and were not completed as required by schedule. • The majority of interviewed employees were not following operating procedures. 	List of specific training that was missed by each individual.
Incident Investigation element not fully implemented as evidenced by: <ul style="list-style-type: none"> • 25% of incidents requiring investigation per procedure were not investigated • 20% of incident investigation actions were past due 	List of specific incident investigation actions overdue.