



2.4 Analyse How the System Supports Legal Compliance, Governance and Continual Improvement





Learning Outcome

By the end of this session, learners should be able to analyse how an Occupational Health and Safety Management System (OH&SMS) supports legal compliance, governance, and continual improvement. Learners will examine legal compliance processes, audit and assurance mechanisms, management review, and corrective action frameworks that strengthen organisational performance.





Learning Objectives

After completing this topic, learners will be able to:

- Analyse how legal requirements are integrated into an OH&SMS.
- Evaluate audit trails and compliance assurance mechanisms.
- Explain the purpose of management reviews.
- Assess the role of corrective and preventive actions in continual improvement.



Introduction

An Occupational Health and Safety Management System (OH&SMS) is not simply a collection of policies and procedures; it is a governance framework that helps organisations demonstrate legal compliance, monitor performance, and continually improve their occupational health and safety performance. ISO 45001 promotes a proactive approach by integrating legal obligations into everyday business activities, ensuring organisations not only comply with legislation but also strengthen governance, accountability, and organisational resilience.



1. Mapping Legal Requirements to System Controls

One of the primary objectives of an OH&SMS is to ensure that legal and other compliance obligations are systematically identified, implemented, monitored, and reviewed.

Legal Compliance Process

A typical process includes:

01

Identify applicable legislation.

03

Determine organisational obligations.

05

Implement operational controls.

07

Review legislative changes.

02

Maintain a legal register.

04

Develop policies and procedures.

06

Monitor compliance.

08

Take corrective action where necessary.

Mapping Legal Requirements

Legal requirements should be linked directly to organisational controls.

Legal Requirement	System Control
Risk assessment requirements	Formal risk assessment procedures
Training obligations	Competency and training programmes
Emergency planning	Emergency response procedures
PPE requirements	PPE policy and inspection programme
Incident reporting	Incident reporting and investigation procedure

This ensures legal obligations are translated into practical workplace activities.

2. Audit Trails and Compliance Assurance

What is an Audit Trail?

An audit trail is documented evidence showing that organisational processes have been followed and legal obligations have been met.

Examples include:

Risk assessments.

Inspection records.

Training records.

Maintenance logs.

Incident investigations.

Internal audit reports.

Management review minutes.

Audit trails demonstrate due diligence and provide evidence during regulatory inspections or certification audits.

Compliance Assurance

Assurance provides confidence that the management system is functioning effectively.

Common assurance activities include:



Internal audits.



External audits.



Workplace inspections.



Compliance evaluations.



Performance monitoring.



Regulatory inspections.

These activities identify weaknesses and support continual improvement.

3. Management Review Processes

Management review is a formal evaluation of the effectiveness of the OH&SMS by top management.

According to ISO 45001, reviews should consider:

Audit results.

Incident trends.

Achievement of objectives.

Legal compliance.

Worker feedback.

Resource needs.

Emerging risks.

Opportunities for
improvement.

Why Management Reviews are Important

They help organisations to:

- ☐ Evaluate system performance.
- ☐ Ensure continued suitability.
- ☐ Allocate resources.
- ☐ Support strategic decision-making.
- ☐ Demonstrate leadership commitment.
- ☐ Drive continual improvement.

Management reviews should result in clear actions, responsibilities, and timescales.



4. Corrective and Preventive Action Frameworks

Continual improvement depends on learning from incidents, audits, inspections, and performance data.

Corrective Action

Corrective action addresses the cause of an identified non-conformity to prevent it from happening again.

Examples include:

Revising procedures.

Improving training.

Replacing defective equipment.

Strengthening supervision.

Preventive Action

Although ISO 45001 does not include a separate preventive action clause (because prevention is embedded throughout the standard through risk-based thinking), organisations should still implement proactive measures to prevent potential non-conformities.

Examples include:



Regular inspections.



Hazard reporting.



Behavioural safety observations.



Predictive maintenance.



Health surveillance.

Continual Improvement Cycle

Continual improvement involves:



This cycle ensures that the OH&SMS evolves with changing organisational needs.

International Standards Supporting Compliance and Improvement

Several international standards support governance and continual improvement:

ISO 45001:2018

Occupational Health and Safety Management Systems.

ISO 19011:2018

Guidelines for Auditing Management Systems.

ISO 31000:2018

Risk Management.

ISO 37301:2021

Compliance Management Systems.

ISO 9001:2015

Continual Improvement and Performance Evaluation.

Practical Case Study

Scenario

An engineering company experiences repeated near misses involving forklift operations.

The organisation:

- Reviews legal requirements relating to workplace transport.
- Conducts an internal audit.
- Identifies weaknesses in traffic management.
- Updates risk assessments.
- Introduces new pedestrian walkways and speed limits.
- Retrains forklift operators.
- Reviews performance during the next management review.

✓ Outcome: Near misses reduce significantly, compliance improves, and the organisation demonstrates continual improvement through its OH&SMS.



Critical Evaluation

An effective OH&SMS supports much more than legal compliance. It establishes governance processes that enable organisations to monitor performance, demonstrate accountability, and drive continual improvement. Audit trails, management reviews, compliance evaluations, and corrective actions provide objective evidence that the system is functioning effectively.

However, organisations should avoid treating audits and documentation as administrative exercises. The true value of an OH&SMS lies in using performance information to make informed decisions, improve controls, and strengthen organisational resilience.

Continual improvement therefore depends not only on system design but also on leadership commitment, worker participation, and a culture of learning.

Summary Table

OH&SMS Element	Contribution
Legal Compliance Mapping	Ensures legal obligations are translated into operational controls
Audit Trails	Provide objective evidence of compliance and due diligence
Compliance Assurance	Verifies the effectiveness of the management system
Management Review	Supports strategic oversight and resource allocation
Corrective Actions	Eliminate the causes of non-conformities
Preventive Measures	Reduce the likelihood of future incidents through proactive risk management
Continual Improvement	Enhances organisational performance over time

Reflective Questions

1

Why should legal requirements be mapped directly to organisational controls?

2

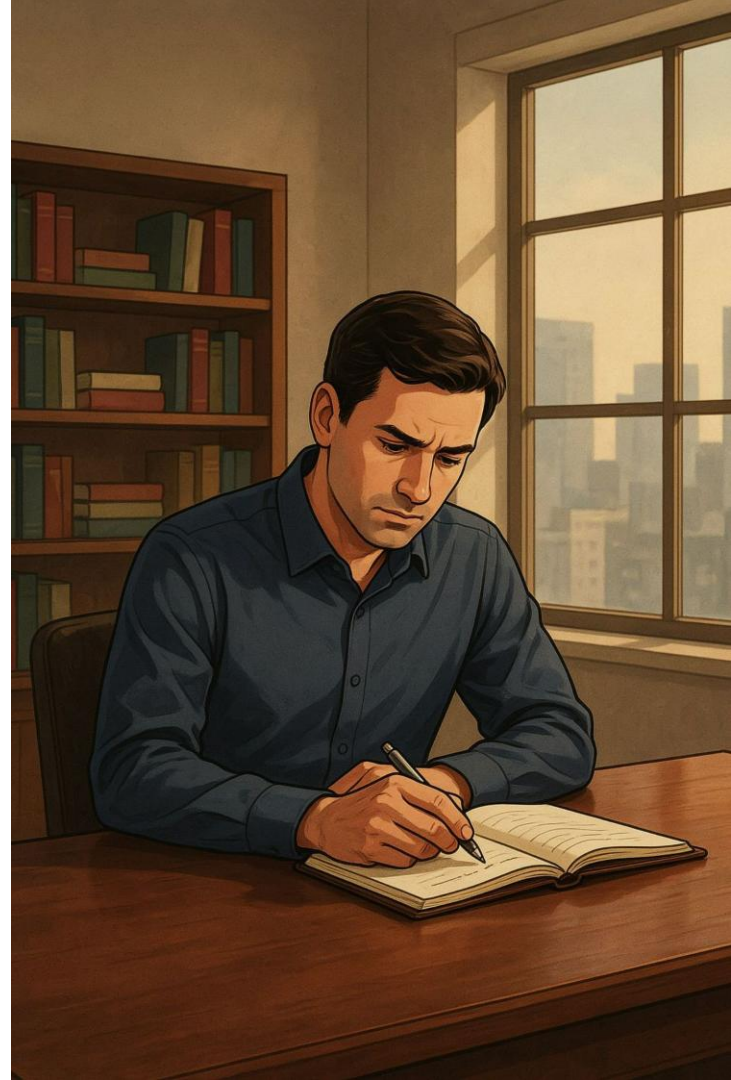
How do audit trails support regulatory inspections and certification audits?

3

What is the purpose of a management review within an OH&SMS?

4

Why is continual improvement considered a fundamental principle of ISO 45001?



Key Takeaways

- An Occupational Health and Safety Management System (OH&SMS) supports legal compliance by systematically identifying, implementing, and monitoring legal obligations.
- Legal requirements should be translated into practical controls through policies, procedures, training, inspections, and operational processes.
- Audit trails and compliance assurance activities provide objective evidence that the management system is effective and legally compliant.
- Management reviews enable top management to evaluate system performance, allocate resources, and support strategic decision-making.
- Corrective actions address the root causes of non-conformities, while risk-based thinking promotes proactive prevention and continual improvement.
- International standards such as ISO 45001, ISO 19011, ISO 31000, ISO 37301, and ISO 9001 strengthen governance, legal compliance, and organisational resilience through structured management system processes.