MANAGING LEGAL COMPLIANCE AS A PART OF ISO 14001 AND ISO 45001

Authors:

Tjeerd Hendel-Blackford, *Head of Thought Leadership*

Elise Saade, *EHS Regulatory Analyst at Enhesa*

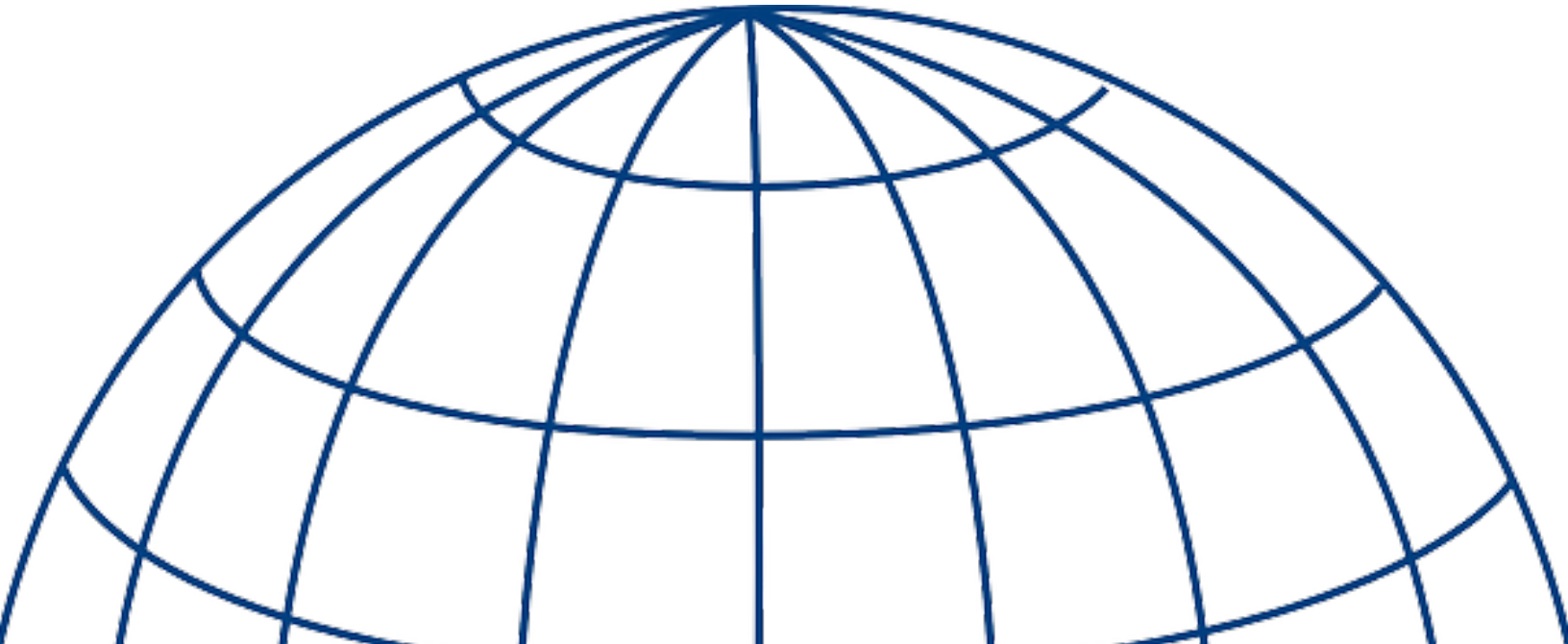

TABLE OF CONTENTS

1 Introduction

2 Back to Basics —ISO EHS Management System Standards

- Statistics
- Recent Changes

3 Ask Yourself

3 What Do The Standards Say?

- Are There Any Differences?
- Relevant Provisions
- Practical Implications

5 Challenges

- Non-Standardized Tools
- Regulatory Complexity
- Compliance Metrics and Risk Determination
- Different Perspectives

7 Conclusion: Best Practice Solution

INTRODUCTION

It will come as no surprise to you that many companies manage their **environmental, health and safety (**EHS) risks through the application of some form of Management System.

When we survey EHS professionals about the management system they have in place, all of their systems require they manage legal compliance.

Your company will need to manage how it complies with EHS laws and regulations. But are you currently doing it in the best way? In our experience, there are a number of misconceptions around what the standards require; as a result,many poor practices have been allowed to permeate. From what we hear from our clients, there is often an inconsistent application by system auditors of what standards require.

With that in mind, let's go back to basics on the ISO Standards we are looking at today.

BACK TO BASICS – ISO EHS MANAGEMENT SYSTEM STANDARDS

Statistics

As of 2016, approximately 346,000 ISO 14001 certificates were held around the world. This represented an increase of **8 percent increase** from the 2015 figures.

The geographical distribution of the certifications provides an interesting insight :

- Companies in East Asia held over half of all certificates. Chinese and Japanese companies with around 137,000 and 27,000 certificates respectively make up the vast majority of these.
- Europe has approximately 120,000 certificates, with strong numbers across most individual countries.
- There are only 8,438 certificates across North America--with approximately 5,500 of the certificates being in the United States. This most likely stems from the different historical, cultural and legal approaches to managing EHS.

It is too early to have any statistics in regards to ISO 45001. However, concerning OHSAS 18001 (the ISO 45001 predecessor, which will be phased out come March 2021), it is estimated that 80,000 companies across 127 countries are certified. It is likely that the geographic distribution of these will resemble that of ISO 14001.

Recent Changes

ISO management standards are designed to be similar in structure to allow for easier integration of the systems. The most recent version of ISO 14001 was adopted in 2015. ISO 45001 was adopted in March 2018.

Both ISO 14001:2015 and ISO 45001 follow the High-level structure now adopted by ISO across all standards. In overall terms, the main changes to both standards are as follows:

- The new structure puts more emphasis on the need to consider the Organizational context (as well as external impacts). In terms of internal impacts, companies need to take working conditions as well as the perceptions and values of workers into consideration.
- Strengthened provisions around communication and awareness have also been introduced.
- There is increased emphasis on the need for strong leadership in the form of Top Management. Top management is required to demonstrate an understanding of the company's strengths and weaknesses to how these could impact their ability to deliver on goals and commitments. This will also mean that management will need to be closely engaged with the process of "management review."

- An emphasis on the use of performance indicators will allow for the increased use of data analytics to measure the key aspects for the EHS management system.
- The term "documented information" was introduced given the technology-driven industry, moving away from the more paper-focused word "documents."

These changes are important when we discuss the provisions regarding legal compliance.

ASK YOURSELF

Consider:

1) What are the requirements in ISO 14001 and 45001 regarding legal compliance?

Whenever we ask EHS-professionals this question we typically get a variety of answers. One of the most common responses is: *"You need a legal register!"*

Which leads us onto a second question:

2) How many times does the phrase "legal register" appear in the standards?

You guessed it: Not once! The term "legal register" does not appear in either standard. This often comes as a surprise to people, even those who have been practitioners for a number of years.

WHAT DO THE STANDARDS SAY?

Are There Any Differences?

First, let's consider whether there are fundamental differences between how the standards deal with legal compliance.

The terminology in how each standard defines "legal requirements" is slightly different. ISO 14001 in fact refers to "***compliance obligations,***" whereas ISO 45001 discusses "***legal requirements and other requirements***". This difference is superficial.

In addition, due to the uniform structure, the fundamental provisions are similar. For example, the stated aims and scope of both standards refer to the fulfilment of compliance obligations (or legal and other requirements – we will use the terms interchangeably) and both standards reference the need to have processes for managing that compliance.

Both standards essentially provide the same requirements.

Relevant Provisions

The standards do not specifically require that companies comply, and as we already pointed out, there is no reference to a legal register.

However, we can find references to the words “process” and “compliance evaluation” in Sections 6.1.3 and 9.1.2, respectively, in both standards.

Under Section 6.1.3, “*Compliance Obligations,*” companies are required to establish, implement and maintain a process to determine and have access to the applicable compliance obligations. This means that companies need to have a process in place to determine which laws apply to them, have access to those laws and stay up to date with those laws. This is most likely where the concept of legal registers evolved from —and it has since become a *de facto* term.

Section 9.1.2 of both standards relates to the “*Evaluation of Compliance.*” Under this section, companies are required to establish, implement and maintain a process to evaluate compliance. This takes us back to the concept of “process.” Meaning that in order to be compliant, companies need to have a compliance evaluation process and carry it out periodically.

How often does a compliance evaluation need to be undertaken? This will depend on the nature of the organization in question and the risks it faces.

One of the most important requirements in the standards is contained in section Cof 9.1.2. This refers to the need to **maintain knowledge and understanding of compliance status**.

This is a large difference from the provisions of OHSAS 18001; it now implies an ongoing process—not just an annual exercise .

Compliance evaluation is also backed up by Section 9.3. The section requires top management to review the overall management system periodically, with a particular consideration to compliance obligations and conformity with them.

Practical Implications

What do companies need to do to meet these requirements?

1. Have process to determine which laws and their specific requirements apply to you and keep up to date.

2 Have a process to evaluate compliance and maintain knowledge and understanding of your compliance status.

What Do The Standards Say?: Practical Implications

Ask yourself:

- Am I aware of my compliance status across my company sites, globally, today?
- Do I have clear knowledge and understanding of that status?
- Will I have the same vision and clarity a week—or a month—from now?

This is perhaps easier said than done; in our experience, many companies are far from achieving this. There are a number of challenges to overcome to meet the needs of the ISO standards.

CHALLENGES

Non-Standardized Tools

Are the tools you use across your organization to manage compliance with EHS laws all in the same format?

If your sites have legal registers, are those practically useful? Are they just a list of laws with a brief summary of what each law requires? Are the legal registers up-to-date? Do your legal registers break down each requirement within each law to enable you to evaluate compliance? Are the legal registers updated on an ongoing basis?

Clearly, what qualifies as a legal register can vary widely and greatly. We have seen them in hard copy in dusty lever arch files. We often still see them in Excel files, with only the briefest summary of what the law actually requires. These are not fit for purpose.

Regulatory Complexity

Each country's laws and requirements will vary in terms of language, complexity, structure etc. Each of your sites will be doing different things—what regulations apply to each site may differ. Legal language is also often dense and can be impenetrable to those without legal training.

What's more, if you don't have a consistent and reliable approach to determine which laws are applicable to your company (and evaluate compliance with them) it makes it even harder to have a view on your compliance status at any one time, and for top management to have insight on that.

Compliance Metrics and Risk Determination

Companies will often have a myriad of different solutions to comply with EHS laws. At site level, they will have a legal register—often in the local language. The Corporate EHS department or EHS auditors may then have another service on top of that.

Challenges: Compliance Metrics and Risk Determination

Another challenge we often see is companies having a myriad of different solutions; companies risk spending money on essentially the same things, more than once. If your sites are not using a standard format for their legal registers, compliance self-assessments or external audits, how reliable and effective will the collected compliance data be? How can you identify which sites pose the greatest compliance risk? How can you monitor and evaluate improvement in compliance status?

What you need to do, or what your legal compliance process needs to, will depend on your role and perspective.

Different Perspectives

If you are at site level, you are the first level of responsibility for being compliant with applicable laws. You will need to have a clear understanding of which laws apply to your specific location and the operations you carry out there. Naturally, this will be in your own local language.

You will also need to be aware of changes in law as they occur— and how change in process or introduction of a new piece of equipment might impact the legal requirements that apply to your site.

It is at the site level that we typically see the maintenance of a legal register.

Site level staff must be aware of their legal obligations; they will be the first people to assess whether or not they are doing enough to comply. Their compliance status will then be periodically evaluated—usually by 2nd or 3rd party auditors.

The perspective at the corporate level is very different, but crucial, within the context of ISO 45001 and 14001. Corporate EHS staff need to have an overview of performance; the buck will ultimately stop with them and they have an overall responsibility to ensure their company is as compliant as possible. However, they will not have the local regulatory knowledge. In many countries, they will not even be able to read the laws as they will be in another language. However, corporate, regional or business unit teams will need to audit or verify the accuracy of site self-assessments. Corporate EHS staff also have a wider responsibility to look at how regulatory developments might impact their business across various countries or jurisdictions. This might present opportunities, as well as risks, for the company.

The processes, methods and tools you put in place to meet the ISO requirements need to take these different perspectives into account.

CONCLUSION: BEST PRACTICE SOLUTION

Best practice for meeting the aforementioned challenges is to adopt an *O*ngoing Compliance Management approach globally across your organization, enabling you (and your Top Management) to maintain knowledge and understanding of your compliance status.

This involves the implementation a system that allows:

- The determination of applicable laws and requirements, at the site/facility level
- The carrying out of compliance self-assessments at site level
- The verification of compliance by external or internal auditors
- A Corporate view on compliance status and performance
- Notification of regulatory changes on a rolling-basis
- All within one centrally accessible, standardized solution

This approach brings many benefits. One of the key benefits is that the global aspect fosters a corporate-wide strategy and approach to managing EHS and seeks to embed those values deep into the culture of the organization—across all locations. Which is also one of the key aims of the ISO Management Systems.