

	IAF Technical Committee	Issue 1
	White paper	2004-09-15
	The relationship between ISO 14001 management system conformity assessments and Regulatory Compliance	Page 1 of 6

Introduction

Since the publication of ISO 14001 in 1996, there have been many examples of organizations improving their level of regulatory compliance as a result of the structure and discipline of an environmental management system (EMS) conforming to the standard. Governmental agencies have also recognized the potential contribution of EMS implementation in some cases by either directly requiring implementation as part of regulatory compliance, offering relaxation of governmental oversight where an EMS is in place or otherwise encouraging their use.

Unfortunately, there has also arisen an expectation that certification of an organization's EMS as meeting ISO-14001 implies that the organization is in full compliance with all legal and regulatory requirements. This has led to concern and disillusionment when some organizations with certified EMSs have experienced environmental incidents or have otherwise been found to be out of legal compliance.

This paper does not seek to develop interpretations of the requirements of ISO-14001 but identifies the requirements of the standard that directly relate to regulatory compliance and explores what a certification assessment should cover in order to support a set of reasonable expectations by stakeholders.

For the purposes of this paper, the term "EMS" will be used to represent an environmental management system conforming to the requirements of ISO-14001 and "regulatory requirements" will indicate all legal and regulatory requirements related to an organization's environmental aspects and impacts. Clause references in this paper refer to ISO/FDIS-14001:2004.

Deliberate non-compliance (e.g. an organization decides to pay a fine and continue to operate without seeking to address non-compliance) should be considered a serious failure to support the policy commitment to regulatory compliance and should preclude certification or cause an existing ISO 14001 certificate to be suspended, or withdrawn.


Any organization failing to demonstrate their commitment to legal compliance through the elements discussed below should not be certified as meeting the requirements of ISO 14001 by the CRB.

The requirements of ISO-14001 with respect to regulatory compliance:

ISO-14001 requires that an organization "commit" to compliance with all legal and regulatory requirements applicable to its environmental aspects and impacts. It further requires that the organization supports this commitment by identifying applicable regulatory requirements, determining how these requirements relate to its activities, products and services, evaluate conformity with the identified requirements and take action to correct any nonconformities that exist or occur. The standard also requires that this commitment and the related supporting activities are maintained on an on-going basis.

The specific clauses of ISO-14001 most important with respect to regulatory compliance are the following:

- public commitment to legal compliance (subclause 4.2);
- full detailed identification of legal requirements (subclause 4.3.2);
- how those legal requirements apply to the organization's environmental aspects (4.3.2, 4.4.6, 4.5.1);
- objectives/targets/programs (subclause 4.3.3)
- comprehensive evaluation of legal compliance (subclause 4.5.2);
- corrective and preventative actions where necessary (subclause 4.5.3); and
- management review (subclause 4.6).

	IAF Technical Committee	Issue 1
	White paper	2004-09-15
	The relationship between ISO 14001 management system conformity assessments and Regulatory Compliance	Page 2 of 6

How should a certification body evaluate a management system with respect to legal compliance before granting certification and during the maintenance of certification?

Through the certification assessment process, a Certification Body (CRB) should evaluate an organization's conformance with the requirements of ISO-14001 as they relate to regulatory compliance and should not grant certification until conformance can be determined. The CRB should also, through an appropriate follow up program, assure that conformance is maintained during the certification period. The CRB auditors should evaluate the management of compliance based on demonstrated implementation of the system and not rely only on planned or expected results.

The following discussion identifies what should reasonably be expected on the part of the certification body in evaluating the management system with respect to regulatory compliance.

A public commitment to legal compliance (subclause 4.2):

The CRB should determine if the following specific points are demonstrated with regard to the organization's environmental policy statement:

- that there is a policy;
- that it addresses 4.2 of ISO 14001;
- that it is approved by top management;
- that it is publicly available; and
- that it is subject to periodic review of its relevance and appropriateness.

Identification of, and access to, legal requirements (subclause 4.3.2):

The CRB should determine whether the EMS has adequately identified and provides access to the specific applicable legal requirements, in sufficient detail to facilitate development and control of the management system and to enable a satisfactory evaluation of compliance. The CRB should also verify that these regulatory requirements are periodically reviewed in order to identify new and/or changed requirements and to accommodate any changes to the organization, its activities or products.

The CRB should check the completeness and relevance of identified legal requirements but the CRB is not responsible for verifying the identified legal requirements as being the final or definitive list. CRB assessment teams should have sufficient knowledge of the applicable legal requirements that are relevant for the location and environmental aspects of the organization so as to identify significant omissions from their client's identified legal requirements.

How legal requirements apply to the organization's environmental aspects (4.3.2):

The CRB should determine whether the organization understands how each legal requirement applies to its activities, products and services, and that the organization has considered this in establishing and maintaining the management system.

Determination by the CRB that the organization has sufficiently translated legal requirements into suitable EMS elements may come from an onsite walk-around, and by taking examples of significant aspects and following the trail back through the EMS to specific legal requirements. Then in the reverse order, by taking specific legal requirements and assessing how they are actually fulfilled within the normal operation.

The status of compliance may be determined from a number of sources, including reports of specific instances of non-compliance and the items in 4.6 of ISO FDIS 14001 (i.e. results of internal audits, communications including complaints, environmental performance (e.g. results of monitoring and measurement), objectives and targets, corrective and preventative actions, follow up from previous

	IAF Technical Committee	Issue 1
	White paper	2004-09-15
	The relationship between ISO 14001 management system conformity assessments and Regulatory Compliance	Page 3 of 6

reviews, changing circumstances and requirements (including legal requirements), and recommendations for improvement).

Objectives/targets/programmes (subclause 4.3.3):

The CRB should determine whether objectives and targets set within the EMS take into account legal requirements and that specific objectives and targets have been established as necessary to address any lack of compliance.

Where a significant non-compliance with regulatory requirements occurs, objectives, targets and programmes would normally be the appropriate way to resolve the non-compliances in a controlled and/or managed way.

In any case where the organization is not in full compliance with regulatory requirements (excluding minor, transitory deviations), in order to be considered in conformance with the standard, the objective of achieving compliance supported by appropriate targets and programs should have been established.

Comprehensive evaluation of legal compliance (subclause 4.5.2):

CRB assessors assess conformance of an EMS to the requirements of a standard. They do not make a comprehensive evaluation of compliance, like a regulatory auditor, to determine the organization's compliance with regulatory requirements.

The CRB should determine whether the organization has established the necessary procedures and has fully evaluated its compliance with each of the applicable regulatory requirements. Part of this determination should consider that persons performing the compliance evaluation have appropriate knowledge of the legal requirements and their application.

The CRB should test the effectiveness of the evaluation through:

- sampling the organization's determination of compliance with examples of specific legal requirements;
- looking for evidence of compliance or non-compliance during other assessment activities (on-site assessments and audit of operational controls, etc.); and
- checking that the organization's evaluation of compliance has covered all of the identified legal requirements.

In some cases, compliance audit information is considered confidential or privileged. However, sufficient data on an organization's compliance with relevant legislation and regulations, gathered during the assessment process, are relevant and necessary to determine whether the organization's systems conform to the standard. "Affirmative statements" from the organization that it is in legal compliance are not sufficient for the purposes of certification.

In the event that certain specific data or other information related to legal or regulatory compliance are not made available to the CRB for review because of an assertion of legal privilege or their proprietary nature, certification should not be granted, or should not continue, unless the CRB can obtain demonstration by objective evidence that the full system requirements relating to legal compliance, covering the applicable section of the standard, have been effectively implemented by sufficiently documented and verifiable means. This would include at least a documented procedure for evaluating legal compliance, objective evidence of its implementation, objective evidence of compliance review by management and objective evidence of implementation of identified corrective and preventive actions.

Corrective and preventative actions where necessary (subclause 4.5.3):

	IAF Technical Committee	Issue 1
	White paper	2004-09-15
	The relationship between ISO 14001 management system conformity assessments and Regulatory Compliance	Page 4 of 6

The CRB should determine that the organization has developed an appropriate corrective action procedure(s) and that regulatory non-compliances find expression in the corrective and preventative actions within the EMS. In the absence of such a connection, the CRB should be concerned about the overall effectiveness of the EMS, and its ability to support the organization's environmental policy, objectives and targets.

If a non-compliance situation is more than a minor temporary deviation, then objectives, targets and programmes may have been established. In any case the EMS should demonstrate the ability to resolve non-compliances in a controlled and/or managed way.

Management review (subclause 4.6):

The CRB should determine whether the organization has included in management reviews the status of legal compliance. This is to ensure top management are aware of the risks of potential or actual noncompliance and have taken appropriate steps to meet the organizations commitment to legal compliance.

Conclusions

ISO 14001 Environmental Management System certification is a tool for the dynamic management and improvement of an organization's environmental performance. It is not a substitute for legal requirements, or legal determinations by a regulator or a court on matters on legal compliance. EMS auditors assess an organizations EMS pursuant the requirements of the standard, they do not provide an evaluation of legal compliance nor are they regulatory inspectors.

Certification of an organization's EMS indicates conformity with the requirements of the ISO-14001. This includes a demonstrated *commitment* to compliance with applicable legal requirements.

ISO 14001 certification cannot guarantee legal compliance but neither can any certification or regulatory scheme guarantee ongoing legal compliance;

ISO 14001 requires a public commitment to comply with legal requirements. It does not require actual compliance with the law as a pre-requisite to certification, or for maintaining certification;

ISO 14001 certification confirms that there is an effective environmental management system that provides an ongoing foundation and support for an organization's legal compliance.

In order to maintain stakeholder confidence in the above attributes of a certified management system, the certification body must assure that the system *demonstrates effectiveness* before granting or continuing certification.

The EMS can act as a dialogue tool between regulators and organizations, and become the basis for a trusting partnership, replacing historical adversarial 'them and us' situations. Regulators and the public want to trust organizations with a certified EMS, perceiving them as being able to constantly and consistently manage their legal compliance. An organization with an EMS certified to ISO-14001 should have the following attributes that would be on interest to regulators, the public and other stakeholders:

- a better knowledge of legal requirements;
- a better and broader knowledge and understanding of their environmental impacts;
- more consistent awareness, training and competence of personnel;
- better use and implementation of this knowledge in its processes;
- availability and consistency of information related to environmental performance;



- management of the risk of legal non-compliance;
- management of the risk to the wider environment;
- the use of structured and systematic corrective and preventive actions;
- more rapid improvement than would be achieved by focusing on legal compliance alone;
- ongoing independent assessment of their management of legal compliance;
- both internal and external methods of assessment and verification of their commitment to legal compliance that provides top management confidence;
- coverage of a wider range of issues than those addressed in specific legal requirements; and
- confidence in the management system to then allow for focus on actual environmental performance.

Additional considerations

Auditor capabilities:

CRB auditors, in addition to basic auditor skills, should have appropriate competence in environmental issues including:

- environmental science;
- environmental management principles;
- environmental management tools;
- environmental laws and regulations
- environmental aspects of operations

Certainly, an auditor, in order to evaluate and EMS does not need to be an environmental scientist or be an expert in the specific industry or product or have detailed knowledge of every conceivable regulatory requirement. However, the levels of knowledge, education, training or experience in these areas should enable the auditor to:

- understand the environmental aspects and impacts of the candidate organization;
- understand how the management system is implemented to control these aspects and impacts and achieve its objectives;
- understand in general terms the applicable regulatory requirements;
- determine whether the EMS is effective in controlling its aspects and impacts

A one-week EMS lead auditor course will not be sufficient to impart this level of knowledge and understanding for someone without any prior environmental exposure. EMS auditor candidates should have some relevant experience in these areas before hire and the EMS lead auditor course should be a means to focus their knowledge toward the audit process.

When and auditor suspects a regulatory non-compliance:

Management system auditors should not perform *regulatory compliance* audits as part of ISO 14001 audits. Where auditors find suspected regulatory noncompliance issues, they should immediately notify the organization's Management Representative.

Suspected regulatory noncompliance issues should be reviewed by the auditors to determine whether the EMS has appropriately identified and addressed them. Specifically:

	IAF Technical Committee	Issue 1
	White paper	2004-09-15
	The relationship between ISO 14001 management system conformity assessments and Regulatory Compliance	Page 6 of 6

- Is the organization aware of the condition?
- Has the organization determined whether the condition represents a regulatory compliance issue?
- Has appropriate corrective action been taken to immediately address the condition
- Have any required regulatory notifications occurred

The CRB should identify nonconformity if the EMS has failed to identify or appropriately respond to non-compliance situations.

How the CRB should respond to stakeholder complaints:

When a CRB receives a complaint from a stakeholder about the environmental performance of a certified organization they should:

- Report the complaint to the organization without delay and determine its validity
- Determine whether the EMS has recognized and adequately responded to the complaint or condition
- Determine whether the condition represents a nonconformity to the standard
- Follow up with the complainant to inform them of the outcome (while maintaining appropriate levels of confidentiality with the certified organization)
- Take appropriate action where the EMS is found to be out of conformance.

It is the CRB's responsibility to report the complaint to the certified organization and to determine whether the management system continues to conform to the requirements of ISO-14001.

The organization is responsible for follow up and appropriate response to the complaint and to assure the continued conformance or correction of the system to the requirements of the standard.

The balance between office/paper auditing and on-site evaluation of the implementation of the system in the day to day activities of the organization:

Every EMS assessment involves evaluation of the planning, implementation and effectiveness of the environmental management system. This process requires that the system documentation be reviewed and that records be examined. The effectiveness of the system cannot be evaluated, however, without significant evaluation of its appropriateness and implementation in actual practice.

While the first stage of the assessment involves a determination of the completeness and readiness of the audit for audit, in the vast majority of cases this cannot be realistically evaluated without the auditor's on-site exposure to the facilities, activities and products.

During the second stage of the audit, implementation must be evaluated in terms of how well the EMS controls environmental aspects at their point of occurrence. Further, much of the EMS relies on communication and commitment on the part of all appropriate personnel to the environmental policy, which can only be evaluated through observation of the routine activities of the organization.

The auditor then must strike a balance between paper review and evaluation of the EMS implementation during normal activities in order to make an adequate assessment of the effectiveness of the EMS. Unfortunately, there is no formula to define what the relative proportions will be, as the situation is different in every organization. However, there are some indications that too much of the audit time dedicated to paper review is a problem that occurs with some frequency. This could lead to an inadequate assessment of the effectiveness of the EMS and potentially to poor performance issues being overlooked and leading to a loss stakeholder confidence in the certification process.