

Audits and Privilege in the ISO 14000 Arena

by Reeva I. Schiffman

Can an organization embrace the ISO 14000 series of standards without the risk of opening up its environmental shortcomings to scrutiny by external parties? The International Organization for Standardization (ISO) 14000 series of standards represents a novel approach to environmental management that relies on changes in organizational commitment, focus and behavior rather than on coercion from regulatory authorities. The ISO 14000 process contemplates rigorous internal auditing and self-assessment, the results of which will be communicated to both internal and external interested parties. Audit confidentiality and/or provisions addressing the effects of disclosure of audit results are critical issues for organizations seeking registration to the standards.

ISO 14000 is an evolving series of standards being developed to provide organizations with the structure for managing environmental impacts. The standards address the following six distinct but related subjects:

- Environmental management systems;
- Environmental auditing;
- Environmental performance evaluation;
- Environmental labeling;
- Life-cycle assessment; and
- Environmental aspects in product standards.'

The underlying premise of ISO 14000 is improvement of environmental performance through self-regulation and market-driven pressure. An EMS provides organizations with order and consistency which enables them to address environmental concerns through the allocation of resources, assignment of responsibilities, and on-going evaluation of practices, procedures and processes. An EMS is essential to an organization's ability to anticipate and meet its environmental objectives, and to ensure ongoing compliance with national and/or international requirements.

Under the management system standard, ISO 14001, companies proceeding with registration will develop an environmental policy; identify aspects and impacts of their activities, products and services; define significance and prioritization of impacts; identify legal and other requirements governing the operation of the organization; establish objectives and targets; implement a program or programs to meet those targets; a reporting system; audits; reports to management; as well as follow-up and corrective action with regard to audit findings.

Three specific issues (commitments) must be addressed under the ISO 14001 policy requirements: (1) commitment to continual improvement; (2) commitment to prevention of pollution; and (3) commitment to compliance with relevant environmental regulation, laws and other criteria to which the organization subscribes. The commitment to compliance with relevant environmental regulations and the resulting documentation is of particular concern to the legal community; specifically, what privilege/ protection will be afforded to audit documentation. Before we delve further into the issue, it is important to understand the distinctions between a traditional regulatory compliance audit and EMS audits.

Traditional Regulatory Compliance Audits

In a traditional compliance audit, the organization's performance is evaluated in a "snapshot" of time against a set of requirements, whether imposed by regulatory authorities or by the organization itself. The environmental activities of the organization are compared to a prescribed set of activities or results found in permits, regulations, legislation and the organization's own internal standards. Performance is usually related to predetermined parameters such as

emissions levels, reporting, number of exceedances. etc.

Judgement calls are not usually required in traditional compliance audits. The auditor is looking for areas where the organization has failed to follow the rules, so that it can be warned before the regulators find out. Compliance auditors generally are concerned with the paper trail, and interview only as necessary to clarify the paper trail and to understand where the rules have not been followed. Interaction is primarily with the environmental staff, and the approach used to follow the rules is immaterial.

ISO EMS Audits

An EMS audit is not a compliance audit. The distinction between the two types of audits relates to what is being audited, how the audit is being conducted and the time perspective. It is important to note that ISO 14001 does not require 100 percent regulatory compliance. Rather, it addresses compliance by requiring a commitment in the environmental policy to comply with relevant laws and regulations (Section 4.1), establishing and implementing a procedure to identify and have access to legal requirements (Section 4.2.1), and establishing and implementing a documented procedure to periodically evaluate compliance with legal and regulatory requirements (4.4. 1). An auditor should be looking for objective evidence that the appropriate procedures and related activities are in place. Regulatory non-compliances that are identified and corrected through established procedures may offer evidence that the procedures are effective.

The EMS audit required by ISO 14001 Paragraph 4.4.4 is an audit of the management system or program, which asks the question: Does the system address the requirements of the standard. and is there evidence that it is being implemented? An

EMS audit goes beyond environmental data and looks at a company's organization and structure to determine if the methods used to achieve the results are working. An EMS audit evaluates the process of how the results are achieved. It looks at the documentation to understand whether the system is "doing what it says and saying what it does."

The auditor is interested in evidence of policies, plans, programs, procedures, clearly assigned responsibilities, measurement, internal audits, reviews, follow-ups and signs of improvement. The focus of the EMS audit is on whether management's system for compliance is effective. Does it include processes, procedures, technology and tools needed to enable end-users to fulfill their compliance requirements?

Whereas the traditional compliance audit looks at the present and the past, the EMS audit looks at the present and the future and answers the question: "Will my system keep me in compliance?" The EMS audit takes a more prospective look and helps establish whether a company structurally has the ability, either through technology or other "systemized" means, to manage documents to enable compliance with the standard and more importantly, safeguard against future problems.

In addition, unlike the traditional compliance audit, an effective EMS audit requires that a broad spectrum of personnel be interviewed. Interaction with environmental personnel alone will not provide the full picture, but rather management will be included in the EMS audit to demonstrate that there is genuine support for the EMS, an understanding of the environmental needs and a commitment to allocate the resources. In addition, interviews with production personnel, line workers and quality personnel will assist with the evaluation of the EMS.

Distinctions between the two types of audits may be best summarized by detailing what EMS audits are, and what they are not. EMS audits are:

- A good way to assess a company's commitment to environmental performance and to continuous improvement;

- A way to evaluate the sustainability of that performance;

- Tools to address how activities are carried out, the organizational structure, the review processes, and the reporting of information;

- Tools to provide an understanding of how a facility carries out and meets its environmental responsibilities;

- A way to verify that appropriate systems are in place and are functioning to ensure continued compliance;

- A way to confirm that appropriate environmental performance goals have been established;

- Tools to review the existence of internal company audit procedures to ensure ongoing compliance with goals and regulations;

- Tools to assess that systems are in place to ensure continuous improvement;

- Tools to look at the programs and the linkages of the programs to other processes;

- Tools to evaluate a company's organizational structure, looking for effective integration of accountability and responsibility throughout the organization.

EMS audits are NOT:

- Tools to identify non-compliance with regulations or departures from internal or voluntary standards;

- Meant to establish the adequacy of certain environmental performance measures;

- Compliance audits.

Whereas compliance audits are the "snapshots" of performance, EMS audits are the documentaries, probing the commitments to environmental performance and continuous improvement over the life of the organization.

Privilege

ISO 14000 will move companies in the direction of voluntary, self-auditing and self-correction.

However, little provision exists for protections (privileges or immunities) for those entities which do self-audit. None of the traditional bases for protection, the attorney-client privilege or the attorney work product doctrine, meets all of the concerns regarding disclosure of environmental audits. The self-evaluative privilege could potentially be applied to ISO 14011, however, the privilege has not been widely recognized.

ISO 14011 audits will not have any of the criteria normally required to successfully assert the traditional privileges. They are generally not performed by attorneys, but rather by management personnel. They are generally not performed to obtain legal advice, but rather to obtain a business advantage. They are not conducted in anticipation of litigation, and they are generally not kept confidential. In fact, the audit results are just the type of information that needs to be disseminated for educational purposes; to demonstrate progress and shortcomings to employees.

In response to the inadequacies of these traditional privileges, there is a growing movement on the part of state legislatures to enact state audit privilege laws. The legislation extends self-evaluation type privileges to information contained in voluntarily prepared environmental audit reports. The laws provide varying degrees of protection for environmental compliance audit results and/or immunities from civil and criminal action. This type of legislation has been enacted in 19 states (as of July 1996) and 24 other states (as of April 1996) have audit legislation under consideration.

However, each of these laws has significant exceptions: they do not always address systems audits specifically, and without companion federal legislation, provide no help in federal courts.

In addition, the focus of these laws is to protect companies who seek-out and correct instances of non-compliance. Since the ISO audit does not directly focus on non-compliance with applicable laws, there is a question as to

whether the results of such an audit would be deemed privileged.

Why is this lack of privilege so important? ISO audits are not compliance audits, and will not focus on issues of non-compliance with applicable laws. The reality of the matter is that an important element of an EMS is how well it helps the company achieve its goals, one of which is a commitment to comply with applicable regulations and other requirements. To evaluate how well the company is achieving this goal, it is likely that compliance status will be looked at during the audit. The audit will identify instances of non-compliance and evaluate the effectiveness of the system for detection of the non-compliance and corrective action and reporting, once the matter is discovered. Such an evaluation can have critical implications in terms of corporate liability.

Strategies

There is no easy answer, but the following strategies have been identified to help maximize the prospect that at least portions of the audit results and associated documentation can remain confidential:

- Conduct a bifurcated audit;
- "Red-flag" compliance issues and separate them from the main part of the audit;
- Conduct "pre-audits" under attorney-client privilege as a precursor to formal certification audits;
- Discuss audit philosophies with prospective auditors beforehand to determine how they would handle a non-compliance issue discovered in the course of an audit.

The bifurcated audit offers protection by handling management and information systems through the regular audit process, and addressing questions of legal compliance with a separate team operating under the direction of counsel. This will take a great deal of planning, and naturally will take a lot more time and money to implement. A "red-flagging" procedure

could be developed and implemented whereby as soon as a non-compliance issue or an issue that could lead to liability arises, the problem would be referred to legal counsel. From the time the non-compliance is first identified, the evaluation would proceed under the attorney's supervision. Although the non-compliance may have to be noted in the audit, the detailed information regarding the resolution of the problem could be protected by virtue of this bifurcation. In essence, once a non-compliance was identified there would be a different procedure for addressing the non-compliance, ultimately resulting in corrective action.

The auditor would be looking at the standard and the procedures that have been implemented to ensure conformance to the standard.

Use pre-audits/initial reviews as tools. An initial environmental review/pre-audit, consisting of a comprehensive analysis of the environmental issues, impact and performance related to activities at a site, is not required either expressly or by implication by the 14001 specification. However, many organizations will find such reviews to be useful tools.

Not only does the pre-audit give the company an opportunity to identify and correct any serious legal exposures in advance of the formal audit process, it helps to define the scope of the EMS, it helps in the identification of aspects and impacts, and, it gives the organization an idea of the time and money costs associated with the audit process. A good compliance audit should indicate where performance deviates from compliance, and if there have been several consecutive audits, there may be indications of patterns of non-conformance that may suggest a structural change in how things are done. Although these pre-audits might not receive the full protection, it will have greater protection than the ISO 14011 audit.

Finally, remember, the auditee is the client, and as such will interview and select the auditor. It

is important to have a meeting of the minds between auditor and auditee. Auditors will be called on to make judgement calls, and as such the company should select an auditor or registrar that is experienced in the industry sector, is knowledgeable about the environmental issues typical of that sector, and thoroughly understands the ISO 14001 requirements.

Although registrars are expected to treat all information, including regulatory non-compliances uncovered during the audit process, as entirely confidential, leaving the organization to make any required notifications to appropriate regulatory agencies, the specific handling of non-compliances is left to the individual registrar. Interviewing auditors to ascertain their philosophy on critical issues, including areas of regulatory non-compliance, should be a part of the selection process.

Conclusion

The ISO series of standards continues to evolve, and issues continue to be raised. The issues identified above are real, and must be understood and addressed in advance. Environmental counsel should be consulted throughout the process to ensure the success of an organization's implementation of the ISO 14000 standards. The learning curve is steep. However, as we learn more and as consciousness is raised, the fear of the loss of privilege will be outweighed by the benefits of implementation of ISO 14000.

Endnote

1. The final environmental management system (EMS) standards (14001 and 14004) were issued in September 1996: ISO 14001 Environmental Management Systems Specification with Guidance for Use and ISO 14004 Environmental Management Systems - General Guidelines on Principles, Systems and Supporting Techniques. The three environmental auditing standards Guidelines for Environmental Auditing - General Principles on Environmental Auditing (14010). Guide