How ISO 9001 and 14001 Support Sarbanes-Oxley Compliance

By Sandford Liebesman

Introduction

In September 2005, I published an article in Quality progress entitled "Mitigate SOX Risk with ISO 9001 and 14001[1]. This paper is an extension of that article.

In October 2003 the SOX-Q/E Team was formed to identify how ISO 9001:2000[2] and ISO 14001:1996[3] can be used to reduce the risk that CEOs, CFOs and the Board of Directors face when complying with SOX. Note that any comprehensive quality and environmental management system such as the Malcolm Baldrige Award criteria can be used in place of the ISO standards.

SOX mandates a system of internal controls to manage risk in the organization. A system published by the COSO Committee[4] in 1992[5] provides the basis for internal controls used by many organizations. This system is the foundation for good governance which preceded SOX. There are five components of the COSO internal controls:

- Control environment
- Information and Communication
- Risk management
- Monitoring
- Control Activities

Let us compare these components of COSO internal controls with requirements of ISO 9001 and ISO 14001.

Control Environment

The control environment must set the tone of an organization and form the foundation of the guidelines which provide discipline and structure. It includes the way management assigns authority and responsibility, and organizes and develops its people.

ISO 9001 and ISO 14001 require identification of an organization's processes, their sequence and interaction and the definition of quality and environmental policies. Further, ISO 9001 requires the establishment of quality objectives and ISO 14001 requires definition of environmental objectives and targets. They also require control of documents and records. Both standards state that personnel must be "competent based on education, training, skills and experience."

Information and Communication

To satisfy COSO, information must be identified, captured and communicated so that people can carry out their responsibilities. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously.

ISO 9001 and ISO 14001 are used to enhance the decision making process and manage the operations through information and communication within the organization. Both standards require communication with customers and suppliers.

Risk Management

Risks must be identified, analyzed and managed. Key inputs are corporate objectives linked at different levels and internally consistent. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

The data obtained in ISO 9001 as a result of process and product measurements can be used in risk assessment and continual improvement. ISO 9001 requires analysis of this data, turning it into information that can be used to identify risks to the organization. The standard requires trend analysis which is a good predictor of developing problems. These activities are all reviewed by top management in the management review process.

ISO 14001 requires identification of environmental aspects which can interact with the environment. In addition the standard requires identification of significant aspects and the operations and activities associated with these aspects. Again, we have an early warning tool that can be used to identify impending risk.

Monitoring

Monitoring requires assessing the quality of system performance over time. This is done through periodic assessments and continual monitoring of processes. Monitoring includes regular management and supervisory activities, and review of other actions personnel take in performing their duties.

ISO 9001 requires monitoring and measurement of processes and products. The raw data obtained may provide the first warnings of impending problems. Another monitoring activity, measurement and analysis of customer satisfaction in ISO 9001 is also a tool for early warning of organizational concerns. Implementing ISO 9001 turns this data into information. ISO 14001 requires monitoring and measurement of key characteristics of operations and activities that may result in significant environmental impacts.

Control Activities

Control activities are the actions taken to address risk and achieve the objectives of the corporation. Control activities occur throughout the organization, at all levels and in all functions.

In ISO 9001, the key to controlling the health of an organization is the “improvement loop.” As part of the loop, ISO 9001 requires documented procedures to define corrective and preventive actions. Both tools provide methodologies to manage or eliminate risks to the organization. One source of corrective actions is the requirement to implement a documented procedure for internal audits and to provide follow-up activities through corrective actions.

ISO 14001 requires taking corrective and preventive actions to mitigate impacts and reduce environmental risk. In addition, ISO 14001 requires management of non-conformances, taking actions to reduce impacts using corrective and preventive actions. For both environmental and quality management systems, the result is improved alignment of the organization with basic corporate objectives.

Top management asserts control of risk through the management review process in ISO 9001 and ISO 14001. These meetings are used to pull together the key bits of information and actions that are used to set the direction of the organization and to implement risk reduction activities.

Auditing to Add Value

The main goal of internal audits is to provide Top Management and the Board of Directors with an accurate understanding of the organization’s financial and operational status. Combining QMS/EMS “tools” with the financial auditing function and procedures will result in more effective audits and increase the understanding of the material non-financial information of the organization.[6]

Two of the many values of ISO 9001 and ISO 14001 are the process approach and continual improvement. Many organizations extend the process approach to a set of process audits which result in an effective means of evaluating the status of the organization and managing the risks that they face.

Conclusions

Three goals of corporate governance are management of risk, effective process management and continual improvement of company performance. Quality and environmental management systems such as ISO 9001:2000 and ISO 14001:2004 are excellent tools for accomplishing these objectives. The board should move the corporate mentality from correcting problems to preventing them. Accomplishing these goals will provide an excellent step toward satisfying the Sarbanes-Oxley Act.

I’ve made the case for quality and environmental people “to be at the table” when the internal financial auditors develop their reports to top management and the Board of Directors. The goals are risk reduction, expanded information for top management decisions and help in satisfying the requirements of the Sarbanes-Oxley Act. Table 1 contains a description of the COSO guidance and the corresponding ISO 9001 clauses.

COSO model for SOX	ISO 9001	Clause
1. Internal Control Environment	4.1	Quality management system
*Foundation for all other COSO elements. *Does the organization do things right? *Does the organization do the right things and maintain a high degree of integrity in its dealings? *Few complaints alleging misconduct are received from customers or others. *Competence of personnel maintained. *Effective management style or “Tone at the Top” maintained.	5.3	Quality policy
	5.4.1	Quality objectives
	5.5.3	Internal communication
	6.1	Provision of Resources
	6.2.2	Employee competence
	7.1	Planning Product Realization
	8.1	Planning Measurement, Analysis and Improvement
2. Information and communication	4.2.3	Control of Documents
*Information captured and communicated enabling people to carry out their responsibilities. *Reports used to run and control the business.	4.2.4	Control of Records
	5.1	Top management communication
	5.5.3	Internal Communication
	7.2	Customer Requirements

*Information about external events, activities and conditions for making informed business decisions. * How is information identified, captured, and communicated? Does it flow across the organization? * Do employees understand their roles in the control process? * Are there processes in place to address employee, supplier, and customer concerns in a timely manner?	7.2.3	Customer communication
	7.4	Purchasing
	7.4.2	Supplier communication
3. Risk Assessment	5.4.1	Measurable Objectives
* Establishment of objectives, linked at different levels and internally consistent. * Identification, analysis and management of risks to achieving objectives. * Mechanisms to deal with change and the risks relevant to change. * Effective Risk Assessment requires: o Definition of the objectives. o Determination of the compatibility of the objectives. o Identification of risks to achieving the objectives. o Determination of risks associated with change. o Judgment as to which risks are critical. o Determination of actions to mitigate risks starting with the critical ones.	5.6	Management Review
	7.2	Contract Review
	7.4.3	Supplier Data
	8.2.1	Customer Satisfaction Data
	8.2.2	Internal audit
	8.2.3	Monitoring and measurement of processes
	8.2.4	Monitoring and measurement of products
	8.4	Data Analysis to demonstrate QMS suitability & effectiveness
	8.5.1	Continual Improvement
	8.5.2	Corrective Action
	8.5.3	Preventive Action
	14001,4.3.1	Environmental Aspects and Identification of Significant Aspects.
4. Monitoring	5.4..1	Measurable Objectives
* A process that assesses the quality of the system's performance over time through separate evaluations and/or ongoing monitoring activities * Key tools include internal auditing, management and supervision of operations and actions of personnel performing their duties. * Management is responsible for implementation. * Auditors must drill down to "root causes," follow audit trails and identify significant deficiencies and material weaknesses.	5.6	Management Review
	8.2.1	Customer Satisfaction Data
	8.2.3	Monitoring and measurement of processes
	8.2.4	Monitoring and measurement of products
	8.4	Analysis of data
	8.5.1	Continual improvement
5. Control Activities	5.6 and 14001,4.6	Management Review
* Policies and procedures that help ensure management directives are carried out, including approvals, verifications, the security of assets, authorizations, reconciliations, and the segregation of duties.	8.3	Control of Nonconforming Product
	8.5.2	Corrective Action
	8.5.3	Preventive Action
	14001,4.4.7	Emergency Preparedness & Response

* Timely actions taken to address risks to the achievement of the entity's objectives, exceptions and information that requires follow-up. * Control activities are based on objectives, risks and what appears to be effective. * Control activities are put in place for significant plans and programs such as the management of supplier products and outsourced services.	14001,4.5.3	Nonconformity, Corrective Action and Preventive Action

About The Author

Sandford Liebesman, Ph.D.**,** is a senior professional recognized as a leading expert on international quality standards, ISO 9001 and TL 9000 assessments, business excellence models, risk mitigation based on quality management systems and the Sarbanes-Oxley Act. He is an ASQ Fellow and Chairman of the ASQ Electronics and Communications Division. Dr. Liebesman is also a senior consultant for Change Management Consulting, Inc. He may be reached at sliebesman@cmc-changemanagement.com.

[1] Sandford Liebesman, "QMS and EMS Support Financial Management Systems," Quality Progress, September 2005, 83-85.

[2] The International Organization for Standardization, *ISO 9001:2000: Quality Management Systems – Requirements*, Geneva, Switzerland, 2000.

[3] The International Organization for Standardization, *ISO 14001:2004*: *Environmental Management Systems – Requirements with Guidance for Use*, Geneva, Switzerland, 2004.

[4] COSO: The Committee of Sponsoring Organizations of the Treadway Commission.

[5] "Internal Control – Integrated Framework, Evaluation Tools, the Committee of Sponsoring Organizations of the Treadway Commission., September 1992.

[6] The SEC stated that senior officers must certify that material non-financial information is also included in the quarterly and annual reports.