An ENLAR® Compliance Services White Paper

Introduction to ISO 19011, Guidelines for Auditing Management Systems

Executive Summary

An important internal audit function is evaluating the effectiveness and efficiency of an organization's control processes. These control processes include the policies, procedures and activities in place within an organization for managing risk and achieving organizational objectives.

In the standards developed by the International Organization for Standardization (ISO), "control processes" are defined as an organization's management system. To conform to the ISO standards, organizations are required to establish and maintain management system processes. Organizations are also required to establish internal audit programs. The guidelines for understanding these internal audit requirements are set out in ISO 19011, *Guidelines for Auditing Management Systems*.

The purpose of this white paper is to provide an introduction to the audit guidelines set out in the ISO 19011:2011 standard. This white paper also summarizes some of the challenges that are likely to be important topics of discussion during the upcoming revision of ISO 19011.

Standards for Organizational Control Processes

As business operations have become increasingly complex, establishing control processes has become critical for organizations. Equally important is establishing robust audit programs for assessing the effectiveness of these control processes in managing risk and achieving the organization's objectives.

Several organizations have developed standards and frameworks to assist organizations in establishing and auditing organizational control processes. These include the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the International Organization for Standardization (ISO) and The Institute of Internal Auditors (The IIA).

COSO Internal Control Framework

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published its *Internal Control – Integrated Framework*. This document was updated and expanded in 2013.[1] The COSO framework provides an approach organizations can use to develop and maintain systems of internal controls for achieving their established objectives. The COSO Framework consists of five core components:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

A key part of the monitoring component is conducting periodic evaluations to determine whether appropriate internal controls are present and functioning. Internal auditors are encouraged to use the COSO Framework for assessing the effectiveness of an organization's system of internal controls.

ISO Management System Approach

The International Organization for Standardization (ISO) published its first management system standard in 1987. This standard, ISO 9001, set out requirements for a quality management system. In 1996, ISO published its next management system standard, ISO 14001, which established requirements for an environmental management system.

Since then, the development of ISO management system standards has grown exponentially. Today, there are over 20 discipline-specific management system standards.[2] These standards have been written to provide a basis for third-party certification, and many organizations have obtained certification to multiple management system standards. Based on the surveys conducted by ISO, over a million organizations worldwide have obtained third-party certification of their quality management system.[3] Many of those organizations have implemented environmental and occupational health and safety management systems as well.

Facilitating Management System Integration

To facilitate management system integration within organizations, ISO has established a mandatory framework for its management system standards. This framework (commonly referred to as "Annex SL") sets out mandatory definitions, a common high-level structure and core requirements for ISO's management system standards.[4]

These core management system requirements are organized into the following clauses:

- Context of the organization
- Leadership
- Planning
- Support
- Operations
- Performance evaluation
- Improvement

A key component of all of the ISO management system standards is the requirement that an organization have an internal audit program in place to evaluate whether its control processes are effectively implemented and maintained. The guidelines for establishing an effective internal audit program are set out in ISO 19011, *Guidelines for Auditing Management Systems*.[5]

International Professional Practices Framework

The IIA International Professional Practices Framework (IPPF) recognizes the importance of evaluating organizational control processes. Performance Standard 2130 states, "*The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.*"

The IIA has developed several Practice Advisories and Practice Guides relevant to the assessment of different types of operations and the evaluation of the effectiveness of controls for responding to various kinds of risk. Several of these are directly related to topics that are also addressed in ISO management system standards. This includes:

- Practice Advisory 2120-1 – Assessing the Adequacy of Risk Management Processes
- Practice Advisory 2130-1 – Assessing the Adequacy of Control Processes
- Practice Advisory 2030.A1-1 – Information Reliability and Integrity

Introduction to the ISO 19011 Guidelines

ISO first published audit guidelines in 1990 and 1991. These initial guidelines focused on auditing quality systems. When ISO published ISO 14001 in 1996, it also published guidelines on auditing environmental management systems. In 2002, these six separate quality and environmental audit standards were consolidated into one standard for both types of management system auditing. That standard is ISO 19011. When ISO 19011 was revised in 2011, the scope of the standard was expanded to cover all management system auditing.

The ISO 19011:2011 standard contains guidance on the following topics:

- Principles of auditing
- Managing an audit program
- Audit activities
- Competence and evaluation of auditors

Principles of Auditing

Clause 4 of ISO 19011 sets out six general principles that guide the performance of management system audits. These principles are:

- Integrity
- Fair presentation
- Due professional care
- Confidentiality
- Independence
- Evidence-based approach

Conformance with these principles is necessary to ensure an audit is an effective and reliable tool in support of management policies and controls.

Managing an Audit Program

Clause 5 of ISO 19011 provides guidance on establishing and managing an audit program that meets the requirements set out in the ISO management system standards. The required audit program activities include:

- Establishing audit procedures and methodologies
- Selecting audit personnel and defining roles and responsibilities
- Defining objectives, criteria and scope for each audit
- Ensuring the audit results are communicated

ISO 19011 also suggests approaches that can be considered for assessing the effectiveness of the audit program itself to ensure it is meeting the objectives set by the organization.

Audit Activities

Clause 6 of ISO 19011 outlines the general steps followed in planning and conducting individual audits. These steps are:

- Initiating the audit
- Preparing for the audit
- Conducting the audit
- Preparing and distributing the audit report
- Completing the audit
- Conducting audit follow-up

The guidance in ISO 19011:2011 currently focuses primarily on the activities typically associated with on-site audits, i.e. audits conducted at the physical location where the activities being audited are conducted.

Competence and Evaluation of Auditors

Clause 7 of ISO 19011 outlines criteria for selecting auditors for management system audits.

In the beginning of this clause, a four-step process is suggested for evaluating auditor competence. This is followed by guidance concerning the types of competence needed for performing management system audits. To be competent, auditors need both 1) generic knowledge and skills needed to audit management systems and 2) discipline-specific knowledge needed to audit a particular type of management system in a particular business sector.

Audit Program Challenges

In early 2016, ISO approved the next revision of the ISO 19011 standard. This revision will be conducted within an ISO Project Committee (referred to as a PC) that has been established specifically for this work – PC 302.

There are a number of audit challenges to be addressed in the upcoming revision of ISO 19011. Some of these challenges include:

- Conducting risk-based audits
- Impact of evolving information technologies
- Addressing complex business structures
- Safeguarding audit objectivity
- Ensuring competence of audit personnel

Challenge #1: Conducting Risk-Based Audits

One of the new focuses in the ISO management system standards is "risk-based thinking." The planning requirements set out in Clause 6 of the newly-revised quality and environmental management system standards (ISO 9001 and ISO 14001) require that the organization determine those risks and opportunities that need to be addressed to give assurance that the management system can achieve its intended outcomes. The organization is then required to implement the control processes needed to address those risks and opportunities.

This requirement is similar to the guidance set out in the COSO *Internal Control – Integrated Framework* that organizations develop and maintain systems of internal controls that enhance the likelihood that the organization will achieve its objectives.

What this means for internal audit programs is that auditors must have the knowledge and skills needed to be able to understand and evaluate the processes an organization has established for determining its risks. Auditors must understand and be able to utilize appropriate audit techniques in assessing the adequacy and effectiveness of internal control processes. This includes the control processes in place for achieving a range of organizational objectives across multiple management system disciplines and for ensuring compliance with often complex legal requirements.

Currently, ISO 19011 does not include specific guidance on conducting process audits or on risk-based auditing.

Challenge #2: Impact of Evolving Information Technologies

Since the ISO 19011 standard was last revised in 2011, new information technologies have developed that impact how internal audits are conducted.

There have been significant advances in video and audio capabilities that allow for remote observations and off-site interviews. The availability of easy-to-use web-based survey tools can change how audit information is collected. Increasing reliance on cloud technologies for data collection and storage means that auditors can conduct more audit tasks remotely.

For both on-site and remote audits, the increasing reliance on electronic storage of documents and records also changes how "documented information" is defined, used and retained. This creates new challenges for auditors in verifying information. In many audit situations, needed information is stored in multiple database systems – all with different storage structures, controls and access protocols. This can create significant challenges for auditors in being able to access information and in determining whether the information provided is reliable.

Currently, the guidance in ISO 19011 presumes that audits are always conducted on-site with formal opening and closing meetings using in-person interviews.

New information collection options may require rethinking the traditional paradigm that management system audits are always structured as on-site activities. Audits may no longer need to be conducted using traditional audit teams or even in-person interviews. Auditors may no longer need to travel to locations where activities are being performed. Formal opening and closing meetings may not be needed or even appropriate for every audit situation.

Challenge #3: Addressing Complex Business Structures

Organizations are increasingly reliant on a complex network of outsourced functions and processes. This means that critical business functions may no longer be internal. These processes may be performed by contractors or business partners at facilities in multiple locations across the globe.

The ISO management system standards based on Annex SL include a requirement that the organization ensure that relevant outsourced processes are controlled. In order to determine whether this requirement is being met, many organizations will need to perform supply-chain audits.

The auditing of outsourced processes is another topic not specifically addressed in ISO 19011.

Challenge #4: Safeguarding Audit Objectivity

A significant challenge with management system audits is ensuring the objectivity and independence of those conducting audits, as well as those who manage internal audit programs. Maintaining independence is an on-going issue as auditors are increasingly pressured to provide recommendations for addressing system nonconformities, and audit program managers are asked to justify that audit programs are providing business value.

Much has been published since ISO 19011 was last revised on the various sources of bias in auditing, including the impact of cognitive bias. The interrelationship between bias, independence and objectivity is a subject that remains one where additional guidance is needed.

Challenge #5: Ensuring Competence of Audit Personnel

Confidence in audit results depends in large part on confidence in the competence of those conducting the audit. It also depends on the competence of those managing the audit process, as well as the competence of any technical experts providing input relied on within the audit program.

The guidance in ISO 19011 explicitly recognizes that one individual is unlikely to have the competence needed to perform every type of audit. Organizations need to establish an evaluation process to ensure that auditors have the competence needed to achieve the objectives established for the audits they have been selected to perform.

As discussed at length in ISO 19011, in order to conduct management system audits, auditors need a combination of audit skills, management system expertise and discipline-specific technical knowledge. Auditors need to understand the commonly-used risk assessment techniques and typical control processes relevant to the audits they are conducting. For example, auditors conducting environmental management system audits need to understand techniques for identifying and assessing environmental aspects, taking into account the associated environmental impacts.

ISO 19011:2011 has an entire clause devoted to competence and evaluation of auditors. The challenge in revising the standard will be drafting language that provided guidance that is helpful to organizations without being overly prescriptive.

What ISO 19011 does not address in the same depth is the competence required for other audit personnel. Increasingly, audit program managers are relying on third-party contractors and software vendors to assist them in developing the audit protocols and databases they use to plan audits, manage the audit process, collect audit evidence and record audit findings. The competence of the personnel performing these outsourced functions can be equally important to the completeness and reliability of the audit results obtained.

White Paper Author

Thea Dunmire is an environmental attorney who specializes in the implementation of effective environmental, health and safety management systems that help organizations improve their EHS performance.

Thea is a recognized leader in the development of ISO management systems. She has participated internationally in the development of multiple ISO standards, including ISO 19011:2011. She maintains a blog on the ISO 19011 standard at: www.iso19011expert.com.

Thea got her undergraduate degree from the University of Iowa in biomedical engineering and received her law degree from Syracuse University. She is a certified industrial hygienist (CIH) and a certified safety professional (CSP). Prior to starting ENLAR, she was an attorney with U.S. EPA Region 5 and a partner at the law firm of Dickinson Wright.

Contact Information:

Thea Dunmire, JD, CIH, CSP
ENLAR Compliance Services, 3665 E Bay Dr. #204C, Largo, FL 33771
www.enlar.com
727-754-3670
tdunmire@enlar.com

---

[1] This document can be accessed at http://www.coso.org/IC.htm

[2] A current list of the ISO management system standards can be found at: http://www.iso.org/iso/home/standards/management-standards/mss-list.htm.

[3] Information on the survey results for management system certifications can be found at: http://www.iso.org/iso/iso-survey

[4] The ISO Directives (including Annex SL of Part 1) can be accessed at: http://www.iso.org/iso/standards_development/processes_and_procedures/iso_iec_directives_and_iso_supplement.htm

[5] The ISO 19011:2011 standard can be purchased from the American Society for Quality (ASQ) at: http://asq.org/quality-press/display-item/?item=T883E.