Audrey Milesi (audrey.milesi@amc-advisory.com) is CEO of AMC Advisory in Switzerland.

Leveraging compliance monitoring programs for successful ISO audits

By Audrey Milesi

Compliance monitoring programs play a pivotal role in ensuring organizations comply with regulatory requirements. Organizations are expected to have a robust compliance monitoring program in place to ensure appropriate governance. Depending on their field of activities, organizations may also be subject to International Organization for Standardization (ISO) certification(s) to guarantee a certain reputation. ISO was founded in 1947, and its standards are vital to companies wanting to be certified.

ISO audits are a critical aspect of the certification process, serving as the litmus test for an organization's adherence to these global standards. Hence, if a company already has a compliance program in place, it would be recommended to leverage it to efficiently avoid duplicating work. This article delves into the intricacies of compliance monitoring programs, their significance, and how they can be effectively used for a successful ISO audit.

Understanding the purpose of ISO audits

ISO standards are globally recognized benchmarks for quality, environmental responsibility, information security, and other facets of business operations. Achieving ISO certification can provide an organization with a competitive edge, foster trust among customers, and enhance the overall efficiency of operations. Note that ISO certifications are not always required; some organizations decide to get certified only to improve their reputation and credibility.

ISO-certified auditors carry out ISO audits over a three-year period. Auditors will assess a company's overall alignment of policies, processes, and procedures against ISO standards and expectations.

These audits indicate an organization's commitment to quality, continual improvement, and adherence to global best practices.

The role of compliance monitoring programs

Compliance monitoring programs serve as the backbone of an organization's ISO audit readiness. These programs encompass the systematic and ongoing evaluation of an organization's processes, policies, and procedures to ensure they meet the specific ISO requirements.

Here are some essential aspects of compliance monitoring programs and their significance in ISO audit preparation.

1. Setting the foundation

Before even considering ISO certification, an organization must establish a robust compliance monitoring program led by the compliance team (and may also include the risk management team). This program is the foundation upon which the organization's ISO journey can be built. It defines how compliance with ISO standards will be assessed and maintained.

2. Ongoing monitoring

Compliance monitoring is not a one-time activity; it's an ongoing process. Regular monitoring of processes, policies, and procedures is crucial to ensure compliance is maintained over time. This continuous evaluation demonstrates that an organization doesn't just temporarily meet ISO standards but remains compliant in the long run. The frequency may vary depending on various factors. For example, policies are usually reviewed annually (or ad hoc any time there is a significant change in process); however, some operational activities (such as a client's transactions) may be reviewed daily or weekly.

It is good practice to define all activities in the program and their frequencies and report on the results quarterly, biannually, or—at the very least—annually.

3. Identifying gaps

One of the primary purposes of compliance monitoring programs is to identify gaps in an organization's compliance with regulatory requirements, which can also be used toward ISO standards. Any ISO audit starts with the preparation of a so-called statement of applicability. The organization must fill in this document so auditors can customize their audits. In doing so, the organization can already identify potential gaps early in the process and be able to take corrective actions to rectify them.

4. Corrective action

Compliance monitoring programs are not just about identifying issues but also about proposing corrective actions—subject to management and sometimes board of directors approval. When gaps in compliance are identified, organizations can implement corrective measures to address these shortcomings, thus improving their adherence to ISO standards.

5. Data gathering and documentation

Proper documentation is a crucial aspect of any compliance program. It requires organizations to maintain thorough records of their activities and corrective actions taken. This documentation can also be used during ISO audits, as it provides evidence of an organization's commitment to compliance.

Steps to leverage compliance monitoring for ISO audits

Now that we understand the significance of compliance monitoring programs, let's explore the steps to effectively leverage these programs for ISO audits.

1. Identify applicable ISO standards

The first step in leveraging compliance monitoring programs for ISO audits is to identify the ISO standards applicable to your organization. Different ISO standards pertain to various aspects of business, such as quality management, environmental management, and information security. Choose the standards that align with your

organization's goals and needs. The most common standards are 9001 (quality management) and 27001 (information security). But there are standards for nearly all sectors of activities.

2. Establish an audit schedule

Once you've identified the relevant ISO standards, establish a regular audit schedule with ISO auditors. Usually, an agreement covers three years.

3. Create an audit checklist

Develop a comprehensive audit checklist based on the requirements of the selected ISO standards. This checklist will serve as the roadmap for the audit and ensure that all relevant aspects are examined thoroughly.

4. Training and awareness

Ensure your employees are well-informed about the ISO standards that apply to your organization. Conduct training sessions and awareness programs to familiarize staff with the standards and their implications on daily operations. It is important to identify key people (usually department heads) to prepare the documentation in case their activities are in scope.

5. Conduct internal audits

Ideally, any organization would perform internal audits regularly according to the established schedule. These audits should be thorough, evaluating compliance with the selected ISO standards. Each team would be responsible for checking its own area, which could be delegated to the compliance and risk management team if it exists.

6. Continual improvement

A crucial aspect of ISO standards is continual improvement—or the PDCA cycle: Plan, Do, Check, Act.

Compliance monitoring programs should not only focus on maintaining existing standards but also on finding ways to enhance processes and systems to meet evolving requirements.

7. Documentation and record-keeping

Accurate documentation is essential throughout the compliance monitoring and audit process. Maintain detailed records of audit results, corrective actions, and improvements made. This documentation will be invaluable during ISO audits.

8. Post-audit actions

Following external audits, address any nonconformities or observations made by the external auditors. Note that ISO findings are defined in two categories: critical and noncritical. As the name indicates, critical findings must be corrected immediately, and noncritical findings may be resolved by the next audit. Take corrective actions as necessary and ensure that all issues are resolved to the satisfaction of the auditors. A common mistake among organizations is that team heads and management commit to resolving issues while knowing they will not be able to do so (e.g., due to lack of investment in an automated solution, lack of human resources or knowledge in the team). Transparency with the ISO auditors should be a keystone of communication since any delay in resolving issues—or issues left completely unresolved—may result in the certification being withdrawn.

9. Continuous monitoring (see also, number 6!)

After achieving ISO certification, do not become complacent. Continue to monitor compliance with the standards and conduct regular internal audits to ensure that the organization remains aligned with ISO requirements.

Benefits of leveraging compliance monitoring for ISO audits

Leveraging compliance monitoring programs for ISO audits offers several benefits to organizations.

1. Enhanced legal and regulatory compliance

Compliance monitoring programs ensure that an organization consistently adheres to ISO standards. This leads to improved product and service quality, increased customer satisfaction, and reduced operational risks. Adherence to ISO standards often aligns an organization with various legal and regulatory requirements. Compliance monitoring programs can help ensure you meet these obligations, reducing the risk of legal issues and penalties.

2. Cost-savings

By identifying and addressing compliance issues, organizations also tackle ISO requirements, thus saving some costs by avoiding duplicate work (e.g., teams involved, time spent).

3. Improved operational efficiency

During the compliance monitoring process, organizations frequently identify improvement areas. Corrective actions can lead to increased operational efficiency, reduced waste, and streamlined processes—this not only benefits compliance but also overall organizational performance.

4. Risk management

Effective compliance monitoring helps identify potential risks and vulnerabilities in your processes. By addressing these issues, organizations can reduce the likelihood of quality problems, security breaches, and other adverse events that can affect your organization.

5. Customer satisfaction and access to new markets

ISO certification indicates a commitment to meeting and exceeding customer expectations. Satisfied customers are more likely to return to and recommend your products or services to others, contributing to business growth. ISO certification can open doors to new markets and opportunities, especially in industries or regions where ISO standards are highly regarded. Many organizations require their suppliers to be ISO-certified, making it a prerequisite for collaboration.

6. Employee engagement

Employees are often more motivated and engaged when they work in organizations that uphold high standards and focus on quality. ISO certification and compliance monitoring programs can foster a culture of excellence, boosting employee morale and retention.

Conclusion

In conclusion, leveraging compliance monitoring programs for ISO audits is not just a procedural requirement but a strategic choice that can yield significant benefits for your organization. These programs promote excellence, customer trust, and a culture of continual improvement, positioning your organization for long-term success in a competitive global market.

Takeaways

- Ensure the involvement of management and department heads from day one.

- Establish an internal roadmap highlighting roles and responsibilities from the beginning to the end.

- Be transparent with auditors. Good communication is key to establishing a realistic audit schedule and sticking to it.

- Make sure you understand the findings identified and their implications and don't commit to resolve if you cannot deliver.

- Don't produce documentation for the sake of it and bury the auditors! Use the documentation you already have.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login