COSMOS
Navigate the Compliance Universe

# SCCE Compliance 101 Third Edition
# Chapter 7. Monitoring, Auditing, and Reporting

An effective compliance program involves constant evaluation and improvement. To keep improving your program, risk areas need to be consistently monitored and audited. Auditing and monitoring are a compliance program's detection mechanisms. This element can assist you in finding risks that have been escalated or in detecting new risks. Additionally, this element can verify that management has put mechanisms in place to mitigate previously identified risks. A reporting system is also necessary for staff to use if they encounter instances of noncompliance and are not comfortable raising issues with management. The reporting system is the safety mechanism for an employee to feel free to raise issues without fear of retaliation or retribution. With these tools and processes in place, an organization demonstrates its commitment to continually improving its compliance program.

While an expectation of 100% compliance is an ideal goal, it is also unrealistic since organizational compliance relies on each individual's compliance and accountability. The key to strive for and *demonstrate* is a process for continually improving and evolving your compliance program and its activities. There is a strong emphasis on the importance of evaluation in most recent settlements with regulatory agencies.

The need for regular monitoring is ongoing. Management should monitor the risks of the organization and ensure that they are mitigated. Monitoring helps to identify early on if risks are escalating so that they can be addressed quickly and reprioritized when needed. Moreover, all government compliance program guidance states that ongoing evaluation is critical to a successful compliance program. Regulators (such as the DOJ) have also identified key areas they look at when evaluating the effectiveness of compliance programs.

## Auditing and Monitoring Plan

Every compliance program should have an auditing and monitoring plan, and this can be conducted by the compliance program itself or by another department in the organization. Either way, a plan should be developed according to the priority risks identified in the compliance risk assessment. If the compliance professional is not the person who develops the auditing and monitoring compliance plan, and another function is responsible, it would be good to include a narrative in the plan as to how priority risks are evaluated and how ongoing monitoring occurs. Also, it is important to focus on how compliance will be integrated into another function's process of forming and implementing the auditing and monitoring plan.

The compliance professional needs to be involved in determining how audits and monitoring processes will be conducted if the responsibility does not belong to the compliance department. Observations from those activities help compliance adapt training plans, reporting, communications, and more. It is difficult to have an effective compliance program without auditing and monitoring. These processes are key to validating compliance to policies, rules, and regulations. They are also important in identifying further action needed around risk priorities, monitoring for remediation of risks, and controls. Involvement by the compliance professional is critical, regardless of who does the auditing and/or monitoring work!

Areas of risk common to most organizations—regardless of business, size, or geography—may include the following:

- Third-party relationships

- Mergers and acquisitions
- Conflicts of interest
- Intellectual property uses and protections
- Data privacy and security
- Foreign corrupt practices (for companies crossing international borders and which are domiciled in the US)
- Antitrust
- Contract management
- Travel and entertainment

Other risks to be reviewed depend on the industry and type of organization, i.e., private, for-profit, tax exempt, or public. Some risk areas won't necessarily be the compliance department's focus, but compliance should ensure that audits occur and that issues are addressed. Examples include the following:

- Publicly traded companies should have their financial statements and supporting worksheets audited regularly.
- Tax-exempt organizations should monitor that their mission is being fulfilled and that earmarked funds are being used appropriately.
- Government contractors should ensure that illegal kickback arrangements have not been initiated.
- Food distributors should ensure that all U.S. Food and Drug Administration (FDA) regulations are being met.
- Restaurants should monitor compliance with the U.S. Department of Health's requirements.
- Banks should have the appropriate controls in place to handle money per regulatory requirements.

Any areas of concern and risk priorities previously identified, either internally or by an outside agency, should be monitored carefully and regularly. The reporting system will also identify new risks in the organization or can show trends of repeat and unresolved issues. Risks are always changing, and monitoring helps identify those changing risks. The audit and monitoring plan will be dynamic and potentially reprioritized after ongoing risk assessment occurs. For more information on the risk assessment process, see Chapter 5, "Risk Assessment."

## Audit Approach

There are at least two ways to approach auditing: *a concurrent or prospective* audit and a *retrospective* audit. Because every organization is unique, again, you must choose what is best for yours and appropriate for the specific situation. The approach will depend on the potential scope of the audit and the defined outcomes.

A **retrospective audit** provides a broad baseline risk assessment, a snapshot, or what is essentially a laundry list of all the things the organization needs to fix. However unlikely, if a government agent does knock on your door, all identified problems will be nicely itemized for them. It is optimistic at best to think that one can identify in some finite period everything that could possibly be wrong and then try to set up a realistic time frame for addressing

those problems (and absent of government timeline requirements for reporting compliance issues). Moreover, any problems identified in a retrospective audit will require not only corrective actions to ensure the problem does not recur, but also remedies to any third parties that may have been affected. It is an organization's duty as part of its compliance program to remediate any problems identified. Thus, an organization cannot merely go forward after a retrospective audit has identified past improprieties. Additionally, many enforcers will expect that if a problem was found in the past, your assessment will include going back to the statute of limitations that may apply for your audit risk and time period. Retrospective auditing is usually conducted to prove something does or does not exist, review high-risk priorities, identify baselines for large volumes of issues in a risk area, prepare for self-disclosure, or report to a regulatory agency.

A **concurrent audit** will identify and address potential problems as they arise and before they cause harm to the organization or another party. If a problem does indeed exist, then this approach allows you to immediately correct the related process and assists with identifying any policies or procedures that need to be developed or revised. Concurrent auditing is one of the best ways to change behavior. You can communicate new or revised policies to all affected parties and then go back a predetermined amount of time (e.g., to when the process changed) to review the process and its resulting documents to ensure that the problem has been resolved. It may be determined upon repeated review that further corrective actions are necessary, including disciplinary action against employees who continually fail to correct the problem after repeated retraining.

## Auditing Method

Data collection and tracking are the heart and soul of auditing (and monitoring) because they provide trend analysis and a measure of progress. Data collection and tracking can be done through various methods. Some regulatory agencies recommend that the compliance officer or reviewer consider the following techniques:

- Perform on-site visits.
- Interview personnel in management, operations, contracting, marketing, finance, and other related activities.
- Develop questionnaires to solicit impressions from a broad cross section of the organization's employees.
- Review written materials and documentation prepared by the different divisions within the organization.
- Conduct trend analyses in specific areas over a given period.
- Review internal and external complaints filed.
- Review internal audits, observations, and findings.
- Review trends and analyses of whistleblower hotline calls.
- Review regulatory activity in your industry and/or geographic market.
- Include compliance-related questions in exit interviews (responses to these questions should be reported to the compliance officer), such as:
    - How do you feel about communications in your unit?
    - How about communications overall?
    - How do you think the organization lives up to its code of conduct?

- Did you have any concerns about ethical issues or compliance-related practices? If so, please explain.

For an example of a method for tracking audits, see Appendix 8, Sample Auditing/Monitoring Review Form. For audit plan templates, see Appendix 9, Audit Review Plan Templates.

## Monitoring

Monitoring is also necessary to determine whether compliance elements, such as dissemination of standards, training, and disciplinary action, have been satisfied. It also will target potential control and system deficiencies and areas where modifications might be in order. A good starting place to monitor is to talk to the employees. Employees hold a wealth of knowledge, and they often enjoy participating in the process of improving their organization. Thus, employees may offer an unexpected amount of information. Ask them openly about risk, their daily activities, and whether their processes and procedures are sound. Ask if policies and procedures are followed. Periodically send out questionnaires to staff for feedback, or conduct focus groups. Remember to always reassure employees that the organization maintains a strict nonretaliation policy—meaning employees will not be retaliated against for reporting suspected misconduct.

Management should set up systems for regular and sometimes random reviews of documents (e.g., invoices, worksheets, notes, legal opinions, financial analyses, schedules, budgets, and expenses) to make sure policies are being following, as well as to identify any gaps or issues that have escalated.

## Auditing and Monitoring Responsibilities

Who is responsible for coordinating the monitoring or conducting the internal audit? Is this an internal auditor's responsibility, the compliance professional's responsibility, or perhaps a combination of the two? First, to avoid duplication or overlap, consider whether other departments in your organization perform audits. Try to leverage those activities for compliance, making sure they are integrated with your compliance program efforts and communicated.

Areas to consider may include:

- **High-risk business functions.** These can include supply chain, finance, IT, privacy, data protection, third-party relationships, revenue and reimbursement, quality improvement, or quality assurance activities. These functions are usually underway at all levels of the organization and can dovetail with the monitoring and auditing elements of an effective compliance program.
- **Internal *ad hoc* groups—compliance SWAT teams**. To monitor specific issues or review potential problem areas.
- **Subject matter experience in the area auditors are observing**. It is important to consider involving subject matter experts to ensure there is a good understanding of the business area being reviewed. If outside resources are used, carefully check their references to ensure auditors are credible and capable.