COSMOS
Navigate the Compliance Universe

Compliance Today - October 2018
Effective auditing and monitoring for your compliance program

by Marti Arvin

Marti Arvin (marti.arvin@cynergistek.com) is Vice President of Audit Strategy at CynergisTek, in Austin, TX.

- linkedin.com/in/marti-arvin-7a6a587

What is effective auditing and monitoring in support of an effective compliance program? There is no clear-cut answer, but it is clear that doing nothing will not get you to effectiveness. The key question is how much of something must be done? It is helpful to understand what the two terms mean. They are often used as a single phrase, but the two activities are distinctly different. Understanding what the two activities entail can help determine if what is being done supports an effective compliance program.

Auditing versus monitoring

An audit is usually a formal, structured process with a defined scope of work to evaluate controls and determine if a process is functioning as expected. An independent, objective, and knowledgeable third party should perform it. The scope of work would generally define what controls are being tested, the universe from which a sample is being identified, the method for randomly selecting the sample, and the size of the sample that will be evaluated. It might also include a background regarding why the audit is being performed and the identified references and resources used in support of the audit.

Some organizations refer to activity under this element of the compliance program as "reviews" rather than audits, because they recognize what they are engaged in does not have the structure and formality of a true audit. The important factor is to understand the difference in the terms and use them appropriately.

Monitoring does not have the same requirement for independence and objectivity that auditing does. Monitoring is something that can be performed by the Compliance Office as an independent party, but it can also be a self-assessment performed by the business operations unit. Monitoring is often conducted on a more routine, less formal basis than performing a review or an audit. For example, there may be a requirement that all clinical areas complete a self-assessment of coding and documentation practices by selecting ten claims a month and evaluating the accuracy and completeness of the coding and documentation for those services. Because the business unit that performs the work conducts the monitoring, it cannot be considered an independent and objective assessment. That is not to say that the person performing the monitoring will not do a thorough and complete job — it is simply a recognition of the inherent conflict of interest in having someone involved in the process also evaluate the process.

Now that the terms are defined, what are the next steps? The key to effective auditing and monitoring will encompass a number of factors. Key among those are:

- Conducting an effective risk assessment and risk prioritization for the organization,
- Identifying resources to conduct auditing and monitoring activities around the high-risk items, and
- Actually performing the auditing and monitoring activities.

The risk assessment process and risk prioritization

The buy-in of senior leadership and business unit leaders is critical to conducting an effective risk assessment. The compliance officer will be able to identify a number of risks the organization has and provide input into the priority of those risks, but the ultimate decision regarding the risk tolerance of the organization lives with the senior leadership and governing body. There may be risks the compliance officer is not aware of, and even for the risks known by the compliance officer, there may be compensating controls that would impact the overall priority of addressing such risks.

Compliance may drive the risk assessment process, but the final outcome — a prioritized list of the organization's risks based on the likelihood of the risk occurring, the consequences if it occurs, and mitigating factors (e.g., compensating controls) — must be determined by the governing body. This final list will be the road map to the auditing and monitoring program. Rarely does a compliance program have the resources to address all risks but, ideally, the organization will provide sufficient resources to address the highest risk. The decision on which risk will be addressed through the auditing and monitoring program should be formalized in the minutes of the oversight body for the compliance program. It should be clear that the governing body was made aware of the risks, made the final decision regarding which risks would be addressed, and how they determined which resources they would use to address them. If the risk assessment identifies ten high-risk items, but the resources are not available to address all ten, it is important that the governing body is clear on the potential consequences of not addressing each risk or providing support to obtain the resources.

A mistake made by some compliance professionals is to attempt to address all the high priority risk items with the resources available, if their governing body is not willing to support additional resources. This approach can have multiple negative consequences. It can lead to staff burnout because of overwork, sloppy work because of the pressure to complete more audits and reviews than feasible, and/or a continued unwillingness for the governing body to provide resources if they perceive the risks are being addressed.

Compliance professionals should be very clear to the governing body that if they choose not to provide sufficient resources to address the highest priority risks, those risks will not be part of the annual auditing and monitoring work plan. Decisions on risk tolerance should be left to the governing body. The compliance professional may have to fight the inherent natural desire to assure all the high-risk items are addressed in the interest of protecting the organization.

The risk assessment process may be a joint effort with other business units, such as Risk and/or Internal Audit. Not only does this get Compliance the input of these business units, but it also means Compliance will not be standing alone in presenting the risks to the governing body. It also allows for the coordination of efforts that may result in a more efficient use of resources to address more risk areas.

When identifying risk, most organizations will take into account a number of resources. The Office of Inspector General (OIG) Annual Work Plan[1] is one such often-used resource — but it should not be the only resource. Looking at other program integrity and enforcement activities of any regulatory body that has oversight for activities performed by the organization will be important. There can be a multitude of these in addition to the OIG. Those of interest to the organization will depend on the nature of the organization and the laws and regulations it is subject to, but they may include the Office for Civil Rights (OCR), the Food and Drug Administration (FDA), the Office for Human Research Protections (OHRP), and the Department of Justice (DOJ), just to name a few.