Compliance Today - September 2022
Risk assessments: Why, what, when, how

By Christopher Tonellato, JD, CHC, and Sarah Couture, RN, CHC, CHRC

- linkedin.com/in/chris-tonellato-a65971129
- linkedin.com/in/sarah-couture-rn-chc-chrc-367a4390/
- @SarahCompliance

A compliance program can only be truly effective at accomplishing its goal of preventing and detecting fraud, waste, and abuse when the program, its infrastructure (i.e., the seven elements), and the work the program does (i.e., the compliance work plan) are oriented around the organization's compliance risk profile.[1] To best prevent fraud, waste, and abuse, it's logical to focus on those issues where fraud, waste, and abuse are most likely and where the consequences of noncompliance are the most significant. Why would a compliance program spend its, oftentimes, small number of resources on issues that are not as crucial to get right? Nevertheless, compliance programs have not always understood, nor prioritized, risk assessment, leading to ineffective and inefficient efforts not oriented around the organization's most significant compliance risks.

Implementing an effective compliance risk assessment approach is beneficial in multiple ways. It is the most efficient and effective way to ensure that the compliance program spends its time and resources on the appropriate issues (to best prevent and detect fraud, waste, and abuse). It also helps ensure that operations leaders and managers understand compliance risk and the importance of operations' responsibility for compliance. Effective compliance risk assessment, management, and mitigation promote an engaged and aware culture throughout an organization and is a best practice that has become a requirement in recent corporate integrity agreements (CIAs). Risk-based compliance programs promote the highest level of service for employees and patients and help ensure proactive compliance programs. Perhaps the most compelling reason to provide an exceptional risk assessment approach is that it can be protective in cases of wrongdoing. The Department of Justice *Evaluation of Corporate Compliance Programs* states, "Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction."[2]

While every organization's risk profile is unique, there are certain common healthcare-specific industry risks, especially when narrowed to healthcare providers, that these organizations have in common. These shared industry risks include, but are not limited to, state and federal statutes and regulations, matters seen in recent enforcement actions, Department of Health & Human Services Office of Inspector General (OIG) reports and work plan items, government audit priorities, changing regulatory priorities, and certain broader state and national issues such as "the great resignation" and pandemic-related concerns, among others. An organization's risk profile becomes further customized when adding internal risks or those particularly applicable to the organization. These may include, but are not limited to, organizational structure and legal relationships, the control environment, the culture of compliance and accountability, operations' engagement with compliance, specific issues reported to management or compliance, specific investigation outcomes, and specific audit findings.

Essential concepts in compliance risk assessment

There are several essential concepts to consider when developing an approach for compliance risk assessment.

Maintenance of an ongoing, dynamic compliance risk profile

For practical and logistical purposes, it is essential to designate a specific time during the year to perform the risk assessment (see further discussion later). However, it is also necessary to establish processes to ensure the risk assessment is kept up to date throughout the year. Both the regulatory landscape and healthcare organizations themselves are dynamic, constantly changing, and need to adapt to those changes when needed. Therefore, risk assessments must be able to reflect changes in the risks themselves and their prioritization. This can be accomplished by staying abreast of external activity (e.g., new enforcement actions and regulatory changes), responding to internal changes (e.g., reports to compliance, audit findings, or investigation results), and considering the concerns of risk area/operations leaders and managers, etc. Operational leaders and managers, as well as the compliance program team, should be involved in these ongoing discussions, perhaps through a compliance committee, whether monthly or quarterly. Also, keep senior leadership and oversight committees or the board updated on developments and changes made to the risk assessment.

Operations engagement

Just like the compliance program cannot be successful in a silo, the compliance risk assessment process will not be as effective without the input and collaboration of operations partners. Leaders and managers in operational risk areas, such as privacy, billing and coding, physician practice, clinical research, human resources, supply chain/procurement, etc., are (or should be) experts in that subject matter and should have significant, productive, and essential perspectives to consider in the compliance risk assessment. If the compliance program staff performs the risk assessment without this input, it is likely that certain risks will not be considered or that the prioritization will not be as accurate.

Before engaging risk area partners in the risk assessment, ensure they have a strong understanding of compliance, why risk assessment matters, and how their perspective is necessary for the organization and the effectiveness of the compliance program. Educate these operational partners on why compliance risk matters, the risk assessment process, how compliance work needs to be based on the entire organization's compliance risk profile, and their role in the process. This collaboration works best when operations leaders and managers are engaged in compliance and understand their compliance responsibilities.

Once operations partners are educated on the background and engaged in the process, solicit their input for the most impactful risk assessment. Seek operational risk area perspectives on what risks should be considered in the risk assessment. Collect their responses via in-person interviews, surveys, and/or compliance committee meeting discussions. In addition to ensuring input into what risks should be considered, compliance should collaborate with operations on risk ranking and prioritization. Seeking risk area leaders' and managers' perspectives on the risks' impact, likelihood, controls, etc., helps ensure a well-balanced and more accurate prioritization, and also promotes operations' engagement with the compliance program and their compliance responsibility. Partnering on ranking prioritization can occur with a smaller group of operations partners, perhaps each working independently on ranking, and/or in a larger group discussion setting such as with a compliance committee.

Once risks have been gathered and prioritized, ensure senior leaders are informed and engaged with the process, and seek their input on the completeness of the risks considered as well as their perspectives on appropriate prioritization.

Tie program activity to prioritized risks

As discussed in the introduction, compliance priorities should be tied to prioritized risks to most effectively prevent and detect fraud, waste, and abuse. The risk assessment should drive where compliance focuses time and resources, where compliance seeks to understand the control environment, where audits are performed, where and how operations are engaged, etc. The most straightforward way to accomplish this is to translate the highest-ranked risk areas, per the risk prioritization, into the compliance work plan. The compliance work plan maps out compliance program areas of focus and audits for the year, often by quarter, and should be oriented around the organization's most significantly ranked risks. Furthermore, the compliance officer should ensure that the development and implementation of the seven elements themselves consider the organization's risk profile.

Staffing and resources

While compliance professionals often know that the compliance work plan should be oriented around the risk profile, not all compliance programs think to tie the compliance program staffing and resources to the risk profile. While we have staffing and resource benchmarks, such as the HCCA's *Healthcare Industry Compliance Staffing and Budget Benchmarking and Guidance Survey*,[3] to evaluate program resources, these reports consider only employee count and revenue, so they are relatively risk-agnostic. A savvy compliance program will consider both the benchmarking reports as well as the organization's specific risk profile to ensure the compliance program is adequate for the size and complexity of the compliance program, as well as the best skill sets to include on the compliance program team. *Practical Guidance for Health Care Governing Boards on Compliance Oversight* states, "the complexity of the organization will likely dictate the nature and magnitude of regulatory impact and thereby the nature and skill set of resources needed to manage and monitor compliance."[4] Program resources including staff quantity and expertise, time allocation, budget needed, and other resources should be appropriately prioritized and allocated based on the compliance risk profile. In other words, organizations should be able to explain what resources are necessary to best prevent and detect fraud, waste, and abuse specific to their risk profile.

Scope of the risk assessment

While this discussion is specific to compliance risk assessment, it is important to understand what other risk assessment activities may be taking place in your organization. Many organizations have adopted an enterprise risk management (ERM) approach to assessing, prioritizing, and mitigating organizational risk, with compliance risk being a domain of the overall organizational risk profile. In organizations with a mature approach to ERM, compliance should work within the ERM risk assessment and framework to best understand and prioritize compliance risk. Alignment across the organization of risk assessment activities can increase effectiveness and reduce redundancies.

Communication

Compliance program communication to the organization should be oriented around the risk profile. Focusing communication on the most significant risk areas will help prevent fraud, waste, and abuse.

The compliance officer should ensure that both leadership and the board of directors understand the organization's risk profile and how the compliance program is oriented to address prioritized risks. Additionally, the compliance officer can use the framework of the risk profile to help determine what information is most important to share with leadership and the board of directors. Compliance officers sometimes struggle with what types of information and what level of detail should be shared in leadership and board reports. Orienting communications around the risk profile can both aid the compliance officer in prioritizing what and how to report and help with leadership engagement and the board's oversight responsibility.