COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual
Risk Assessment and Management

By Jeffrey Driver,[1] JD, MBA, MSc, CHC, CHRC, CCEP-I, CHPC, DFASHRM; Steven Ortquist[2]; Judith W. Spain,[3] JD, CCEP; Stephen Martin[4]; Toby Ralston[5]; Andrew T. Wampler[6]; and Jose Tabuena[7]

Conducting an effective risk assessment is an essential first step to developing a strong compliance program, as well as an essential operating process for managing the ongoing inherent and emerging risks that every business will face. An effective risk assessment framework and process, among other things, helps organizations identify direct and indirect compliance hot spots that when used in combination with technology and data analytics, can pinpoint unknown or unwanted trends in order to maintain an effective compliance program.

Regularly conducting a comprehensive risk assessment is recognized as one of the key elements of an effective compliance and ethics program. More broadly, as regulators have emphasized the importance of effective risk management, boards and management teams have increased their focus on the concept of "risk" and have observed a measurable shift on this focus at their organizations. By understanding the nature and the impact of the risks an organization faces, it is expected that an organization can better design programs and develop controls to mitigate those risks.

Performance of risk assessments often fall under the discipline of *risk management*, where organized frameworks and techniques have emerged. Risk management, in its most elemental form, comprises the identification, assessment, and prioritization of risks followed by the coordinated and efficient use of resources to monitor, mitigate, and otherwise control the probability and/or impact of the risks occurring. Broadly, organizational risks arise in many forms from the board room to the storeroom and everywhere in between. Examples include uncertainty in financial markets, operational failures, third-party risks, and natural disasters, to legal liabilities and reputational harms, and even missed opportunities (known as the "upside" risk).

More than ever there are areas of overlap between risk management and compliance. Risk management has become even more integrated into organizational processes and hardwired into various laws, rules, and regulations since the beginning of the 2008 financial crisis. So, the failure to have a risk assessment process may now itself represent noncompliance for many modern organizations. Some companies in the financial services industry have gone so far as to merge the two areas so that their related activities are better coordinated, though many are of the view that the disciplines have quite different skill sets and simply need to work more closely together as managers of risk.

The U.S. Department of Justice (DOJ) updated its guidance for federal prosecutors in 2020 on how to evaluate an organization compliance program when making charging decisions or sentencing recommendations. DOJ emphasized the importance of a robust risk assessment process in assuring that a compliance program was designed and operating to effectively mitigate compliance risks:[8]

> The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand…how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.[9]

DOJ guidance goes on to cite the following areas that prosecutors should consider as they evaluate the extent to which a company has appropriately assessed its risk profile and designed a compliance program to mitigate identified risks:

> **Risk Management Process:** What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?
>
> **Risk-Tailored Resource Allocation**: Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas…? Does the company give greater scrutiny, as warranted, to high-risk transactions…than more modest and routine [activities]?
>
> **Updates and Revisions**: Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?[10]

As legal, compliance, and ethical risks are a major subset of the overall risks faced by an organization, it is essential for compliance professionals to be aware of risk management techniques, particularly those used in the industry sector in which the compliance professional works. Risk-management components and the role of risk managers vary by industry, the size and structure of the organization, as well as the risk financing strategies employed by the organization. Similar to the field of compliance and ethics, the risk management profession has evolved along functional needs and growing regulatory mandates.

Risk assessments are a proactive and preventive measure that should be a regular and systemic part of an organization's compliance efforts. If the organization does not have a compliance program in place, a thorough, enterprise-wide risk assessment could be conducted as a first step in identifying potential areas of compliance risk and exposures.

Why Conduct Compliance Risk Assessments?

For the compliance professional, the risk assessment is both the foundation upon which the program is built and the lens through which it can be evaluated on an ongoing basis. As a fundamental tenant, an organization cannot design an effective compliance and ethics program without first thoroughly identifying the laws and related standards with which it must comply. Moreover, periodic compliance risk assessments enable the organization to establish priorities that permit the most targeted and efficient use of compliance program resources.

Benefits of a compliance risk assessment include:

- Providing an early warning process for detecting compliance and ethics threats
- Mitigating and controlling identified problem areas, rather than having them discovered first by regulators, investors, potential acquirers, buyers, the media, or potential plaintiffs
- Prioritizing compliance and ethical risks and strengthening related existing controls; or developing of new

controls to mitigate priority risks

- Revising ethics and compliance policies, training, auditing, and initiatives that require attention
- Improving decision-making by providing managers with critical information on compliance risks, as well as mitigation and control strategies
- Demonstrating to regulators a proactive approach to compliance and thereby meeting a due diligence element of an effective compliance and ethics program

The U.S. Federal Sentencing Guidelines (FSGO) explicitly include risk assessment within the definition of an effective compliance program. Although commentators believed that the importance of performing a risk assessment was already implicit in the original definition of an effective program, the Advisory Group appointed by the U.S. Sentencing Commission intended to make clear that: "risk assessments need to be made at all stages of the development, testing, and implementation of a compliance program to ensure that compliance efforts are properly focused and effective."[11]

Thus, to obtain the benefit or credit for an effective compliance program (and the reduction in the organization's culpability score) the revised U.S. Federal Sentencing Guidelines mandate the performance of periodic risk assessments in order for the program to be considered effective. Specifically, the amended guidelines state that: "The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each (of the components of an effective compliance and ethics program) to reduce the risk of criminal conduct identified through this process."[12]

Additionally, the guidelines comment that organizations must: "Prioritize periodically the elements of the program in order to focus on preventing and detecting the criminal conduct identified in the risk assessment process as most likely to occur."[13]

These provisions in the guidelines put forth the foundational insights for the performance of the well-designed compliance risk assessment. A well-designed risk assessment often precedes all other steps in the establishment of the compliance program to help assure that program efforts are properly focused. How would you know what policies, training, auditing, etc., are needed without an assessment of the compliance risks? Further, while a risk assessment is a good starting point, it clearly is not a one-time event and must be conducted periodically as a comprehensive assessment in order for the program to adapt to changing business and regulatory conditions. The frequency of comprehensive risk assessments is determined in part by risks the organization is managing, but in practice should be conducted on an annual basis.

Proactive organizations will try to undergo risk assessment activities before an organization sets its budget, so that funding decisions can be driven in part by needed risk-mitigation strategies. In order for the program to remain effective, the risk assessment must then be integrated into the organization's overall compliance program and company processes on an ongoing basis. This may sometimes mean interim or focused risk assessments to evaluate the effect of mitigation strategies and to assure accurate, ongoing measurement of organizational risk.

The U.S. Department of Health & Human Services (HHS) Officer of Inspector General (OIG) developed a series of documents outlining compliance program requirements aimed at numerous entities supporting the healthcare and delivery system, which were modeled after the FSG. As an example, among other compliance program elements, the Centers for Medicare & Medicaid Services (CMS) requires organizations offering Medicare Advantage (MA) and/or Part D benefits to establish and implement an effective system for routine monitoring

and identification of compliance risks.[14] Subregulatory guidance requires policies and procedures to conduct a formal baseline assessment of major compliance and fraud, waste, and abuse risk areas, such as through a risk assessment. The assessment has to take all Medicare business operational areas into account. Each operational area or department must be assessed for the types and levels of risks the business operations presents to the Medicare program, and to the organization.

Responding to the question of "how" to do an assessment can be more of a challenge. The agency does not specifically outline how an organization must conduct the assessment. However, suggestions are made by CMS regarding the factors for considering risks, such as size of the department, complexity of the activities conducted, and past compliance issues. Additional factors can and should be included, based on an organization's past experience and the knowledge of the experience of other organizations in similar business within its industry. Armed with a range of factors, an organization may estimate organizational compliance risks using a wider lens. These factors include:

- **Beneficiary impact**: How do the operational area's activities impact the health, wellness, and finances of Medicare beneficiaries and Medicaid recipients?
- **Experience of the staff**: Has an operational area experienced recent or significant turnover? Has a change in management or other restructuring occurred in the last 12 months?
- **Division responsibilities**: Does the operational area work on the Medicare line of business only or on other lines subject to different regulations, such as Federal Employees Health Benefit Program, marketplace plans, and/or Medicaid?
- **Vendor support**: Is an operational function shared with or supported by a vendor? Is the function performed entirely by a vendor?
- **Enrollment growth**: Has recent enrollment growth affected an area's ability to perform its function?
- **Agency audit protocol**: Is the operational area a focus in the most recently published government audit protocol?

Scope of the Assessments

A strict reading of the U.S. Federal Sentencing Guidelines would appear to limit the focus of the risk assessment to possible "criminal" conduct. The commentary to the amended guidelines states that the organization should identify the *criminal* conduct that might occur considering "the nature of the organization's business."[15] The organization is to further consider "the prior history of the organization" and the legal violations highlighted by government regulations.[16]

Although the guidelines focus on criminal conduct, most organizations take the prudent view that a broader range of compliance and ethics risks must be examined, including those that affect civil liability, regulatory exposure, business ethics or conduct, and the organization's reputation.[17] Essentially, a key step in conducting the compliance risk assessment will be establishing a working definition and shared understanding in the organization of what constitutes a compliance risk.

Extending the risk assessment beyond exposure to criminal conduct is essential, as legal mandates can be ambiguous and cumbersome, especially in highly regulated industries. When employees understand how the company's ethical values apply in gray areas, they are more likely to align their behavior in an appropriate manner.

Examining ethical factors and reputational impacts can demonstrate the organization's commitment to ethical business conduct by providing support and guidance when employees are unsure what to do. By emphasizing the commitment to ethics as well as technical compliance, the organization is affirming that *how* business is conducted is just as important as the business itself. Such an approach is further supported by the U.S. Federal Sentencing Guidelines' emphasis, when the guidelines were amended in 2004, on the importance of promoting "an organizational culture that encourages ethical conduct and a commitment to compliance with the law."[18]

A compliance risk assessment should therefore, at a minimum, involve the assessment of information concerning risks of:

- Criminal misconduct
- Legal liability arising from failure to adhere to legal and regulatory requirements (both civil and criminal)
- Ethical lapse
- Reputational harm

Compliance Risk Assessment vs. Compliance Program Assessment

A compliance risk assessment is not intended to serve as an audit or investigation, although issues and circumstances that require a deeper examination may be brought to light from the process. A compliance risk assessment is not a financial or operational audit, though it can be incorporated with these other processes. Most importantly, a compliance risk assessment should also not be confused with a compliance program assessment/audit, although the objectives and activities of both exercises can overlap. Here is how to keep these two assessments distinct from each other:

- **A compliance program assessment/audit** is a comprehensive review of compliance *processes and activities* to assess the overall impact and effectiveness of the compliance program. A program assessment/audit can include a risk assessment, especially if one has not been performed before. Such an instance often involves a baseline effort to identify the range of compliance obligations and ethical risks the organization faces in order to determine if those obligations and risks are being addressed.
- **A compliance risk assessment** more specifically involves the identification and evaluation of a *company's compliance risks*, assessing their significance based on likelihood and impact, current and desired level of mitigation controls, and the acceptable level of risk (risk tolerance) in line with the organizational risk philosophy (risk appetite).

A compliance program assessment/audit necessarily will overlap with a compliance risk assessment, because the organization cannot assess risks without understanding how well its compliance program is mitigating them; and conversely one cannot measure compliance program effectiveness without reference to the identified risks.[19] Therefore, a program assessment/audit should include a review of

compliance risk assessments that have been completed as well as the process by which they are performed. And findings from the compliance risk assessment should be evaluated to determine if the results have been used to improve or design/redesign compliance program elements and the overall state of compliance in the organization.

Enterprise Risk Management (ERM) Initiatives and Other Risk Assessments

Compliance risk assessments, when performed from a compliance and ethics perspective, do not delve into the full range of business and operational risks of an organization. But as noted, risk management has taken on more importance in the corporate environment, spurring more risk assessment-type activities across organizations. The compliance and ethics professional should be cognizant of other risk assessment initiatives that may be taking place within the organization.

Following on from Sarbanes-Oxley regulations, many elements of risk assessment such as compliance and internal controls, regular risk assessments, along with the ranking and mapping of findings and results began taking place within various business functions. This encouraged business functions, each with its own business function owner (e.g., manager), to evaluate its specific risks and contribute to a comprehensive understanding of the organization's overall risk profile.

Because compliance risks touch so many areas of the enterprise, organizations should consider integrating when possible the compliance risk assessment into an existing enterprise risk management process. Studies have suggested that while formal risk assessments have become common, companies initially did not undertake them in an integrated manner, and when they did so, did not address compliance- and ethics-related risks in adequate depth.[20]

One obvious benefit of an integrated approach is consistency and uniformity with respect to terminology, criteria, process, and the risk information that is collected. When risk assessments are conducted separately by different business units, the use of different frameworks can result in the need and cost for reconciling the information collected across the organization. Integration can lead to a better quality of risk-based information upon which strategic and tactical decisions are based.

Integrating the compliance risk assessment with other business processes can enhance its outcomes and observations, given that ethics and compliance concerns as a practical matter filter into every department and operation. Conducting enterprise-wide compliance and ethics risk assessments in conjunction with financial auditing, manufacturing, marketing, sales, IT, and other business functions, ensures that a more complete range of risks is identified and correlated to ethics and compliance concerns.

Other advantages to a holistic enterprise risk assessment and management approach include:

- Efficiencies gained as risk issues and operational processes often overlap.
- More effective mitigation strategies can be developed if process interdependencies are understood.
- A comprehensive view of risks that face the organization and therefore, a resulting comprehensive prioritization of mitigation and management controls to address the key risks identified.

An integrated approach can also foster an organizational culture that ethics and compliance is central to an organization's activities, rather than as a stand-alone program that may be perceived as outside of mainstream organizational concerns (sometimes referred to as a "siloed program").

There are some operational shortcomings to be aware of and correct for when blending the compliance and ethics risk assessment into a broader enterprise- wide effort:

- Compliance and ethical risks may not be as obvious as operational risks and therefore may receive less attention from the majority of those involved.
- Evaluation of compliance risks utilizing the same metrics used for evaluation of business risks may be misleading and should be carefully considered as a combined risk assessment is conducted. For example, the financial exposure resulting from failure to properly manage a legal or regulatory requirement may be outstripped by the reputational damaged caused by the failure. The compliance professional should assure that these differences are understood and accounted for in context of an enterprise approach to risk assessment and management.
- Involvement by the compliance unit in an enterprise assessment led by the risk department may require more time, participation, and resources from program staff than when driving the assessment from purely a compliance and ethics perspective.