COSMOS
Navigate the Compliance Universe

HCCA Compliance 101, Fifth Edition
Chapter 6. Risk Assessment

Risk assessments must be dynamic and ongoing: *dynamic*, to address the changing risks of the organization, and *ongoing*, to continually review and prioritize the existing risks and assess emerging risks of the organization. After your initial focus on infrastructure (the framework of the seven elements), conducting a risk assessment assists you in understanding the cultural variables related to risk. These include risk tolerance and risk appetite within the organization. Understanding your cultural norms and expectations related to management accountability to resolve or mitigate risk is critical to know *before* conducting a risk assessment. If the culture is unprepared to own and resolve risks, it is a priority focus for your program to address that issue before conducting a risk assessment.

Risk assessments help identify priority risk areas to target when building the compliance program's education, auditing, monitoring, and communication plans. This is an essential process for launching an effective compliance program. A baseline risk assessment forms the foundation of a new compliance program. The dynamic nature of an organization and its risk portfolio requires an ongoing look at priority risks to keep the program aware of real, potential, and emerging risk areas that need to be monitored and addressed.

Chapter eight of the Federal Sentencing Guidelines suggests that organizations conduct ongoing risk assessments.[1] Additionally, the HHS OIG reinforces the need for a dynamic risk assessment process in its enforcement agreements with organizations. This process involves ongoing risk area reviews, with results incorporated into its compliance prioritization of organizational risks.

Baseline Compliance Risk Assessment

After completing the initial infrastructure design, the next step in launching an effective compliance program is conducting a baseline compliance risk assessment of the organization's operations. A baseline compliance risk assessment is the starting point for understanding the compliance risk profile of an organization. It can be used to compare the risk environment of the organization at one point in time with another point in time. This baseline information helps provide an indicator of whether progress has been made in minimizing or resolving identified risks. Also, as you review risks dynamically and on an ongoing basis, you will be able to compare findings with the baseline risk assessment to identify new risks.

Consider current risk assessment activities already occurring in the organization when developing processes for conducting the baseline compliance risk assessment. The compliance officer should not duplicate efforts around this process. If other functions are performing risk assessments, leverage those processes and either join their efforts or ensure they have compliance-related content included, participate in discussions about process, and discuss receiving the report of their outcomes. Also, leverage other functional activities that gather risk information, such as internal audit risk assessments, quality risk assessments, and security risk assessments.

Dynamic/Ongoing Risk Assessment

Established programs should conduct ongoing risk assessments to identify new or emerging risks or evaluate if risks may have escalated since the baseline risk assessment was conducted.

The methodology for ongoing risk assessments can vary depending on the organization's capacity and available

resources. Ongoing risk assessments can be performed throughout the year as a mini-version of the annual or initial program baseline risk assessment. These risk assessment activities could include using baseline results and interviewing management to identify any areas that have escalated, been resolved, or have emerged since the last assessment activity occurred. Frequency of conducting the ongoing risk assessment also varies according to capacity and resources available. However, it is recommended to review the previous results against the current state at least once or twice during the year to ensure that compliance program elements are continually addressing the organization's key risk priorities and to minimize any surprises.