COSMOS
Navigate the Compliance Universe

Compliance Today - October 2023

Jessenia Cornejo
(jessenia@labinsightsllc.com, linkedin.com/in/jessenia-cornejo/)
is Senior Quality & Compliance Consultant for Lab Insights LLC, Carlsbad, CA.

Brittani Summers
(brittani@sprinterhealth.com, linkedin.com/in/brittani-summers/)
is Senior Compliance Manager at Sprinter Health, Menlo Park, CA.

How to develop an effective risk management program

by Jessenia Cornejo and Brittani Summers

As compliance professionals, we hear (and talk) a lot about risk and the importance of risk assessments in an effective compliance program, but it hasn't always been exactly clear where one should start. We will review the value of risk assessments and go through steps on how to establish a risk management platform that allows for continuous monitoring and re-evaluating of a process for addressing and mitigating risk.

What is risk?

If we're going to be assessing and managing risk, we need to first understand what risk is. Compliance risk generally involves the risk of violations of laws and regulations, but it may also address contract terms, professional standards, organizational policy, and ethics matters. Compliance risks can vary by industry and from organization to organization.

Some of you may be familiar with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Framework, which is used to help organizations identify and manage risks at an enterprise level. The Health Care Compliance Association (HCCA) & Society of Corporate Compliance (SCCE) partnered with COSO and published a guide on applying COSO's ERM framework to compliance risk management, and is based on current practices and expectations for effective compliance and ethics programs and aligns these practices with the COSO framework.[1]

Why is risk assessment important?

Regularly conducting a comprehensive risk assessment is recognized as one of the key elements of an effective compliance program. In fact, it's often said to be the eighth element of an effective compliance program as it forms the basis for determining how risks will be managed. By understanding the nature and impact of an organization's risks, the organization is expected to better design programs, develop controls to help mitigate those risks, and continually look for ways to improve compliance programs.

Government bodies and enforcement agencies also recognize and emphasize the importance of risk assessments. Risk assessments are intended to be preventive as they identify existing risks or program gaps, therefore showing regulators a proactive approach to compliance. You may also notice that most of the seven elements of an effective compliance program[2] are driven by your risk assessment.

The U.S. Department of Justice's (DOJ) *Evaluation of Corporate Compliance Programs* outlines key issues prosecutors consider when assessing the adequacy of corporate compliance programs during charging and settlement decisions. DOJ emphasizes that it's not enough to have a compliance program in place; it must be effectively implemented. There is language around risk assessment and management, specifically where prosecutors look at what companies are doing to assess and address their identified risks and design appropriate controls to manage these risks. A constant theme from DOJ is that compliance programs should be company-specific, and tailored to the company's risk profile and specific business needs.[3]

Measuring compliance program effectiveness is recommended by several authorities, including the U.S. Department of Health and Humans Services Office of Inspector General (OIG), DOJ, and the United States Sentencing Commission.

The OIG–HCCA's *Measuring Compliance Program Effectiveness — A Resource Guide* incorporates the elements of effective compliance programs and provides several ideas for measuring the various elements of a compliance program, including risk assessments.[4] Each element includes examples of what and how to measure. Organizations of any size, industry, and operational complexity can use this guide and tailor it to their specific needs.

The United States Sentencing Commission Guidelines § 8B2.1 requires organizations to establish standards and procedures to prevent and detect criminal conduct, more precisely defining the oversight responsibilities of the organization's governing authority and providing an outline of organizational expectations regarding a compliance and ethics program.[5] One of those expectations is that organizations perform risk assessments periodically, consider the nature, seriousness, and likelihood of occurrence, prioritize the actions taken, and modify as appropriate.

As you can see, the government is a big supporter of risk assessments, and their guidance indicates the significance of having performed and documented assessments.