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.

Risk assessment versus risk management

So, we know that a risk assessment includes identifying, analyzing, and evaluating the severity of risks.

Understanding that a risk assessment is not the final stop is important. Once you identify the risks, then what? Some action must be taken, right? Once we know what they are, how are we going to *manage* them?

That brings us to risk management—managing the risks that have been identified. Risk management includes ongoing review and management of risk. For example, what are you doing about known risk areas? Are your risks changing over time? Performing these steps helps determine the best way to address those risks: to monitor, minimize, or mitigate their impact.

Identifying your risks

To identify risk areas, start by considering your business operations. What are your industry's/organization's requirements? You want to be able to speak to whether something is a risk, so be familiar with the goods/services the company offers. Offering a new product or service may also present new risks.

Consider any of the requirements and regulatory standards that apply to your organization. What industry guidance is available? What are the enforcement trends in this industry? You can always refer to the OIG Work Plans, Advisory Opinions, and Special Fraud Alerts.

You may also get insight into your company's risks by interviewing your leadership team to see what they consider are risk areas.

You can also lean on risk assessment tools/resources that are available. HCCA & SCCE has risk assessment forms and tools available in COSMOS, their online publications platform. As mentioned previously, there is the COSO framework, HCCA & SCCE's publication on applying the framework to compliance risk management, and HCCA–OIG's *Measuring Compliance Program Effectiveness Guide.* Any of these resources can be tailored and applied to your organization.

As you identify the risk areas, some things to consider are internal resources (like your team, other departments) and bandwidth. Bandwidth will play a role in determining the scope and frequency of your assessments and action plans.

Here are some examples of some common risk areas in healthcare:

1. **HIPAA violations** of privacy or data security laws can lead to a breach or theft of personal information.
2. **Billing issues** may arise where services are billed but not provided or are not reasonable/necessary, and improper billing may result in fraud/refunds and other penalties.
3. **Conflicts of interest** may compromise a person's judgment in making business decisions, their ability to carry out job responsibilities, or the delivery of patient care.

Assessing and prioritizing your risks

We've identified our risk areas. The next step is to assess the risk and prioritize. When assessing identified risks, you want to consider the likelihood and the impact from various perspectives.

How likely is it that each risk will occur? For example, consider whether existing policies are in place to currently address a risk area. If not, it may mean that it's more likely to occur. If policies and training are in place, it may be less likely to occur. Policies, procedures, and training are examples of safeguards that are intended to mitigate the risk from occurring. What is the impact on the organization? Will it impact the organization from a legal/compliance, health/safety, financial, strategic, operational, and/or reputational perspective? By considering likelihood and impact, one can determine a risk score that will help prioritize the risks.

There is a possibility that your risk assessment identified a high number of risks. While you may not be able to address all identified risks at once, by prioritizing them, you can start by addressing those with the highest likelihood and impact on the organization. Use a scoring system to assign a risk score that can be used throughout your risk assessment.

HCCA & SCCE's *Compliance Risk Management: Applying the COSO ERM Framework* provides examples on assigning the likelihood of occurrence, as well as determining a level of impact.[6] Once you determine a likelihood and impact score, you could chart it on a matrix for a visual representation of the severity of your risks, or you might multiply the numbers together to assign a risk score.

When it comes to a scoring system, there is no right or wrong way to do it as long as you apply scoring consistently and uniformly and are able to speak to the scoring method that you use. There are tools to help quantify and document the risk level.

Returning to our examples of common risk areas, let's focus on HIPAA violations to determine a risk score to prioritize our risk and action plans.

If you were to assess and prioritize the risk associated with HIPAA violations at "ABC" organization, then consider this information. What if ABC organization had over 20 HIPAA breaches and no training program? How would you score the likelihood? This is a good example of a high-priority risk area due to the circumstances surrounding this risk and the high likelihood of a HIPAA issue or incident occurring in the future.

Mitigating your risks

Once your risk assessment is complete and your risk areas are identified and prioritized, your organization can move forward to mitigate those risks.

Consider what safeguards you can implement at your organization, such as checks or measures within processes. Some examples are policies and procedures, client or physician agreements, and employee and/or board of directors (BOD) training. Policies and procedures can be a safeguard as it's a resource employees can go to at any time to ensure they abide by and understand the steps of a process or how to adhere to a policy.

Another safeguard can be creating a risk dashboard (in a system appropriate for your organization) where all or some risks are displayed and measured. This can allow you to identify issues in real-time.

How can you determine which safeguards are appropriate for your organization? Learning resources are available which can give you ideas on mitigation steps. For example, corporate integrity agreements (CIAs) are publicly available through the OIG website, and HCCA & SCCE have an extensive list of available webinars or publications.

In addition to resources, you can collaborate and partner with other leaders within your organization or network. You can pick their brains on what they may be doing already within their departments to mitigate their departments' risks; then, you can use that idea and incorporate it into your compliance program.

In our previous example, you can mitigate the risks associated with "ABC" organization's HIPAA issues by creating and implementing employee training, a HIPAA Privacy manual, and business associate agreements execution with the appropriate vendors.

Monitoring your risks

You have your safeguards in place, now you want to continuously monitor your risks.

You can start by prioritizing your focus using your risk assessment findings and available resources. Based on your findings, what risk areas require active monitoring? Where are your resources coming from? Other departments? Solely compliance? It's essential to understand the big picture for you to prioritize appropriately.

Once the prioritization is complete, you can start thinking about what you can audit and how often—based on your resources and the risk assessment findings.

For those that use annual compliance or audit work plans, you can place certain risks into your work plans so they can be tracked and monitored. This can be extremely helpful when months have passed, but the risk areas remain front of mind. It's also a way to maintain transparency with your BOD or leadership team by reporting changes, progress, or lack of progress. Something to be mindful of: if you cannot (or decide not to) add a risk area to the 2023 work plan, you can always add it to the 2024 work plan.

Great information can be retrieved from employee surveys—such as culture or exit interviews—by asking specific questions related to your risk areas. For example, if your risk area is HIPAA, survey your employees to see if they know how to report a HIPAA issue or are concerned about HIPAA or protected health information

exposure.

Compliance champions are also a great tool that you can use for monitoring purposes. These are employees who believe in compliance and want to look out for the organization. You can champion others to recognize the risks, and they can come to you if there is an issue with certain risks or if the safeguards are not working.

It's imperative to make leadership and the BOD aware of the risks and if new risks arise. You can do this through education and/or board reports. Or you can have time with them through board or compliance committee meetings. Not only does the BOD have a fiduciary responsibility to be aware of compliance matters, but agencies like OIG and DOJ want to make sure that the board and the compliance committee are aware of the risk areas and how your organization is combating those risks. Such as the recently added CIA language, "The Compliance Committee shall be responsible for implementation and oversight of the risk assessment and internal review process."[7] Additionally, OIG has stated, "Boards should also evaluate and discuss how management works together to address risk, including the role of each in: 1. identifying risks, 2. investigating compliance risks and avoiding duplication of effort, 3. identifying and implementing appropriate corrective actions and decision-making, and 4. communicating between the various functions throughout the process."[8]

You can also perform an annual or regular assessment of issues or concerns raised through your incident management system. An assessment can lead to reprioritizing your risk areas or revising your annual work or audit plan.

As mentioned earlier in the article, effectiveness reviews are essential to assessing your compliance program. Part of your review can probe into what has been done related to your risk areas with a series of questions related to your risk assessment. This is a great pulse check of whether what was implemented is working or not working.

As stated previously, a dashboard is a tool that can be used in real-time to assess your risk areas. For example, we have used a "client-risk" dashboard that would allow us to assess the risk associated with a client to determine if a client request can be fulfilled. If the risk is too high, then we may deny the request.

Regarding our example of "ABC" organization, it may make sense to include a category of "HIPAA" to your hotline or in your web reporting tool so employees can report potential HIPAA violations. Another option is to perform a HIPAA Privacy audit monthly due to the high likelihood or risk.

Presenting your results

Another aspect of your risk assessment is to share the results with your organization. One thing to consider is that each type of presentation will depend on your audience. For example, your compliance committee and senior leadership may want a summary of score/findings, the BOD may only want a high-level report on high-priority risk areas, whereas other departments may want to take a deeper dive into the findings that may impact their department(s). What information do they need to receive? What do they want to know about?

What is essential?

Be accurate and precise as possible and state your findings with each mitigation step. This allows all within the organization to be on the same page regarding the priority risk areas and the organization's focus for the next quarter or year. This also provides an opportunity for individuals to state their objections.

Why is this important?

We know transparency and collaboration are key elements of a compliance program. This allows others within your organization to be aware of compliance matters and share their buy-in on these matters.

How does this meet the strategic business need?

A risk assessment contributes to the financial aspect of an organization by mitigating risk and promoting rule adherence. As a compliance professional, you want to ensure that leadership is aware of any risk areas (financial or otherwise) that may affect the compliance program or the organization overall.

Takeaways

- Identifying your risks includes evaluating requirements, interviewing your leadership team, using resources, and considering the scope and frequency of the assessment. It's important to continue to perform these assessments periodically
- Assessing and prioritizing your risks includes considering the likelihood and impact from various perspectives, including financial, legal/compliance, etc.
- Mitigating the risk areas includes implementation of safeguards.
- Monitoring the risk areas includes prioritizing your focus based on the assessment findings and your resources.
- Present the findings to the leadership team, compliance committee, and board of directors and keep them apprised of the risk areas over time.

1 Society of Corporate Compliance and Ethics & Health Care Compliance Association, *Compliance Risk Management: Applying the COSO ERM Framework, Committee of Sponsoring Organizations of the Treadway Commission*, November 2020, https://www.corporatecompliance.org/coso.
2 U.S. Department of Health & Human Services, Office of Inspector General, "The Seven Fundamental Elements of an Effective Compliance Program," accessed August 14, 2023, https://oig.hhs.gov/documents/provider-compliance-training/945/Compliance101tips508.pdf.
3 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated March 2023, https://www.justice.gov/criminal-fraud/page/file/937501/download.
4 HCCA–OIG Effectiveness Roundtable, *Measuring Compliance Program Effectiveness: A Resource Guide*, March 27, 2017, https://oig.hhs.gov/documents/toolkits/928/HCCA-OIG-Resource-Guide.pdf.
5 U.S. Sent'g Guidelines Manual § 8B2.1 (U.S. Sent'g Comm'n 2021), https://www.ussc.gov/guidelines/2021-guidelines-manual/annotated-2021-chapter-8#8b21.
6 HCCA & SCCE, *Compliance Risk Management - Applying the COSO ERM Framework.*
7 U.S. Department of Health & Human Services, Office of Inspector General, "Corporate Integrity Agreement Between the Office of Inspector General of the Department of Health and Human Services and Providence Health & Services–Washington," March 17, 2022, https://oig.hhs.gov/fraud/cia/agreements/Providence_Health_and_Services_Washington_03172022.pdf.
8 U.S. Department of Health & Human Services, Office of Inspector General, Association of Healthcare Internal Auditors, American Health Lawyers Association, and Health Care Compliance Association, *Practical Guidance for Health Care Governing Boards on Compliance Oversight*, April 20,2015, https://oig.hhs.gov/documents/root/162/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf.