COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2024

Nakis Urfi (linkedin.com/in/nurfi/) is Senior Manager, Provider Relations & Regulatory Compliance at Abbott based in Dallas, Texas, USA.

Ximena Restrepo (xrestrepo@logan.org, linkedin.com/in/ximena-restrepo-m-j-chc-chpc-93a9bb14/) is a Compliance and Privacy Partner at Logan Health in Bozeman, Montana, USA.

Bring your program to the next level: Integrating compliance, ESG, and risk management

by Nakis Urfi and Ximena Restrepo

Following up on our presentation at the SCCE ESG and Compliance Conference held virtually in November 2023, we emphasized how both compliance and environmental, social, and governance (ESG) programs follow some similar approaches and processes.[1] The synergies between the two areas give compliance professionals an opportunity to take their program reporting to the next level. ESG provides additional insights into your organization's culture, structure, and commitment to corporate responsibility as these activities come afloat.

In addition to compliance and ESG programs, an organization's enterprise risk management (ERM) function is a third program that assists organizations in achieving and maintaining corporate compliance. These three essential programs can be run under one umbrella or laterally in coordination to avoid duplication of efforts and enhance your compliance reporting to leadership and the board. What's the biggest barrier to this happening? A lack of alignment and working in silos, which impedes cohesive communication and collaboration between teams.

So how can you break the silos if that's the case? Start at a foundational level with your annual compliance risk assessment. You may incorporate ESG questions in your risk assessment survey to assess your employees' perceptions of ESG and include an ESG risk domain column in your risk register in addition to your top industry risk domains (see Table 1). This would allow you to visualize the intersections and overlaps between the compliance, ESG, and ERM programs. If you want to go deeper, consider conducting an ESG cultural or maturity assessment prior to the annual risk assessment to supplement your compliance risk assessment findings and help you develop a more effective and sustainable compliance program plan.

Hot trends, hot risks

Growing and global trends such as artificial intelligence (AI), cybersecurity, and workplace violence are all efforts that can be tackled using integrated risk management, which compliance professionals can bring to light when reporting to leadership and the board. Reporting in this manner brings more holistic views to an organization's high and trending risk areas and provides stronger avenues for leveraging mitigation efforts with a multistakeholder approach.

Workplace violence under the ESG framework

Under the environmental factor, an organization demonstrates it is providing a safe environment to patients, clients, customers, and employees through internal safety controls to meet not just Occupational Safety and Health Administration standards but other enforcement agencies that may come on-site in response to a complaint or incident. Under the social factor, social movements also affect workplace health and safety. Think about protections and employee health activities promoted in your organization. Common activities may incorporate spiritual care and emotional support, including access to mental health services. Safe and flexible working options such as remote and hybrid arrangements promote well-being.

In the healthcare sector, for instance, clinical staff face a wide range of occupational risks or hazards, such as sharp injuries, radiation, or harmful chemical injuries; sentinel events that result in serious harm to patients; as well as aggressive patient behavior (verbal, physical), threats, and the recent rise in gun violence. How does your organization manage these hazards and report these cases? How does your organization promote workplace safety by preventing work-related injuries and illnesses? Does your organization have proper policies or procedures to address these areas? Does your state require employers to run workplace violence prevention programs?

Aligning with the ERM framework, workplace violence and safety are critical activities associated with the ERM Operational and Patient Safety domains in Table 1 below.

Cybersecurity under the ESG framework—linked to social factors

Cybersecurity under the ESG framework can certainly relate to all three areas of ESG; however, to a great degree, it is a major area supporting social welfare through the protection of privacy (a human right focus), with increasing vulnerable risks that can hurt organizations in ever-growingly devasting ways. This has been pushing investors and leadership to step up their commitment to social responsibility.

Aligning with the ERM framework, data privacy and cybersecurity risks and opportunities would fall under the technology and operational domains in Table 1.

AI under the ESG framework

AI plays a significant role in the social and governance factors of ESG. While its use may streamline complex tasks and improve operational efficiencies, it also imposes significant risks, and these need to be properly managed and monitored so that its potential can be unlocked for social good and its intended uses and purposes. AI technology adoption may challenge corporate decision-making when doing business, potentially in terms of discrimination or bias, privacy, transparency, and surveillance, because the technology itself has no moral standards.

Aligning with the ERM framework, AI risks and opportunities would fall under the technology, strategic, and operational domains in Table 1.

Back to basics: Your risk assessment

As mentioned earlier, consider adding a few strategic or culture questions to assess your employees' perception of ESG efforts or basic concepts when conducting your annual compliance risk assessment. Example questions to ask:

- How do you believe the organization promotes ESG sustainability?
- Do you have other concerns that might relate to any of the ESG factors?

- What activities or initiatives do you believe would promote an ESG culture in the organization?

More specific questions to assess specific efforts:

- Does the organization have a set of guidelines that advise employees on using AI?
- Does the company have a workplace violence prevention plan or policy in place?
- Does the company have a diverse board and management composition?

Also, consider the audience. Does your organization make survey results available to all employees or only a subset or particular audience (e.g., management, director level and up, and the board)? Does your organization have separate assessment surveys for the various audiences?

Sharing surveys, getting opinions, and sharing results and future action goals from the results can help demonstrate that the organization is focused on an ethical and sustainable work environment and business model. This will help with employee engagement and morale and lead to a more productive and ethical workforce.

As shown in Table 1, disseminating your compliance risk assessment results to incorporate both ESG and ERM domains makes the report a more powerful and valuable tool not just for compliance professionals but also leadership and the board.

RISK DESCRIPTION	CONTROLS	CONTROL SCORE 1-5	RISK SCORE 1-25	RISK DOMAIN	ESG
Lab orders, lack of communication	Information security (IS) and IT, contracts arrangements established with vendor(s)	3	4	Technology, Operational	n/a
Staff shortages/retention	Policies, procedures, strategic (sign-on bonus, incentives)	3	25	Human Capital	Social (human capital)
Cybersecurity	IS/IT, policies, procedures, education/training, strategic plan	4	15	Technology, Operational	Social (privacy/data security)
Workplace safety, several injuries, incidents reported last quarter	Policies, procedures, education/training, safety meetings, quality reporting	2	8	Patient Safety, Operational	Environmental and social

Table 1: Risk assessment example

Governance alignment

Another strategy for this integrated approach is that compliance officers include their organizational ESG leader or "champion" in their compliance committee(s). To demonstrate the tone at the top, consider incorporating an ESG commitment statement into your compliance and/or ERM-related committee charter(s), compliance program plan, and code of conduct to set expectations. Ultimately, the goal is to reduce redundancies and maximize your various functions' capabilities by breaking down information silos among stakeholders and building a versatile and competent environment.

Conclusion

Over time, this integrated management approach will empower senior executives and the board to make timely decisions and choices while providing oversight of the compliance program. This will help the compliance officer run a more effective and well-structured program that invests in culture, corporate responsibility, and individual accountability—a key takeaway of the 2022 Monaco Memo and announcement of DOJ's corporate enforcement efforts.[2] As Deputy Attorney General Lisa O. Monaco stated, "With a combination of carrots and sticks—with a mix of incentives and deterrence—we're giving general counsels and chief compliance officers the tools they need to make a business case for responsible corporate behavior . . . empowering companies to do the right thing."

An integrated compliance, ERM, and ESG approach will lead to a healthy corporate culture that is next-level compliance!

Takeaways

- An integrated risk management approach becomes a powerful tool as a strategic asset for any organization.
- Including questions and surveys within risk assessments covering compliance and environmental, social, and governance (ESG) can streamline processes and add value to the organization's risk management.
- Aligning ESG with compliance and risk management can lead to organizational efficiencies and provide a more holistic approach to addressing risks.
- By simplifying ESG, enterprise risk management, and compliance functions into unified reporting, key stakeholders—not just compliance professionals—will gain valuable and in-depth knowledge of their organization's operations and culture.
- An integrated management approach will empower senior executives and the board to make timely decisions and choices while overseeing the compliance program.

1 Nakis Urfi and Ximena Restrepo, "ESG, Compliance, and ERM: Bridging the Gaps," ESG and Compliance Conference, November 30, 2023, https://compliancecosmos.org/esg-compliance-and-erm-bridging-gaps-0.
2 U.S. Department of Justice, Office of Public Affairs, "Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement," news release, September 15, 2022, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement.