

Compliance Today – January 2021

Emerging ERM lessons from COVID-19: Considerations for compliance officers and managers of risk

By Jeffrey Driver, JD, MS, and Sarah Couture, RN, CHC, CHRC

Jeffrey Driver (medrisk1@yahoo.com) is an Instructor at Edson College, Arizona State University, and Principal, Soteria Risk Works LLC in Phoenix, AZ, and **Sarah M. Couture** (sarah.couture@ankura.com) is Managing Director at Ankura Consulting in Chicago, IL.

- [linkedin.com/in/jeffdriversrw/](https://www.linkedin.com/in/jeffdriversrw/)
- [linkedin.com/in/sarah-couture-rn-chc-chrc-367a4390/](https://www.linkedin.com/in/sarah-couture-rn-chc-chrc-367a4390/)

For months, our world, our country, our healthcare systems, and our lives have been drastically altered by the COVID-19 pandemic. It has been impossible to hide from the realities of the pandemic as news, social media, and conversations with friends and colleagues have frequently centered on the continuously developing COVID-19 stories. At the same time, our healthcare systems have not been able to hide or be sheltered from the course-altering effects of the pandemic. Healthcare providers around the country have been rocked in multiple ways, including their financial health, their ability to take care of patients, and the new normal of taking both small and drastic measures to help prevent COVID-19 transmission. While pandemics are no “black swan” events,^[1] very few in our country were fully ready for the effects of one. Households rushed to hoard pantry supplies and toilet paper, and healthcare systems clamored to reorganize operations and try to guess and react to what was coming next. Businesses and organizations around the country and around the world are wondering what they could have done to be more prepared. Should they have known this was coming? Could they have more intentionally planned for and forecasted this event in order to be better equipped to handle the sequelae of the pandemic, or even been able to flourish through it and come out stronger on the other side? These are questions that our country’s healthcare leaders should be asking. And many of the answers can be found in the discipline of enterprise risk management (ERM).

ERM overview

While ERM programs are not new to healthcare, many healthcare organizations may not have a good understanding of ERM either because they do not have an ERM program or because their ERM functions are not structured or have not been updated in an industry-standard way. Past iterations of risk management roles or programs may have included only a slice of an organization’s risk profile, such as insurance or malpractice risk, or patient safety or quality risk. Modern ERM, however, includes all risks that could affect an organization, from the boardroom to the storeroom, as well as everything in between within an organization and risk adjacent or external to the organization. Any risk that could affect an organization is considered in ERM.

The best practice of ERM provides a framework by which all organizational risks are identified, thoroughly analyzed and prioritized, and appropriately mitigated in order to allow the organization to make thoughtful and informed business decisions. Modern ERM does more than protect value; it also creates value. The business decisions resulting from a best practice ERM framework can create value by looking for risk mitigation/treatments that are both protective and beneficial for the organization’s bottom line by providing a

financial return on risk and compliance management investments. In addition, ERM helps enhance compliance effectiveness, ensures interdepartmental understanding and collaboration, promotes proactive mitigation of risk instead of reactive responses, and helps strengthen organizations during events that create uncertainty.

ERM will be most successful when those involved in the ERM process all speak the same language, have a similar set of risk perspectives, and have a common way of viewing the risk management process. This can be achieved by developing the organization's risk management framework and processes. At a high level, an ERM framework helps an organization define how it will survey the universe of risks, prioritize and select the risks to mitigate, and then allocate appropriate resources to address the risks. There are two alternative main frameworks popularly used in ERM: International Organization for Standardization guidelines^[2] and Committee of Sponsoring Organizations of the Treadway Commission guidance.^[3] Both frameworks have been updated recently, displaying continued growth and evolution in the field of risk management. A simple internet search shows how much has been written about each framework and how each could be more beneficial in different contexts. Organizations pursuing risk management should explore both frameworks and develop a pragmatic solution based on one or a combination of the frameworks.

In order to ensure that all of the organization's risks are considered, it is important to consider whom to involve in the ERM program. There is no one right answer as to who should lead ERM activities. Large organizations may have a chief risk officer whose primary responsibility is to oversee ERM. Organizations with fewer resources or varying organizational dynamics may appoint the chief compliance officer, chief financial officer, vice president of internal audit, or another executive to oversee ERM. In the authors' view, it makes little difference who "owns" it, as long as the owner has sufficient authority to lead the program and the purview of the program is truly enterprise wide and ensures input of all risks from around the organization.

When deciding who should provide input on risk and collaborate with the ERM function, the phrase "from the boardroom to the storeroom" will again be helpful. Ensure that each operational area has a conduit to direct its risks into the ERM process. Even if assessed informally or without much structured thought, understanding, prioritizing, and mitigating risk is not new to operational areas. A normal part of doing business and running operations is continual understanding and mitigation of risks.

In essence, all operational areas in a healthcare organization have some sort of micro risk-management processes going on to manage specific business processes and outcomes. Throughout this article, we will use the terms "micro risk" and "micro risk management" to describe risk management efforts that occur within a specific operational area that are in place only to address those risks that are relevant for that specific area. By contrast, we will use the terms "macro risk" and "macro risk management" to describe enterprise-wide risk management efforts that are in place to address risks that are applicable to and potentially significant for the organization as a whole. In some operational areas, like compliance and finance, the micro risk management, or selection and management of relevant risks, may be intentional, well defined, and documented. In other operational areas, like supply chain or food or interpreter services, the management of pertinent risk may not be formalized or documented, yet it occurs as the operations ebb and flow and as issues arise and require solutions. In many healthcare organizations, each area's micro risk-management efforts occur in silos and in disparate ways that are specific to each department. While multiple and often informal micro risk-management efforts may be occurring around the organization, there may be little to no effort on the part of the organization as a whole to understand the micro risks of each area, and understand how the micro risks may affect the organization as a whole. ERM programs provide a framework for the enterprise and its leadership to understand not only the micro risk-management efforts taking place disparately, but also provide a forum for those micro risks to be evaluated at the macro, or enterprise-wide, impact level. Many risks will remain primarily relevant for only the operational area to address, but some risks, as assessed through the ERM framework, will become larger

and more complex macro risks that must be understood and addressed at the enterprise level. Thus, ERM capitalizes on the expertise, risk knowledge, and risk management efforts from partnerships around the organization and ensures that relevant risks that could reasonably affect the organization as a whole are identified, prioritized, and addressed. Additionally, ERM can help organizations standardize risk assessment processes in the various operational areas in order to more efficiently and effectively prioritize enterprise-wide risk.

This document is only available to members. Please [log in](#) or [become a member](#).

[Become a Member](#) [Login](#)