Enterprise Risk Management: Moving beyond Compliance

By Marian C. Jennings, M.B.A., M. Jennings Consulting

Key Board Takeaways

Creating Robust Enterprise Risk Management

- The board can play a key leadership role in moving the organization to a more robust, multidimensional, and coordinated approach to overall enterprise risk management (ERM).
- Ask questions about today's approaches and adopt an ERM framework that differentiates between preventable, strategic, and external risks.
- Determine the best committee approach to help the board fulfill its risk management responsibilities.
- Ensure that your board exhibits a culture that supports effective ERM.

If 2020 has taught us anything, it is to never say "never." One year ago, how many healthcare leaders or futurists would have guessed 2020 would be the year for the COVID-19 pandemic and its cascading effects on U.S. hospitals and health systems?

The vast majority of health systems and independent hospitals maintain a board compliance or audit/compliance committee.[1] But effective enterprise risk management (ERM) is much broader than compliance alone. A typical corporate compliance committee for example, would not be discussing such "what if" scenarios.

> As part of its fiduciary duties, a board is required to review the adequacy of the organization's risk management processes and can play a key leadership role in moving beyond traditional reactive and siloed risk prevention approaches.

While compliance typically—and correctly—focuses on prevention of risk, the American Hospital Association's Society for Healthcare Risk Management defines ERM more broadly, recommending that, "healthcare boards develop a broad view of threats and opportunities that affect the organization's strategic goals. A mature ERM program supports the organization in the evaluation and treatment of risk."[2] Such a mature program should be structured and analytical, focused on identifying and mitigating the financial impact and volatility of a portfolio of risks.

As part of its fiduciary duties, a board is required to review the adequacy of the organization's risk management processes and can play a key leadership role in moving beyond traditional reactive and siloed risk prevention approaches.

Tip #1: Understand Where You Are Starting

Start by reviewing your current compliance and ERM approaches and address key questions. Are today's approaches siloed or coordinated? Is your approach more proactive or reactive? How do you measure the success of your compliance or ERM program? Have you agreed on which major risks should be shared with senior management, the compliance committee, or the full board? How aligned are your ERM approaches with your strategic plan?

Tip #2: Adopt an Enterprise Risk Management Framework

If you have not already done so, adopt a framework that comprises more than just compliance. Start by recognizing that there are three categories of enterprise risk[3]:

- Preventable risks: typically internal and a primary focus of corporate compliance (e.g., fraud and abuse, HIPAA requirements, etc.).
- Strategic risks: often external, these arise related to your strategic decisions or positioning (e.g., investing in new urgent care centers to compete with a CVS health hub or new risks associated with sponsoring your own health plan, etc.).
- External risks: these arise from events outside your organization and often are beyond your influence or control (e.g., a pandemic, ransomware attack, major cut in Medicare payments, etc.).

Don't fall into the trap of believing one category of risk is worse than another. A "preventable" risk is no less dangerous than a "strategic" risk. Any category of risk could substantially harm the organization and its reputation.

Equally important is to recognize that risk can occur across multiple domains: clinical, operational, strategic, financial, legal, technology, and hazard. Any category of risk (prevention, strategic,

1 Kathryn Peisert and Kayla Wagner, *Transform Governance to Transform Healthcare: Boards Need to Move Faster to Facilitate Change*, 2019 Biennial Survey of Hospitals and Healthcare Systems, The Governance Institute.

2 American Society for Healthcare Risk Management, *Enterprise Risk Management for Boards and Trustees: Leveraging the Value.*

3 Robert S. Kaplan and Anette Mikes, "Managing Risks: A New Framework," *Harvard Business Review*, June 2012.

or external) could occur in each of these domains, yielding a 3x7 framework of risk categories and domains.

Tip #3: Develop a Risk Inventory

While risk events may occur individually, the enterprise's overall risk is cumulative. A risk inventory includes risks across all domains and categories. Importantly, this risk inventory also needs to assess both the potential impact on the organization and the likelihood of each risk event. For example, a potential $20M risk event with a likelihood of five percent results in an "expected impact" of $1.0M. This is the same expected impact as a $5M risk event with a 20 percent likelihood. Recognize that the likelihood assessment is an assumption and needs to be based upon the best available, credible data—and considered the most likely case, not the worst or best scenario.

Also incorporate into the risk inventory specific mitigation (or prevention) strategies that could reduce the likelihood of the risk event. Finally, develop a list of risk events, ranked by greatest expected impact, into an inventory that presents the overall cumulative portfolio of risks.

Tip #4: Update Your Compliance Committee Charter and Membership

Review your compliance committee charter to ensure that it incorporates all desired elements of ERM. Consider changing the committee name to "Compliance and Enterprise Risk Management" and using this committee as the board's locus for a robust, multidimensional, and coordinated approach.

Additionally, identify the competencies needed on such a committee. If needed, add or replace members of today's committee—and consider whether the board itself needs to recruit new members to lead or serve on this committee.

Tip #5: Ensure that your Board Culture Supports Effective ERM

We all know the adage, "culture eats strategy for lunch." It is critically important that the board create a culture of safety that encompasses all enterprise risks. Leaders need to encourage transparency when an adverse event occurs in any domain—whether clinical, operational, strategic, financial, legal, technology, or hazard.

The board must be courageous and willing to consider a "stress test" scenario. Encourage willingness to ask "what-if" questions around potential disruptors that, even if unlikely, could substantially harm the organization. Consider: "What if several of our major risks occurred simultaneously? Could we remain viable? Are we spreading ourselves too thin?"

Conclusion

Now is the time for the board to establish a multidimensional, coordinated, and proactive enterprise risk management approach. While recognizing myriad risks may feel uncomfortable or even overwhelming, anticipating these events today allows the organization to identify mitigation approaches in advance of an untoward event. Remember, never say never.

The Governance Institute thanks Marian C. Jennings, President, M. Jennings Consulting, and Governance Institute Advisor, for contributing this article. She can be reached at mjennings@mjenningsconsulting.com.