ASHRM AMERICAN SOCIETY FOR HEALTH CARE RISK MANAGEMENT

Enterprise Risk Management for Health Care Boards: Leveraging the Value

AHA Trustee Services

Boards will be asked to make

decisions as health care delivery models continue to evolve. Leaders must be willing to appropriately embrace entrepreneurial risk and pursue risk-bearing strategies.[1] Boards will be asked to make decisions that can help recognize and mitigate risks associated with these strategies and business objectives.

Hospital leaders need to be prepared for a wide variety of situations that involve risk, such as disruptions in services, pandemics, and changes in reimbursement structure.

Health care organizations are facing higher levels of risk as they implement new care delivery and payment models. By employing Enterprise Risk Management (ERM) practices, health care organizations and their boards can better anticipate, recognize and address the myriad risks associated with the transformational changes now occurring in the field.

ERM is a strategic business discipline that supports the identification, assessment and management of risks. Through an enterprise-wide approach, ERM can advance internal control of material risk and improve an organization's ability to generate greater value from strategic and operational activities. However, to achieve these advantages, organizations must embed ERM elements into their culture and structure, and examine the nature of the risks they face.

An ERM program can provide the board with the support it needs to manage uncertainty and focus on the issues critical for successful value creation. An ongoing and iterative process, ERM relies on an organization's ability to learn, collaborate, communicate and report. When successfully implemented, ERM can provide the board with the information it needs to appropriately oversee and reduce risk for the organization and its stakeholders. When strategic ERM is fully implemented it creates value for the organization by allowing for resiliency and the ability to take advantage of opportunities for growth which may present unexpectedly. Boards that understand the ERM framework and associated concepts will benefit from applying ERM to risk oversight. ■

The Board's Role in ERM

A health care organization's board and senior leadership set the stage for adopting and sustaining a successful ERM program, which enables the board to fulfill its stewardship role and fiduciary duties. Effective risk oversight is the foundation of prudent organizational decision making and governance.[2] Asking the questions necessary to establish and/or oversee an ERM program; determining the organization's risk appetite, and tolerance; and monitoring ERM execution help the board fulfill its duty of care and ensure that organizational resources are appropriately deployed in service of the organization's mission.[3] Board support also is critical for successfully engaging employees in ERM activities.[1] Ultimately, successful ERM helps support achievement of the organization's strategic goals.

Because risk oversight has become increasingly important to organizational sustainability, boards in both the for-profit and non-profit sectors are spending more time on risk oversight and incorporating it more visibly into their structure and function. Some health care organizations boards are developing separate committees devoted to risk oversight. Other boards often include risk oversight in their compliance or Internal audit committees activities. Discussions reflecting ERM concepts and principles are often part of today's board meetings and leadership retreats. ERM also is the subject of webinars, articles, publications and other resources for health care boards. See additional resources on page 9.

Figure 1 – Traditional Risk Management (TRM) vs. Enterprise Risk Management (ERM) Focus

AREA	TRM	ERM
RM Focus	Reactive	Proactive
Outcome	Asset preservation	Value creation
Breadth/Depth	Department/silos	Enterprise-wide
Activities	Risk response	Risk Mitigation
Engagement	Practitioner/staff	Top-down, bottom-up board/C-suite

Traditional Risk Management Versus Enterprise Risk Management

The traditional health care risk management (TRM) framework focused on insurance concepts, generally related to liability and hazard coverage programs. Some risk management programs also addressed regulatory and accreditation concerns. Providers defined the role of risk management as "protection from loss" in narrow insurable categories, such as medical malpractice, general liability, property loss, directors' and officers' risk and others.

Many risk management programs later evolved to include early patient safety efforts. As a result, these programs are referred to today as clinical risk management programs. These programs also relied on reported events and incidents to identify risk, so their activities tended to be reactive and retrospective. Program success was measured based on insurance premiums, reserves, losses and reported incidents, and did not address evaluation of lost opportunities, sacrificed value and evaluation of non-clinical risk. This often resulted in inefficient allocation of resources to address risk.

Health care organization boards must 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. Resources are allocated based on this system-wide evaluation of the risks and benefits, risk acceptance, and business case development (such as for a new service line). All departments are expected to support the plans developed as part of the risk management process.

Figure 1 shows how the characteristics of risk management change when ERM becomes part of an organization's processes, focus and culture.[4] ■

ERM Basics

The following five elements comprise the ERM framework (*Figure 2*):

Figure 2

ERM Framework

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Above are fundamental principles in the ERM decision-making model that will help board members understand several important aspects of managing risk across the enterprise.

A risk-aware culture recognizes the future is unpredictable and outcomes cannot be forecasted with certainty. Each project, activity and strategy has a range of possible inputs: costs, resources, mission focus and outputs: returns, revenues and fulfillment of mission with a variety of risks that influence each potential outcome.

Risk appetite reflects the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value, while risk capacity is an expression of the maximum amount of risk that an entity is able to absorb in pursuit of its strategy and business objectives.[5] Risk appetite is heavily influenced by the culture, mission and values of an organization, while risk capacity relates to the availability of resources and financial position. **Both risk appetite and risk capacity should be considered by health care boards in evaluating risk related to the organization's pursuit of specific strategies and adoption of business objectives.** ■

Risk Assessment involves employing a systematic process to identify and evaluate potential risks to the organization's strategies and business objectives and, ultimately, to the fulfillment of its mission. A risk inventory provides a list of all material risks that can then be analyzed to determine ERM priorities and the allocation of necessary resources. Many health care organizations use risk domains as categories of risks to consider as part of the risk assessment process. (See Figure 3 on page 5)

Risk appetite reflects an organization's culture as well as the amount and types of risk that the organization has previously assumed; organizations that have already accepted a significant amount of risk in pursuit of their strategic objectives may be less able to take on additional risk going forward without exceeding their risk capacity. Developing a risk-aware culture is a deliberate process by which the board and senior leadership set the tone for others in the organization to identify and assess risks to business objectives entity-wide.

- Organizations with a higher-risk appetite generally are more focused on the potential for a significant increase in value and may be willing to accept higher risk in return. Early-stage, high-potential, high-risk, growth startup companies have a high appetite for risk and are usually willing to accept greater volatility and uncertainty.
- Organizations with lower-risk appetite commonly are more risk averse and are focused on stable growth. These organizations may be more averse to market fluctuations and greatly influenced by legal and regulatory requirements.

The articulation of risk appetite and risk capacity are essential considerations for boards in adopting an ERM approach.

A risk-aware culture seeks to:

- Quantify the potential variability of inputs and outputs when evaluating and prioritizing competing projects, initiatives and strategic directions
- Identify the sources of such variability, known as Key Risk Indicators (KRIs)
- Measure the anticipated consequences, positive and negative, of such variability through the use of key performance indicators (KPIs)
- Set risk tolerances to establish the limits of acceptable performance.
- Develop mitigation strategies to lessen the impact of and/or reduce the likelihood of negative consequences
- Develop contingency plans to deal with negative consequences if mitigation strategies fail or are not available

Effective ERM also requires competent decision making conducted within the context of the organization's risk appetite and its risk capacity, established by the board. When ERM is used in the context of the organization's decision making, the board can better understand how uncertainty can be quantified, and how it influences the organization's decision making, sets priorities and develops strategies. Risk-adjusted decision making represents a more sophisticated approach to decision making than typical cost-to-benefit or Return on Investment (ROI) analyses.

ERM looks at risk organization-wide and across various domains. Different organizations may choose to identify domains in a number of ways, but they typically include those mentioned in Figure 3. ■

Figure 3 ERM Risk Domains

Domain	Description/Example
Operational 	The business of health care is the delivery of care that is safe, timely, effective, efficient, and patient-centered within diverse populations. Operational risks relate to those risks resulting from inadequate or failed internal processes, or systems that affect business operations. Examples include risks related to: adverse event management, credentialing and staffing, documentation, chain of command, lack of internal controls, supply chain and identification of existing opportunities within management oversight.
Clinical/Patient Safety 	Risks associated with the delivery of care to patients, residents and other health care customers. Clinical risks include: failure to follow evidence based practice, medication errors, hospital acquired conditions (HAC), serious safety events (SSE), health care equity, opportunities to improve safety within the care environments, and others.
Strategic 	Risks associated with the focus and direction of the organization. Because the rapid pace of change can create unpredictability, risks included within the strategic domain are associated with brand, reputation, competition, failure to adapt to changing times, health reform or customer priorities. Managed care relationships/partnerships, conflict-of-interest, marketing and sales, media relations, mergers, acquisitions, divestitures, joint ventures, affiliations and other business arrangements, contract administration, and advertising are other areas generally considered as potential strategic risks.
Financial 	Decisions that affect the financial sustainability of the organization, access to capital or external financial ratings through business relationships or the timing and recognition of revenue and expenses make up this domain. Risks might include: capital structure, credit and interest rate fluctuations, foreign exchange, growth in programs and facilities, capital equipment, regulatory fines and penalties, budgetary performance, accounts receivable, days of cash on hand, capitation contracts, reimbursement rates, managed care contracts, revenue cycle/billing and collection.
Human Capital 	This domain refers to the organization's workforce. Included are risks associated with employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity, compensation, succession planning and labor unionization activity. Human capital associated risks may cover recruitment, diversity, retention, and termination of members of the medical and allied health staff.
Legal/Regulatory 	Risk within this domain incorporates the failure to identify, manage and monitor legal, regulatory, and statutory mandates on a local, state and federal level. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, Centers for Medicare and Medicaid Services (CMS) Conditions of Participation (CoPs) and Conditions for Coverage (CfC), as well as issues related to intellectual property.
Technology 	This domain covers machines, hardware, equipment, devices, wearable technologies and tools, but can also include techniques, systems and methods of organization. Health care has seen an escalation in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Electronic Health Records (EHR) and Meaningful Use, financial and billing systems, social media and cyber security; cyber risks can be significant.
Hazard 	This ERM domain covers assets and their value. Traditionally, insurable hazard risk has related to natural exposure and business interruption. Specific risks can also include risk related to: logistics/supply chain, facility management, plant age, parking (lighting, location, and security), valuables, construction/renovation, earthquakes, windstorms, tornadoes, floods, fires and pandemics.

The Value of ERM

ERM can deliver value by driving positive change. A recent survey of business executives showed the following improvements:[5]

- Lower cost of borrowing
- Improved risk mitigation
- Greater capital efficiency
- Better business decisions
- Operational cost savings

ERM also can contribute to improved financial sustainability for health care organizations. Standard & Poor's (S&P) includes ERM effectiveness among the governance and management factors it uses to assess an organization's credit rating.[6] S&P assigns positive ratings for ERM programs that successfully identify, monitor and mitigate key risks.

Because ERM takes a holistic, organization-wide view of risk, rather than assessing risk department-by-department or function-by-function, it can help reveal the real impact of risk-related events.

Boards that embrace ERM view its value from two perspectives; optimize decision making and maximize value. ERM helps organizations optimize decision making by identifying the best strategies for reducing risk versus those that are simply good enough. This aspect of ERM helps organizations maximize the value they derive from the decisions they make.

ERM also can support value creation. When risk is viewed only as negative, the goal is to reduce or eliminate the risk and minimize its impact. ERM views risk as uncertainty, which means it also can lead to positive outcomes that enhance revenues, reputation and value.

How the ERM Mindset Adds Value (in the box to the right) illustrates the benefits ERM can create by mitigating risks related to energy management. ■

How the ERM Mindset Adds Value

Utilizing an Enterprise Risk Management (ERM) framework during COVID-19 offers a perspective in managing worldwide pandemic risks and their impact on health care organizations. Understanding the significant risks within this framework allows the organization to evaluate risk, its potential impact and focuses thought processes and decision making into a dynamic, fluid and emerging risk environment. ERM allows the organization to look across the enterprise and manage risk throughout the entire organization. COVID-19 was unique because it transected multiple inter-related departments or domains within the health care delivery model and could not be managed in isolation. This in turn, required an enterprise view of all risks to determine which risks need immediate attention and what others could be addressed later in the process. As part of an ERM strategy, risk mitigation may include:

Initial Steps:

- First focus on safety and security of people (employees, customers, suppliers, and others)
- Pinpoint most critical driver of business value and analyze ability to deliver core services
- Identify the key elements needed to keep critical drivers creating value functioning
- Seek input by collaboration with multiple people across the enterprise
- Communicate frequently

Assess the damage and focus on rebuilding after COVID-19:

- High-level analysis of financial impact, liquidity and ability to sustain operations
- Cash flow analysis and forecasting
- Reach out to key partners and vendors
- Leverage learnings to put organization in stronger position for next crisis
- Invest in ERM processes to proactively manage risks that could impact strategic success and long-term survivability

Assessing Organizational Readiness for ERM

Below are key signs that an organization is in need of an ERM initiative when a threat has occurred or an opportunity has been missed that would have been better managed through assessment or evaluation across the entire organization.[7]

- Key risks to the organization's strategy and business objectives have not been systematically identified.
- Risk data are not being appropriately captured, analyzed or escalated.
- Little or no understanding exists about the composite amount and types of risk assumed by the organization, the entity's risk appetite and its capacity to bear risk.
- While some elements of an ERM framework may be in place, there are multiple non-integrated risk functions with overlapping mandates and uncoordinated approaches to managing risk.

Prior to starting an ERM program, a readiness assessment of the organization's internal environment should be conducted to determine if its culture and climate will embrace and support such a program. The board should be fully engaged with preforming this readiness assessment.[1] Considerations boards should take into account prior to implementing an ERM initiative appear in *Figure 4* on page 8. ■

Figure 4

Questions for Boards Assessing Organizational Readiness

• Why do we think we need an ERM process in our organization?	• Has an executive ERM champion been identified?
• What do we seek to accomplish through ERM?	• Does the current state of the organization's culture and environment support ERM adoption?
• How will the board fully support the ERM process?	• Does the organization's culture (behaviors, beliefs and values) encourage identifying and evaluating risk and utilizing the evaluation in the development of strategies and business objectives?
• Where will enhanced risk management activities deliver the greatest value?	• Are sufficient internal and external resources to support ERM adoption available?
• What impact will the adoption of ERM have on the health care organization, and how should it be managed?	• How effectively can information technology be leveraged to support the organization's risk and control framework?
• How will risks and controls be identified, assessed, monitored and improved?	• Do the relevant skills and experience exist within the organization to execute the ERM framework?
• Have the organization's risk appetite and capacity boundaries been defined, agreed upon, communicated and understood?	• What communication will be needed for both internal and external stakeholders to encourage buy-in to the ERM framework?
• Which existing operations can be leveraged to embed ERM throughout the organization?	• Has consideration been given to continuous improvement of the framework?
• What level of oversight will be required for performance measurement and risk mitigation?	• How will the success and value of the ERM program be defined, measured and monitored?
• Are current risk functions effectively aligned and coordinated to manage risk?	• Is risk awareness integrated into the organization's strategic plan?

Full ERM Readiness survey can be found at www.ASHRM.org/ERM

Conclusion

Traditional risk management is no longer sufficient to sustain organizational success in an environment of transforming health care delivery and payment. Enterprise Risk Management provides a more comprehensive, holistic approach that can help hospitals, health systems and their boards better anticipate, recognize and address the myriad risks associated with the increased complexity of transformational change. Boards that understand the ERM framework and its key concepts will be better able to manage uncertainty, act as effective stewards and fiduciaries, and focus on the issues critical to creating greater value for their organizations and stakeholders. ■

References

1. ASHRM. Health Care Enterprise Risk Management Playbook, second edition – An ERM Guide for Health Care Professionals, 2020.
2. NEJM Catalyst; What is Risk Management in Healthcare? April 25, 2018.
3. Stays 2016.
4. ASHRM. Health Care Enterprise Risk Management Playbook, second edition – An ERM Guide for Health Care Professionals, 2020.
5. COSO, p.17.
6. Standard and Poor's Global Ratings: Enterprise Risk Management Evaluation. Standard and Poor's Financial Services LLC, 2019.
7. Horvath, Ingrid, What are the Key Drivers of Enterprise Risk management? Invensis, July 9, 2020.

Additional ERM Resources

ASHRM Resources

ERM Quick Reference Tool
A two-page document that quickly outlines the framework for ERM, including guiding principles and domains.

White Paper - Enterprise Risk Management: Implementing ERM
This White Paper visually outlines the implementation of an ERM program defines its key structural components in any health care setting and will help to build consistency in your efforts to develop or move forward your ERM efforts.

Enterprise Risk Management: Readiness Assessment Tool
The intent of this ERMRAQ tool is for you to gain information regarding the readiness of your Organization to implement ERM Practices or the maturity of ERM initiatives already initiated.

For more information and to download go to https://www.ashrm.org/resources/erm-resources

AHA Trustee Services Resources

Article - Forward-looking health care executive leaders believe a period of great upheaval has only begun, with one source suggesting that health care will be changed by COVID-19 the way the airline industry was by 9/11. Forecasting Shifts in Strategic Priorities Amid COVID-19

Podcast - This podcast describes how to create and sustain a board with the competencies, skills and perspectives needed to become a valued partner with the executive team. On-Demand Podcast: Proactive Board Renewal

For more information go to https://trustees.aha.org/