ASHRM
AMERICAN SOCIETY FOR HEALTHCARE RISK MANAGEMENT
safe and trusted healthcare
A personal membership group of the
American Hospital Association

Enterprise Risk Management for Boards and Trustees:

Leveraging the Value

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.

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 mitigate and prevent risks associated with these types of situations.

Health care organizations are now 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 all relevant 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. Boards that understand the ERM framework and associated concepts will be better able to 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 for-profit boards are developing separate committees devoted to risk oversight. Health care organization boards often include risk oversight in their compliance committee 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.[4] ■

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

AREA	TRM	ERM
Focus	Reactive	Proactive
Outcome	Asset preservation	Value creation
Breadth/Depth	Department/silos	Risk prevention
Activities	Risk mitigation	Risk prevention
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 and culture:[1] ■

ERM Basics

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

1. **Risk identification** – to reduce uncertainty

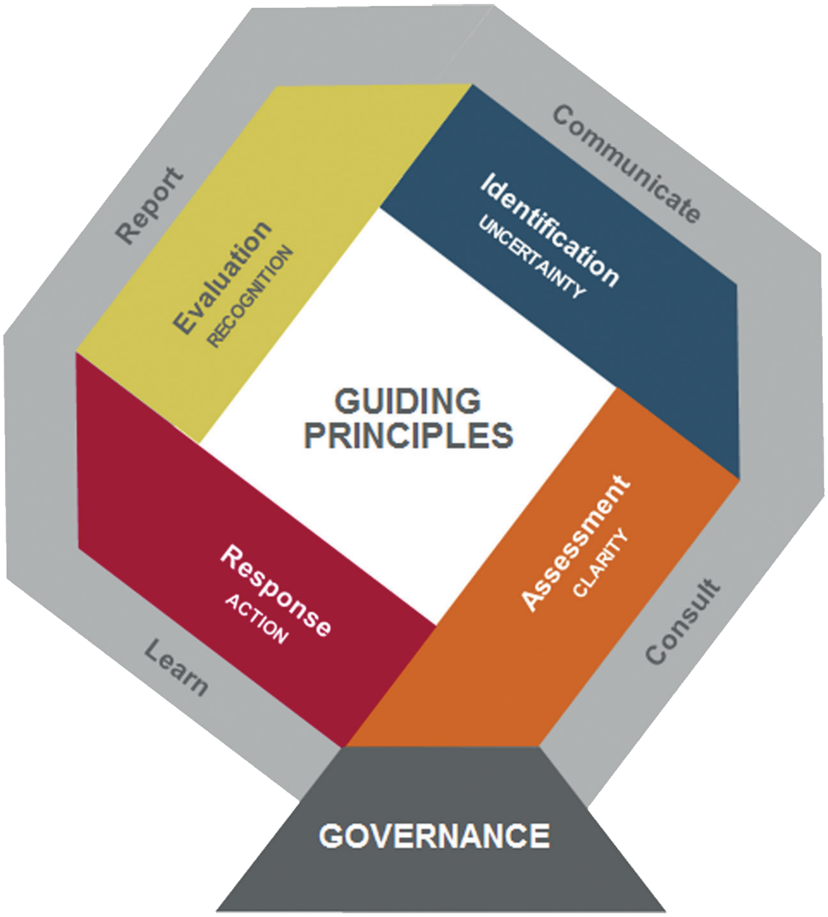
2. **Risk evaluation** – to assist in risk recognition

3. **Risk assessment** – to clarify the nature and extent of known and potential risks

4. **Risk response** – to take action that reduces or eliminates risk

Figure 2

ASHRM ERM Framework



Above are key concepts 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 that the future is unpredictable and outcomes cannot be forecasted with certainty. Each project has a range of possible inputs: cost, resource, mission focus and outputs: returns, revenues and fulfillment of mission with a variety of risks that influence each potential outcome.

Risk appetite is a function of the organization's capacity limitations and tolerance for critical risk - the existence of a vulnerability that could cause exceptionally grave damage to the viability or the operational effectiveness of the organization. For example, an organization may elect to deliver care and treatment in a facility at high risk for flooding due to community need. ■

Risk tolerance is the maximum risk that an organization can afford to take.

Risk assessment involves the evaluation of each risk and all of its potential impacts across the ERM domains: Operational, Clinical/Patient Safety, Strategic, Financial, Human Capital, Legal/Regulatory, Technology and Hazards. (See *Figure 3*, next page.)

Risk appetite and tolerance are influenced by the culture, mission and values of the organization, and the field:[5]

- 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.

Both approaches, high or low risk appetites, impact an organization's culture and the type of risk profile executed. Developing a risk-aware culture is a deliberate process, and the board and senior leadership set the tone by communicating the importance of establishing such a culture, not only at the front line of care delivery but throughout the organization.

Risk appetite and tolerance need to be essential considerations on the board's agenda and are a core reflection of 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
- 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 risk tolerance, established by the board. When ERM is used as the context for the organization's decision making, the board can better understand how uncertainty can be quantified, and how it affects decisions, which influences how the organization makes decisions, sets priorities and develops strategies. Risk-adjusted decision making represents a more sophisticated approach to decision making than the 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* on the next page. ■

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, people or systems that affect business operations. Included are risks related to: adverse event management, credentialing and staffing, documentation, chain of command and deviation from practice.
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) 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: costs associated with malpractice, litigation and insurance; capital structure; credit and interest rate fluctuations; foreign exchange; growth in programs and facilities; capital equipment; corporate compliance (fraud and abuse); accounts receivable; days of cash-on-hand; capitation contracts; billing and collection.
Human Capital	This domain refers to the organization's workforce. This is an important issue in today's tight labor and economic markets. Included are risks associated with recruitment, employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity, compensation, 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 & 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 and tools, but also can include techniques, systems and methods of organization. Health care has seen an explosion in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Risk Management Information Systems (RMIS), Electronic Health Records (EHR), social networking and cyber liability.
Hazard	This domain covers assets and their value. Traditionally, insurable hazard risk has related to natural exposure and business interruption. Specific risks also can include risk related to: facility management, plant age, parking (lighting, location, and security), valuables, construction/ renovation, earthquakes, windstorms, tornadoes, floods and fires.

The Value of ERM

ERM can deliver value by driving positive change. A recent survey of business executives showed the following improvements:[6]

- 72% made better risk-adjusted decision making
- 60% enhanced board risk oversight
- 59% improved performance management
- 58% improved capital efficiency
- 55% experienced organizational and process optimization
- 54% achieved higher quality strategic planning
- 53% improved regulatory compliance
- 50% improved brand reputation

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.[7] 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. 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. ASHRM's ERM Playbook (2015) includes nine ERM pathways to creating value.

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

How the ERM Mindset Adds Value

Energy management of a hospital is critical to the care and treatment of patients. Natural gas and electrical costs continue to rise, sometimes escalating to over $40 million per year. Significant and unpredictable fluctuation of cost makes accurate budgeting difficult. As part of an ERM strategy, risk mitigation may include:

- Conducting an evaluation of utility costs for leased properties and the lease agreement for responsibility of utility costs.
- Knowing tax status and possible refunds available.
- Consolidating the utility billing process.
- Taking advantage of opportunities to lock in utility rates.
- Being mindful of energy requirements of equipment.
- Adopting green building standards and an energy conservation program.

Assessing Organizational Readiness for ERM

Below are key signs that an organization is ready for 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.[8]

- Risk data are not being appropriately captured, analyzed or escalated.
- Little or no understanding exists about what risks fall within the organization's tolerance.
- Multiple risk functions with overlapping mandates and approaches to risk are in place and/or elements of the ERM framework are already in place.

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 the program. The board should be fully engaged with this readiness assessment.[1] Considerations boards should take into account prior to implementing an ERM model or initiative appear in *Figure 4* on the next page. ■

ASHRM AMERICAN SOCIETY FOR HEALTHCARE RISK MANAGEMENT

safe and trusted healthcare

A personal membership group of the American Hospital Association

Figure 4

Questions for Boards Assessing Organizational Readiness

• What is the need for ERM now?	• Has an executive sponsor been identified?
• What level of risk management competency does the board want to achieve across the organization?	• 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 taking appropriate risks?
• Where will enhanced risk management activities deliver the greatest value?	• Are sufficient internal and external resources to support ERM adoption available to our employees?
• What impact will any changes from adopting ERM have on the health care organization, and how should this be managed?	• How effectively will 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 tolerance 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 there be on risk and control?	• How will the success and value of the ERM framework be measured and monitored?
• Are the 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. Carroll, R. (2015). *ASHRM Enterprise Risk Management Playbook* (1st ed., Vol. 1). Chicago: ASHRM.

2. Sanford, N. (2015). The Board's Role in Managing Risk and Corporate Governance, *Deloitte Insights*, Retrieved August 16, 2016 from http://deloitte.wsj.com/riskandcompliance/2013/04/23/the-boards-role-in-managing-risk-and-corporate-governance/

3. Keckley, P., (2016, March 7). The Four Blind Spots of Hospital Governance, *H&HN Daily*. Chicago: Health Forum Inc./AHA. Retrieved August 16, 2016 from http://www.hhnmag.com/articles/7017-the-four-blind-spots-in-hospital-governance

4. Totten, M. (2014, November/December). Compliance Oversight: Responsibilities and Best Practices. Trustee Workbook. *Trustee*: 17-20.

5. O'Rourke, Morgan (Ed.). (2012). *Exploring Risk Appetite and Risk Tolerance*. New York: The Risk Management Society Retrieved June 3, 2016, from https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf

6. Carroll, R. (2015). *ASHRM Enterprise Risk Management Playbook* (1st ed., Vol. 1). Chicago: ASHRM.

7. Standard & Poor's. (2012, November 13). Methodology: Management and Governance Credit Factors For Corporate Entities and Insurers. Retrieved from https://erm.ncsu.edu/az/erm/i/chan/library/SP_MandG_Methodology.pdf

8. Fink, Sheri. (2012, September 9). Hospital Faces Negligence in Trial in Katrina Death. *The Times-Picayune*. Retrieved August 17, 2016 from http://www.nola.com/health/index.ssf/2010/01/hospital_faces_negligence_tria.html