

A Model for Enterprise Risk Management Within a Healthcare Organization

**Wayne L. Brannan, CPHRM, CBCP, ARM
Director, University Risk Management
The Medical University of South Carolina
Charleston, South Carolina**

**Jennifer R. Taylor, ABCP
Business Manager, University Risk Management
The Medical University of South Carolina
Charleston, South Carolina**

Why Enterprise Risk Management? Why now? Consider an audit of your healthcare organization has found your facility failed to report hundreds of mistakes, or your chief Urologist was charged with research conflict of interest. What if your facility inappropriately billed for time and activity while working under a federally funded grant, or your organization was found non-compliant in interim life-safety measures? Given the breadth and complexity of potential risks such as these, healthcare organizations require a logical framework for identifying the true scope of potential risks, evaluating risk exposures and responding to risks. In the midst of mounting regulations, higher standards of accountability, increased competition for services and staffing shortages, healthcare facilities endeavor to continually improve patient care and safety while decreasing unnecessary costs. Understandably, healthcare organizations have, like most other organizations, focused on those risks that could be easily managed at lower costs and have ignored residual risks. By taking a proactive approach to risk management using an Enterprise Risk Management (ERM) model, healthcare organizations will be better equipped to focus on all risks throughout the organization while maintaining patient safety, ensuring compliance and improving their organizations' bottom line.

Incorporating an ERM program at any institution takes time and a commitment by senior management to shift their organization to a new paradigm; a better, continuous method for analyzing all risks throughout the organization. There are three steps involved in implementing an ERM program in an organization. These steps include analyzing risk from a broader, enterprise-wide perspective, defining roles and responsibilities and creating a strategy matrix to address specific ERM elements. While an organization must focus on those steps needed to implement an ERM program, it is important to understand the definition of ERM and the key elements of ERM to truly understand the value ERM can bring to your organization.

This paper will define ERM and the elements of ERM as well as address the steps needed to achieve ERM. Furthermore, we will introduce a new model, the ERM Fusion Model. The use of this module will depict how ERM can bring value to a healthcare organization facing compliance with JCAHO continued readiness, HIPAA, Sarbanes-Oxley, OSHA, CMS and more.

So, What is Enterprise Risk Management?

In September 2004, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an Executive Summary on ERM titled, “Enterprise Risk Management – Integrated Framework.” This Executive Summary defines ERM as a process effected by an entity’s Board of Directors, management and other key personnel aimed at making an organization more profitable by creating a single view of all risks, internal and external, and creating an executive level management strategy to deal with those risks (COSO 2004). Key aspects of ERM include analyzing multiple risks “across the enterprise” rather than in separate risk silos and elevating risk management as a strategic partner in achieving corporate goals and objectives.

Traditionally, risks are identified in separate risk areas, or silos, with insurance risks handled by the insurance department, market risks handled by the sales or marketing department, risks of employee injuries handled by Occupational Safety and Health or Workers’ Compensation, patient safety risks handled by the quality department and so on. Conventional risks such as hazard risks are placed on the back burner and business continuity and disaster recovery is focused on maintaining customer and regulatory confidence (Jablonowski 2006). At the very least, the traditional method addresses risks to an organization at departmental levels. However, this method evaluates risks in a reactive approach rather than evaluating risks proactively. The traditional method also fails to define risks collectively throughout the enterprise in that various departments define risks differently. The traditional method of identifying risks also fails to address two critical aspects of risk management from an ERM perspective: corporate risk appetite or “the amount of risk a company is willing to absorb for the returns it expects to gain” and the management of emergent risks (Shaw 2005). Problems stemming from overlooking these critical aspects have led to a need for a paradigm shift in risk assessment and analysis and the need for an ERM framework.

To fully understand the concept of ERM, it is important to understand the elements of ERM once it is implemented in an organization. According to COSO, there are eight elements that encompass the ERM framework. These elements are:

1. **Education and Internal Environment:** Staff should be educated in the overall risk management philosophy and risk appetite, integrity and ethical values and the environment in which they operate.
2. **Objective Setting:** The process of understanding how corporate objectives and risks interrelate and how they can affect the achievement of an entity’s goals.
3. **Event Identification:** Determine significant events that would affect the entity’s objectives. Distinguish risks versus opportunities.
4. **Risk Assessment:** Risks are analyzed, considering likelihood and impact, and should be evaluated on an inherent basis or a residual basis. Inherent risk occurs without consideration of mitigating controls currently in place and residual risk occurs in light of existing controls.
5. **Risk Response:** The method by which management responds to risks whether through avoidance, acceptance, reduction or sharing (also known as avoid, retain, control and transfer)

and in doing so, maintains that the risks remain in line with the entity's risk tolerances and risk appetite.

6. Control Activities: The organization develops and implements policies and procedures to ensure that the risk responses are carried out.
7. Information and Communication: Relevant and timely information regarding risks is identified, captured and communicated throughout the organization; flowing down, across and up through the ranks.
8. Monitoring: The ERM program is monitored, updated and maintained through ongoing management evaluations.

(Adams, Campbell 2005) (Braz, et. al. 2005) (COSO 2004)

Why Consider Enterprise Risk Management?

So, why consider Enterprise Risk Management? In a recent survey of 150 insurance company executives, administered by Tillinghast – Towers Perrin, it appears ERM is gaining the attention of many. According to survey results, “an overwhelming number of respondents (86%) say that enterprise-level risk management is more of a priority today than it was a year ago.” Furthermore, the survey data reflects the move from the traditional risk silo approach to ERM in an effort to improve communication on risk management throughout organizations. It is apparent that senior executives are giving integrated risk greater priority and attention than ever before. (Chase-Jenkins, Farr 2004). This is a trend that will likely continue as more organizations begin to recognize the value ERM can achieve.

There are a growing number of issues facing the healthcare industry that make ERM an attractive strategy for managing risks. Examples of these issues are included on Figure 1. In such a challenging environment, ERM facilitates an organization's ability to achieve its performance and profitability targets by preventing loss of resource; ensuring compliance with laws and regulations; avoiding damage to reputations and identifying areas where due diligence is prudent due to increased corporate scrutiny. ERM helps achieve organizational goals and objectives by looking at risk from a broader perspective than traditional risk management (Hale, Boone, Maley 2004).

Issues facing the Healthcare Industry



Figure 1: This figure represents issues facing the healthcare industry today.

The underlying premise of ERM is that every entity exists to provide value for its stakeholders. Stakeholders of not-for-profit entities realize value when they recognize receipt of valued social benefit (Hale, Boone, Maley 2004). Moreover, ERM allows for wider responsibility to society, which leads to long-term profitability and sustainable growth (Jablonowski 2006). Again, a key to achieving that social benefit and a key to survival is to identify and manage risk across the enterprise rather than narrowly focusing on certain “traditional” risk areas.

Achieving ERM

While ERM indeed provides value to any organization, achieving it can be cumbersome at first and roadblocks can be met along the way. Effecting ERM is complex and takes time. It requires a new paradigm and organizations must transition from theory to action. The notion of enterprise-wide risk management requires compiled knowledge and focus from key areas including legal, financial, internal audit, clinical, insurance, compliance, operations and more. With this collaboration, turf wars between departments and divisions are likely to develop (Hale, Boone, Maley 2004). However challenging it may seem, your facility can achieve ERM provided the steps listed below are followed.

Step One: On Your Way

The first step to accomplishing ERM at your facility is to analyze risk from a broader “enterprise-wide” perspective. Looking at this step from a healthcare perspective, it is important to identify business streams and associated risks throughout the entire scope of activities, including facilities, physicians, managed care, education, senior care, research, technology and ancillary business

operations. Each manager responsible for a business unit, function, process, or activity needs to develop an assessment of risk for that unit (Hale, Boone, Maley 2004). The definition of risk must be standardized at this point to ensure a unified view of risk across the enterprise. Although specific departments and units may classify a risk as one that is within the facility's risk appetite, combining all risks together may create a combined risk larger than the broader organization's risk appetite.

When taking an enterprise-wide approach, risks should be mapped into various categories prior to implementation of the ERM program. For instance, as mentioned in prior examples, there are various risks facing the health care organization today. These risks can be grouped into the following risk domains:

- Operational: These risks are derived from an organization's core business (i.e. clinical services and outpatient care).
- Financial: These risks are related to an organization's ability to earn, raise, or access capital.
- Human: These risks are human resource management issues, such as, hiring, terminating, and compensating employees, sexual harassment, or unionization.
- Strategic: These are risks related to an organization's ability to grow and expand through mergers, joint ventures and the like.
- Legal/Regulatory: These are risks associated with statutory and regulatory compliance.
- Technological: These are risks associated with the use of biomedical and information technology.

(Braz, et. al. 2005)

In addition to defining and grouping risks across the enterprise, it is necessary to find un-addressed or under-addressed areas of risk such as research, websites, disaster planning, and contractual liability, to name a few. Moreover, exposures in various ancillary operations could potentially be uncovered. For instance, public-access fitness centers, affiliations with community hospitals or clinics that have tort immunity, day care centers, etc. could all be examples of potential risk exposure areas. Upon notification of such exposures, risks should be ranked by loss potential based on severity and frequency of exposure occurrence. The key is to ensure an adequate, uniform response to these risks through avoidance, acceptance, reduction or sharing (Hale, Boone, Maley 2004).

Step Two: The ERM Roundtable/Roles and Responsibilities

The second step to achieving ERM at your facility is to embrace "enterprise-wide" risk oversight by creating an ERM Roundtable (Hale, Boone, Maley 2004). According to COSO, "Everyone in an entity has some responsibility for enterprise risk management" (COSO 2004). Therefore, it is necessary to foster a collaborative effort to address risk and quality, and make proactive decisions regarding risk management considerations as well as operational strategies. An ERM Roundtable unites managers from all areas across the organization including, but not limited to, Information Technology, Internal Audit, Finance, Quality/Safety, Marketing, Operations, Legal, Research, and Medical Staff. Figure 2 represents the collaboration between managers across the organization, and it depicts how this collaboration and communication will allow for all areas in the organization to evaluate risk issues from new business strategies well in advance of those strategies being implemented (Braz, et. al. 2005). It is important to ensure that an organization determine and

assign authority levels for managing risks as well as facilitate open communication of risk through the concept of the ERM Roundtable.

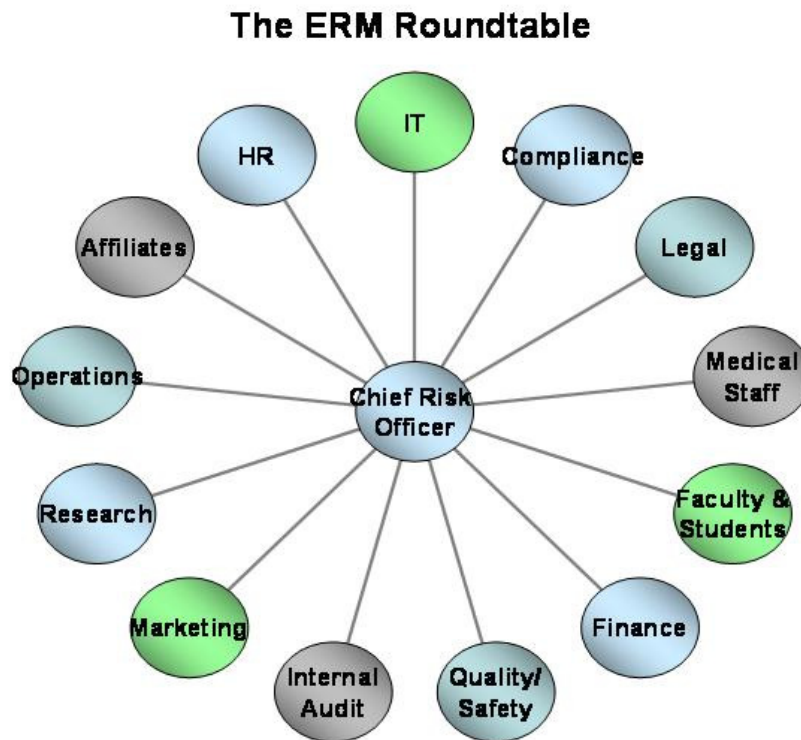


Figure 2: The ERM Roundtable represents ERM collaboration between managers across the organization.

In addition to uniting key managers throughout the organization, the ERM Roundtable empowers the risk management department through enterprise-wide risk oversight. In accordance with this risk oversight there is a need for the leadership from an individual with a global approach to the interrelationship of all risks within the entire organization. The position of Chief Risk Officer (CRO) has emerged from the ERM movement to meet this need (Braz, et. al. 2005). As illustrated in Figure 2 above, the CRO creates the link for risk management communication throughout the organization. The role of the CRO is very different from the role of the traditional risk manager. Whereas CROs have a much more global view of risk in an organization, traditional risk managers often look at risks in a compartmentalized, snapshot view in order to make decisions. These decisions are often based on isolated circumstances and occurrences only allowing the risk manager to narrowly focus on one particular area while missing the “bigger picture.” The CRO, however, is granted unlimited access to relevant information throughout the organization, including financial and operational data. Additionally, the CRO has unlimited access to other members of the senior management team enabling a broader view of risk throughout the organization (Braz, et. al. 2005).

The CRO position encompasses a variety of roles that, as a whole, amount “to creating a risk-aware culture in an organization” (Lee, Shimpi 2005). One such role is to meet with senior leaders

and board members to identify the organization's goals and objectives on a continual basis. In addition, the CRO should familiarize and educate senior management, stakeholders, and other member of the organization with the ERM program. Moreover, CRO's must establish ERM policies, set goals for implementation and frame accountability and authority throughout the organization. It is necessary for the CRO to guide the integration of ERM with other business planning and management activities as well as oversee development of entity-wide and business unit specific risk tolerances. As previously mentioned, it is also the CRO's duty to facilitate managers' development of risk analysis and assessment through the ERM Roundtable (Hale, Boone, Maley 2004).

It is apparent that the CRO wears many different "hats" in an organization, but most important to the success of any ERM program are the traits a CRO must possess. Above all, a CRO must be a good communicator, facilitator, and leader (Lee, Shimpi 2005). As the CRO position achieves prominence throughout all industries, including the health care industry, the traits and roles of the position become more pronounced. With ever-increasing regulatory concerns the CRO has become an important member of senior management teams and ERM programs in general.

Step Three: The Strategy Matrix

With the premise of ERM explained and key personnel roles described, it is important to focus on the strategy behind ERM and the development of the strategy matrix. A strategy matrix should assist an organization in defining strategic objectives and strategies to achieve those objectives. For instance, a strategic objective in a healthcare organization may involve assisting physicians in utilizing technologies in order to improve physician productivity, improve convenience for patients and improve patient safety. A corresponding strategy to this objective may be to incorporate a web-based health portal to provide physicians and patients with a resource library on healthcare issues or to incorporate the use of electronic medical records throughout the organization. Once strategic objectives and strategies to achieve those objectives are realized, an organization must define key risk management issues that will support or threaten them. For instance, using the above example of utilizing technologies for physicians and patients, one possible risk issue may be in the number of privacy violations encountered due to this new technology. Additional issues may include network security breaches, viruses, and information theft among others. When defining possible risk issues, it is also important to prioritize them in order to provide proper focus on larger, more costly risks. The last step in developing a strategy matrix is to develop solutions to risks identified in order to achieve the organization's strategic objectives. This can be done through documenting assignments of responsibility and creating timetables for achieving those goals and objectives. In the above example, a solution to risks may involve reviewing network security policies and contracts from third party vendors as well as reviewing the need and cost/benefit for cyber liability risk transfer (Hale, Boone, Maley 2004).

The ERM Fusion Model: An Illustration of Change

Through a successful strategy matrix, organizations, specifically healthcare organizations, will be better prepared to promote a culture of enterprise-wide risk management and to set measurable objectives that align with organizational goals. One goal of most healthcare organizations is to maintain JCAHO accreditation. Figures 3, 4 and 5 illustrate how incorporating ERM into all processes within the healthcare organization will ultimately ensure continued readiness for a JCAHO survey and accreditation maintenance.

The ERM Fusion Model
Incorporating JCAHO Patient Safety Goals

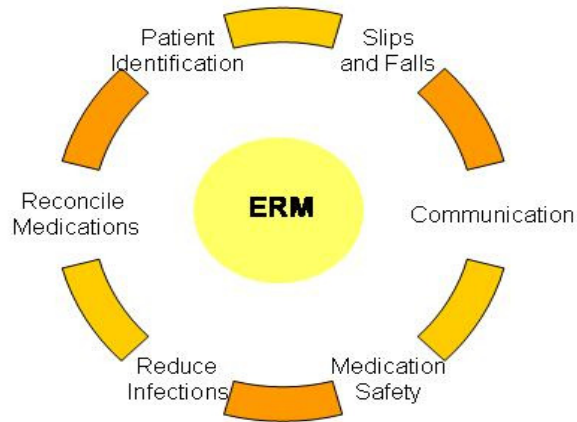


Figure 3: This figure represents the ERM Fusion model as it relates to National Patient Safety Goals (NPSGs).

The ERM Fusion Model
Incorporating JCAHO Patient Safety Goals

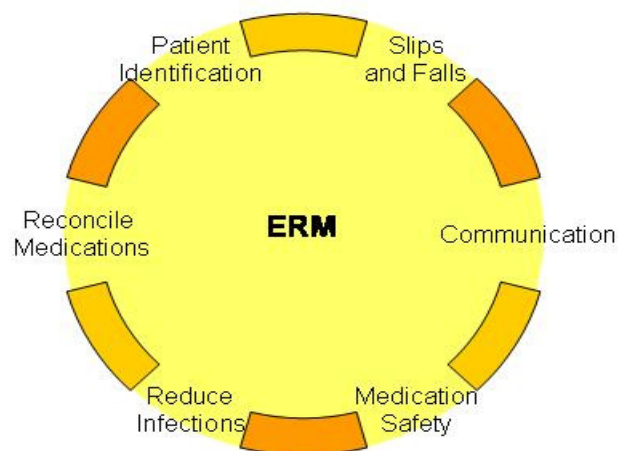


Figure 4: This figure represents the ERM Fusion model and displays ERM's ability to unite and encompass all risks associated with National Patient Safety Goals (NPSGs).

The ERM Fusion Model

Incorporating JCAHO's Top 10 Items that will Make or Break You

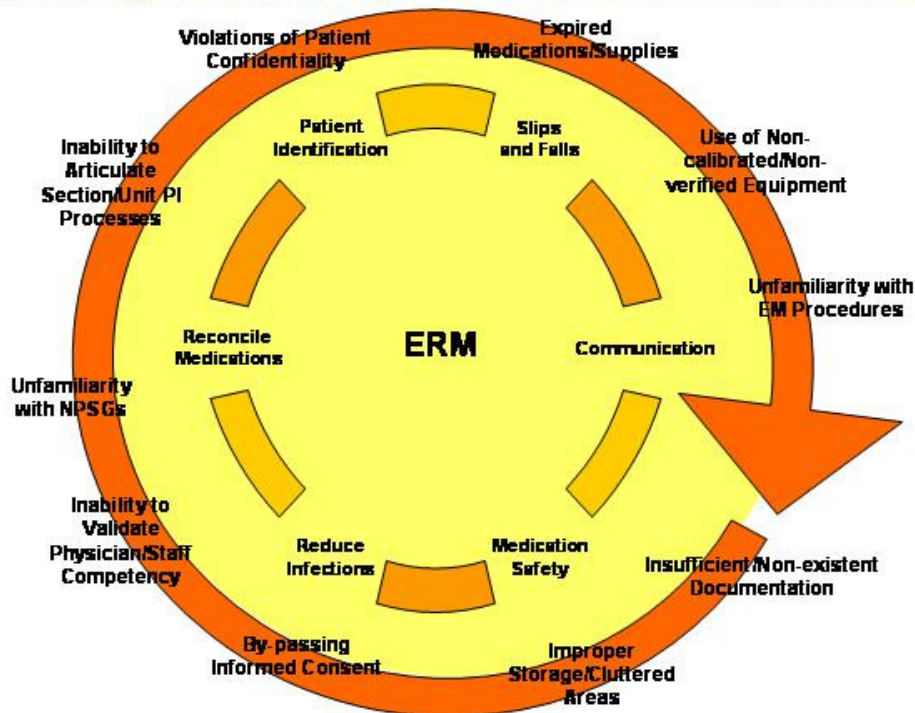


Figure 5: This figure represents the ERM Fusion model as it relates to National Patient Safety Goals (NPSGs) and the top ten items that will affect a hospital's accreditation.

JCAHO emphasis on patient safety, over the past few years, has now moved healthcare organizations into the practice of performing unannounced surveys. The survey process has also changed from a review of documents and manager interviews to the patient tracer model. This new survey model involves a surveyor randomly selecting patient records and following the patient's visit through the facility. The surveyor evaluates JCAHO compliance based on staff responses and documentation review as they travel through the facility as the patient did when they received care. Not only must we now comply with JCAHO requirements, including the National Patient Safety Goals (NPSGs), we must ensure we are in a mode of continual readiness for an unannounced inspection and that all areas of our facility and all staff members are able to "walk the walk" and "talk the talk" of providing quality, safe patient care. The ERM Fusion model is one tool that can be used to assess a facility's exposure to risk of non-compliance with NPSGs as well as those routine requirements that facilities are well aware of. If an organization fails to address both NPSGs and routine items continuously, accreditation could be jeopardized.

Conclusion

As discussed in this paper, healthcare organizations can ill afford to continue to manage risk in fragmented silos. The public perception is that healthcare organizations must maintain the highest level of care for their customers (patients). In order to meet this expectation in today's environment, it is imperative healthcare organizations embrace Enterprise Risk Management. By incorporating the steps outlined in this paper including analyzing risk from a broader, enterprise-wide perspective, defining roles and responsibilities, creating a strategy matrix to address specific ERM elements and utilizing the ERM Fusion Model, healthcare organizations will recognize the value of ERM through increased patient safety and quality care. The transition from traditional risk management to ERM will not take place over night, but it is a journey which we as risk managers must begin today.

Bibliography

Adams, G.W. and Campbell, M. "Where Are You on the Journey to ERM?" *Risk Management Magazine*. September 2005: 16-20.

Braz, R., et. al. "Monographs: Enterprise Risk Management." *Journal of Healthcare Risk Management*. 25(2005): 11-24.

Chase-Jenkins, L. and Farr, Ian. "Adding Value Through Risk and Capital Management." Tillinghast-Towers Perrin, 2004. <http://www.towersperrin.com/tillinghast/publications/reports/2005_ERM_Survey/ERM_Survey.pdf>

"Enterprise Risk Management – Integrated Framework." Commission of Sponsoring Organizations of the Treadway Commission (COSO) executive summary and complete report, September 2004. <<http://www.coso.org/publications.htm>>

Hale, J.L., Boone B. and Maley R. "A Working Man's Approach to Enterprise Risk Management." *ASHRM*. Orlando, FL 2004. 1-33.

Jablonowski, M. "The Real Value of ERM." *Risk Management Magazine*. February 2006: 33-37.

Lee, C. R. and Shimpi, P. "The Chief Risk Officer: What Does it Look Like and How Do You Get There?" *Risk Management Magazine*. September 2005: 34-38.

Shaw, J. "Managing All of Your Enterprise's Risks." *Risk Management Magazine*. September 2005: 34-38.