ASHRM AMERICAN SOCIETY FOR HEALTH CARE RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT:

A FRAMEWORK FOR SUCCESS

Lead Author:

Roberta L. Carroll, RN, ARM, MBA, CPCU, CPHQ, CPHRM, HEM, DFASHRM, LHRM

Contributors:

Michelle Hoppes, RN, MS, AHRMQR, DFASHRM

Sheila Hagg-Rickert, JD, MHA, MBA, CPCU, DFASHRM

Barbara J. Youngberg, BSN, MSW, JD

Barbara A. McCarthy, RN, MPH, CIC, CPHQ, CPHRM, FASHRM

Denise Shope, BSN, RN, MHSA, ARM, FASHRM

Teresa Kielhorn, JD, LLM

Jeffrey Driver, JD, MBA, DFASHRM

Table of Contents

Abstract: **Healthcare organizations have made significant strides in developing Enterprise Risk Management (ERM) programs, but there is still much work to be done.** To facilitate this process, ASHRM has defined ERM and created an ERM Framework for use in healthcare around which an ERM Program can be formed. This white paper will graphically display the Framework and describe key structural components necessary in any healthcare setting. Use this Framework to help build consistency in your efforts to move ERM forward.

Audience: Novice, intermediate risk professional, or anyone desiring more information on ERM

Keywords: Enterprise Risk Management, ERM, Framework, Guiding Principles, Governance, Risk & Opportunity Identification, Assessment, Risk Response, Risk Evaluation

INTRODUCTION

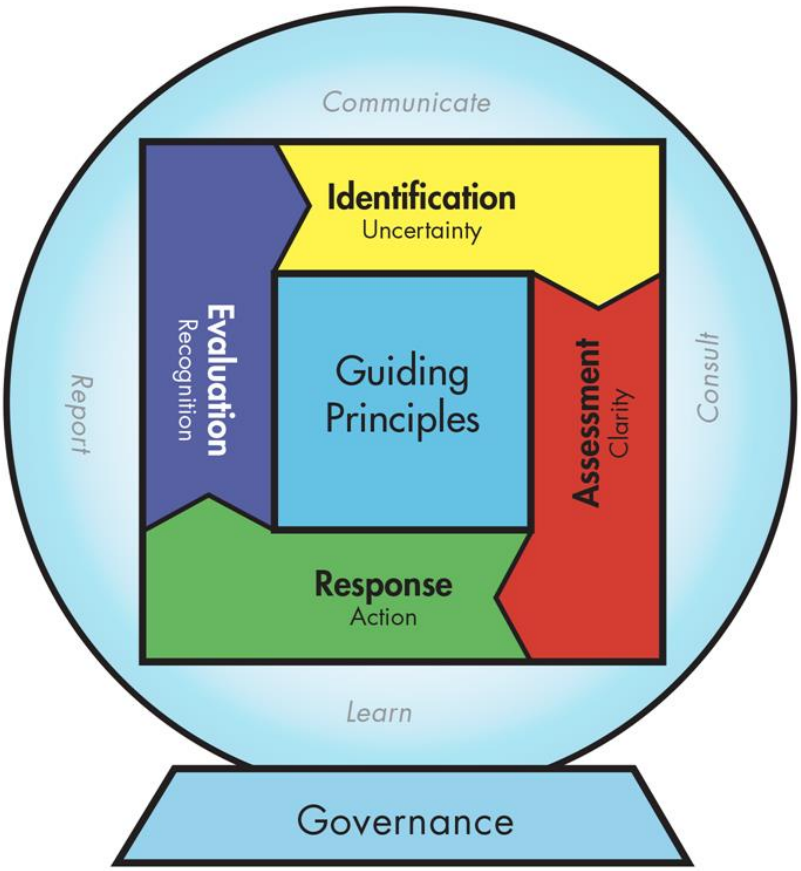
The advancement of healthcare Enterprise Risk Management is a key initiative in ASHRM's Strategic Plan for 2014-2015. The implementation and maturity of ERM programs in healthcare organizations—while making significant strides—still lag behind large organizations, public companies, and financial services organizations. Although many healthcare risk-management professionals implement ERM strategies for new programs, projects and services (particularly to manage clinical, and patient-safety related risks), they fail to advance ERM strategies on an organization-wide basis beyond those risks and thus miss tremendous opportunity to increase or create value. Recognizing the elements necessary for ERM program development and implementation and embedding them in the enterprise is central to program success and sustainability.

Supporting this key ASHRM initiative is the development of a framework around which an ERM Program can be structured along with a clear, concise and easily understood definition of ERM. This paper offers guidance on ERM methods specific to healthcare organizations. It outlines ASHRM's ERM Framework highlighting structural components to support a solid foundation, promote program credibility and success, and advance ERM principles throughout your healthcare organization.

FRAMEWORK

The Framework, as illustrated in this paper (See Graphic #1) *ASHRMs ERM Framework*, depicts a *sample* structure that can be utilized by any risk-management professional as the developmental foundation of an organization-wide ERM program. Understandably, each organization's ERM program will vary due to differences in mission, vision, culture and strategic direction. However, components shown in the *sample* Framework are relevant to any healthcare organization. Each group may adopt these elements in a manner that accommodates the differences noted. Flexibility is important as a one-size-fits-all approach is not applicable in ERM. Realizing this at the outset will encourage the risk management professional to define and modify basic structural elements in the Framework to fit their specific organizational needs, particularly as they relate to unique delivery settings. This *sample* Framework allows for vital flexibility to create a unique and individualized healthcare ERM program. Once a Framework to address the specific needs of the organization is developed, the process may begin for creating program success building blocks such as: informing, consulting, learning, communicating and reporting.

GRAPHIC #1 ASHRM'S ERM FRAMEWORK



GUIDING PRINCIPLES

The following Guiding Principles in concert with ASHRM's mission and vision have been developed as basic building blocks supporting the Framework for ERM in healthcare:

- Advance safe and trusted healthcare
- Manage uncertainty
- Maximize value protection and creation
- Encourage multidisciplinary accountability[1]
- Optimize organizational readiness
- Promote positive organizational culture which will impact readiness and success
- Advance ERM Practices – ERM programs once started are continuous[2] and are a paradigm shift in how an organization identifies and manages risks and opportunities. These comprehensive programs are "not a stop on the road, but a journey."[3]
- Utilize data/metrics to prioritize risks
- Align risk appetite and strategy

GOVERNANCE

The Governing Body[4] of each healthcare organization is ultimately responsible for its ERM program. It is accountable either directly or through the leadership team for:

- Defining ERM as appropriate for the organization
- Creating and maintaining a culture that is supportive of ERM
- Determining strategy and program objectives
- Establishing parameters and levels for risk appetite and tolerance statements
- Establishing the ERM structure
- Approving the ERM plan (as well as communication and reporting plans)
- Providing ERM program oversight

Each of these areas is described in more detail below.

Definition of ERM – Adopting a definition of ERM that is clear, concise and understandable is one of the significant early steps in developing an ERM Program. Without an articulated definition the organization can embrace, the activities associated with ERM development and implementation can become disjointed and without purpose. ASHRM has adopted the following definition.

> "Enterprise risk management in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connections to total value."[5]

Other credible organizations such as the Committee of Sponsoring Organizations of the Treadway Commission[6] (COSO), The American Heath Lawyers Association[7] (AHLA), the Risk and Insurance Management Society (RIMS)[8], and the International Organization of Standardization – ISO 31000:2009[9] have all defined ERM, albeit differently. See the Endnotes for those definitions.

TABLE #1	Terms & Complimentary Descriptions		
Comprehensive Framework	**Value Protection**	**Value Creation**	**Managing Uncertainty**
• Organizational-wide • Holistic • Broad perspective • Synergistic effect • Comprehensive • Strategic • Thorough • Robust • Structured	• Reduce uncertainty • Reduce variability • Duplication • Separation • Shield asset • Efficient use of resources • Quality outcomes • Safe practices	• Increased market share • Competitive edge • Financial strength • Improved ROI • Increased margins • Enhanced reputation • Improved satisfaction scores • Quality Outcomes • Credible • Respected	• Reduce Risks • Eliminate Loss • Promote standardization • Use Evidence-Based Practice • Decrease Variability • View the impact of risk holistically not in silos (eliminate silo mentality) • Understand Chaos theory • Eliminate/minimize lost opportunities • Captures the positive or upside

Culture – A *Guiding Principle* and key element in program implementation is culture and organizational readiness. The Governing Body is responsible for "setting the stage" to ensure the organization's culture will support the ERM program. Organizations that adopt fear as a practice, engage in tactics that are not conducive to a learning environment, are not fair and just in dealing with employees and staff, allow for disruptive behavior, and use risk reporting as the basis for disciplinary action are not ready for ERM and will fail if they try to implement a program.

Anecdotally, a supportive, positive culture correlates (positively) to quality outcomes, performance and employee satisfaction. However, no culture assessment instrument measured all three dimensions easily.[10] Nevertheless, there are many strategic initiatives that support a culture conducive to ERM, including programs such as: Organizing for High Reliability (HRO), Crew Resource Management (CRM), TEAMSTEPPS®, Just Culture, concepts of Mindfulness, and support for critical thinking. Many use the term culture in concert with organizational "climate" and "environment" even given subtle, but distinct differences.

Strategy — A defined strategy is management's game plan for strengthening enterprise performance. It is the long-term action plan designed to achieve a particular goal or set of goals or objectives.[11] In years past, an organization's Board of Directors, in concert with senior leadership, drafted a 5 - 10 year strategic plan. Not the case in 2014! With today's complex and rapid shifts in healthcare, organizations develop strategic plans to cover six months to two years. They rely on committees; engage additional staff, and review and modify the strategic plan as frequently as each quarter. Organizational strategy is directly linked to an organization's vision, mission, goals and objectives. (See Graphic #2: *Steps to Create a Strategic Plan*).

GRAPHIC #2 STRATEGIC PLAN

Objectives — Objective setting is an important step in ensuring the ERM strategy and comprehensive ERM plan are actionable and operationalized. Clear objectives offer a roadmap that will support goal attainment. Several tools can assist in the development of objectives, including: a SWOT analysis to determine organizational Strengths, Weaknesses, Opportunities and Threats and developing SMART[12] goals.

The simple but powerful SMART acronym will assist you in remembering five key objective-setting areas:

- **S**pecific — Clearly articulate the task and what it will achieve.
- **M**easurable — Identify the criteria or metrics by which outcomes will be evaluated and define how success will be measured.
- **A**chievable — Prepare a SWOT analysis to determine if the objective is achievable. Understand challenges and threats to goal attainment in order to identify solutions.
- **R**ealistic — Pragmatically determine resources necessary to complete the objective. Are these resources readily available? If not, what can you do? Keep in mind that resources go beyond the financial cost of attaining objectives and can include additional items such as people, space and energy.
- **T**ime — Can the objective be completed within the allocated timeframe? What is the timeline? Has an identifiable start and stop date (or period of time) been identified? Can you build in a cushion for unexpected interruptions?

Appetite/Tolerance — Appetite refers to a broad-based description of the desired level of risk that an entity will take in pursuit of its mission.[13] Tolerance reflects the threshold or qualitative range of risks taken in pursuit of strategy or variation in outcomes. Set by the board and senior management, risk appetite and tolerance are inextricably linked with the organization's strategic plan and are key components of an ERM program. Therefore, they differ by organization and in the amount and type of risks accepted to achieve desired results. They are most often expressed as statements accompanied by qualitative and quantitative parameters. As with other program components, they require continuous monitoring and may require revisions to sync with current or changing strategy. Appetite and tolerance statements can address the organization as a whole, or be specific to an individual strategy, unit or division.

ERM Structure & Plans — The Governing Body will review and approve the ERM plan and advise on the framework and structure, offering input where necessary. The ERM plan will identify the roles and responsibilities of the Board, leadership team, key committees organized to manage the ERM program, such as a Steering Committee, an Oversight Committee or a Work Group, and key departments such as: Strategic Planning; Internal Audit; Compliance; Risk Management; Capital Budgeting; and Acquisitions and Development. Additionally, the ERM plan may emphasize the specific responsibilities of key positions and could include: the Chief Risk Officer (CRO), Chief Financial Officer (CFO), Chief Digital/Information Officer (CDO/CIO), and the Chief Executive Officer (CEO).

Communication & Reporting Plans — Historically, the lynchpin of all risk management programs has been education. The implementation of an ERM program has the same, if not heightened, need for organizational-wide communication and education plans that:

- Underscore how the ERM program is to be initiated offering a detailed timeline for implementation
- Provide descriptions for all key roles and Committee structures

- Detail activities to educate, inform, and engage all employees
- Describe techniques to update all employee as to the Program's progress and outcomes
- Detail Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) by which the program will be routinely evaluated and monitored
- Sustain the program's viability and credibility by offering business-case scenarios that highlight value creation

Oversight — Regardless of the delivery setting, the organization's Governing Body is responsible for ERM program oversight. On a routine basis, status reports should be developed by senior leadership, the Executive Risk Committee or the ERM Working Group to educate and update the Governing Body on items specific to:

- Progress on risk strategies implemented
- Status on KPIs and KRIs
- Emerging risks
- Recommendations for new projects

ERM Process

Enterprise Risk Management is a business decision making process to identify and manage uncertainty. The process used in ERM programs is the same as that used in traditional risk management programs, except that now the risk management professional looks to create value and optimize risk opportunities not just preserve assets. The steps in the risk management process (or a variety thereof) include: risk and opportunity identification, risk evaluation and assessment, strategic risk response and implementation, and review, evaluation and monitoring. These steps will be reviewed in more detail.

Risk & Opportunity Identification

A variety of methodologies are available to assist in both risk and opportunity identification, including an array of tools, processes and systems. Tools can be formal or informal[14] and can be retrospective, concurrent, prospective, and pre-interventional.[15]

The following are a few of the various tools available:

- Strategic Plan
- Adverse event reporting
- Consultant reports and inspections
- Committee reports
- Staff meetings and departmental reports
- Root Cause Analysis (RCA)
- Failure Mode, Effects, & Criticality Analysis (FMECA)[16]
- Peer review and quality outcome data
- Questionnaires
- Brainstorming
- Focus Groups
- Interviews
- National Quality Forum's (NQF) serious reportable events (SREs)[17]
- The Joint Commission Sentinel Event Alerts[18]
- Patient satisfaction surveys
- IHI Global Trigger Tool[19]

Uncertainty can best be seen in this stage of the process. Where are the risks; and can they in turn create value? When reviewing risk information from any source it is an ideal time to look not only for risks, but also

for opportunities that have the capacity to create value. Examples might include: improved relationships with stake/shareholders, community, patients, and providers; increased market share; improved quality outcomes; deceased turnover; enhanced patient satisfaction; and improved communication and reporting that promotes transparency.

Risk List

As risks and opportunities are identified they should be preserved on a master list commonly referred to as a "risk list." A risk list is simply a listing, in no particular order, of all risks and opportunities identified through the myriad tools, processes and systems (identified earlier in this paper) that capture risks to the organization. At this point in the process, no assessment as to likelihood or impact is done on the risk and opportunities listed.

Domains

Risk domains[20], also referred to as categories or areas of risks, are simply a method used to segregate similar risks into manageable groupings. It is one way to sort or classify risks, keeping in mind that many, if not most risks, will fall into several domains. For example: the risk associated with work-related employee injuries is generally grouped with other risks within the Human Capital domain—a broad term to describe what used to be known as human resources, or personnel. However, keep in mind that employee injuries also have a financial cost to the organization overlapping with the financial domain and could have a regulatory component if mandatory workplace rules are breeched thereby overlapping in the Legal / Regulatory domain. The use of domains encourages a more comprehensive view of risks versus a silo approach and reminds us that there are risks beyond Clinical / Patient Safety risks. This process also might serve to help identify where support and leadership for other departments might be necessary. The use of risk domains visually display related risks or a family or risks so that synergistic relationships become apparent and are easily viewed.

Once the risks to the organization have been identified, assessed and strategies for value protection and value creation have been developed, the utility of risk domains is diminished. They have a distinct and limited purpose and are only one tool in a box of many.

Table 2 identifies the eight ASHRM-supported domains with accompanying definitions and examples. These domains represent typical categories of risks specific to healthcare. But domains are no different from other structural elements in ERM in that they must be personalized and made unique to the organization. Some industries use only two or three domains, while others expand the list to include areas such as market share, brand and reputation. Risk domains should take into consideration an organization's major risks, contracting or expanding them where necessary.

Risk Drivers

Risk management professionals look to identify factors that can create risks. Factors may be classified as either internal or external to the organization, and can exaggerate or minimize risks. Each risk and opportunity identified will have its own set of drivers. Examples of internal risk drivers might include;

TABLE #2		**RISK DOMAINS**
Domain		**Description / Example**
1	Operational	The business of healthcare 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.
2	Clinical / Patient Safety	Risks associated with the delivery of care to residents, patients and other healthcare customers. Clinical risks include: failure to follow evidence based practice, mediation errors, hospital acquired conditions (HAC), serious safety events (SSE), and others.
3	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.
4	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.
5	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 employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity and compensation. Human capital associated risks may cover recruitment, retention, and termination of members of the medical- and allied-health staff.
6	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.
7	Technology	This domain covers machines, hardware, equipment, devices and tools, but can also include techniques, systems and methods of organization. Healthcare 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) and Meaningful Use, social networking and cyber liability.
8	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: facility management, plant age, parking (lighting, location, and security), valuables, construction/renovation, earthquakes, windstorms, tornadoes, floods, fires.

resource availability (or lack of), distraction from task (employee fatigue, inattentional blindness[21], interruptions), and organizational culture. An organization's culture as a risk driver can have a positive or negative impact on risks and opportunity. Examples of external drivers may include: governmental mandates, rules and regulations, competition, activities to unionize, natural disasters, terrorism, and fluctuations in the availability of key personnel. If the organization can manage external drivers, risks may be turned into opportunities.

Emerging Risks

Many organizations take time to understand their market, appropriately evaluate their competition, apply best practice to all mergers, acquisitions and divestitures, analyze large data to both evaluate current practice and create advantages, and forecast trends. These efforts allow them to identify emerging risks and to develop appropriate strategic responses in a timely manner. Keep in mind that predicting all risks is not possible and we will continue to see those events considered to be a "Black Swan".

Black Swan events are those considered to have a low likelihood of occurring, but when they do occur their impact is catastrophic. Another characteristic is that they are impossible to predict. According to an article in the Harvard Business Review[22], "Instead of trying to predict low-probability, high impact events, we should reduce our vulnerability to them." Through proactive efforts to identify emerging risk, the organization will become resilient and better positioned to weather an adverse event should one occur.

Risk Evaluation & Assessment

Once a list of risks to the organization has been identified and memorialized on the risk list, the risk management professional should start the assessment process by reviewing this risk list (keeping in mind, at this point, it could be quite voluminous) to look for similar/same risks (redundancy) noted by multiple people or by different departments. These risks should be combined - reducing the list to a more manageable number. The risk list should also be reviewed to identify opportunities for cost-effective, easily implemented mitigation strategies (low-hanging fruit). Implementing these *quick fixes* will give the ERM Program some immediate "wins" which can be used to engage the employees and inform them about the ERM Program. Further analysis of the risk list will identify risks that have effective risk mitigation strategies already in place. There is no reason, other than verifying that the strategies are still effective, to devote time to risks already being managed. These risks are considered to be *residual* risks and less emphasis is spent on them as opposed to inherent risks or risks before any mitigation strategies are employed. The risk management professional should be alert to opportunities to eliminate redundancy, identify risk correlations both positive and negative recognizing the synergistic effect risks have upon each other, and conserve resource consumption wherever possible. See Table #3: *Sample Risk List*.

TABLE #3		Sample Risk List				
Strategic / External	**Operational**	**Human Capital**	**Financial**	**Legal & Compliance**	**Technology**	**Hazard**
• Competition • Affiliation, Mergers & Acquisitions • Variability in Patient-Related Volume • Research Grant / Funding Availability • New Models for Care Delivery • Diminished Market • Regulatory Change / Healthcare Reform • Conflict of Interest • Decreased Capital Spending • Hospital / Physician Relationship • Availability of Public Data (HAI/HAC)	• Business Management Discipline / Cost Management • Equipment Maintenance • Failure to Identify & Follow EBM • Facility Maintenance • Timely Access to Care • Failure to Refer • Failure to Diagnosis • Clinical Continuity • Insufficient Discharge Planning • Inconsistent Clinical Competency	• Hiring & Retention • Organizational Structure, Alignment & Direction • Succession Planning • Unionization • Turnover • Recruitment • Aging Workforce • Disruptive Behavior • Flex Staffing • Workers' Compensation • Physician Shortage	• Credit / Collections • Financial Performance • Billing Accuracy / Compliance • Payer Mix / Reimbursements • Pension / Retirement Obligations • Philanthropy / Fundraising / Capital Campaign • Failure to Meet Margin • Uncompensated Care • Access to Capital • Contract Management • Revenue Enhancement	• Conflicts of Interest • Fraud, Theft and Embezzlement • Governance, Compliance and Oversight • ACO • HIPAA Privacy & Security • Health Reform • Employment Practices	• Multiple Vendors • Social Networking • Information Breach • Bar Coding • Hybrid EMR • IT Infrastructure & Security • Paucity of IT Professionals • Failure to Act in a Timely Manner • Incompatible Programs	• Natural Disaster • Failure to Plan • Failure to Act Timely • Inability to Manage a Crisis • No Backup Systems or Appropriate Duplicate systems

23

Risk Inventory/Risk Register

As the assessment process continues, the risk list will be used to create a more detailed document called a "risk inventory" and includes additional information such as the category or risk domain (keep in mind that a single risk can cross over into many different domains/categories). On the risk inventory, the risk management professional should choose the domain/category that has the most exposure, and the risk score including a numerical assessment of the likelihood and impact. See Table #4: *sample Risk Inventory*.

Refining the risk inventory into a manageable number of risks and to prioritize which require attention first, most risk management professionals use two dimensions to assess risk: likelihood and impact.

TABLE #4 ***SAMPLE* RISK INVENTORY**

Rank	Risk Name	Risk Domain	Likelihood	Impact	Risk Ranking
1	**Payer Mix / Reimbursements**	Financial	4.33	4.42	19.14 (Very High)
2	**Billing Accuracy**	Financial	4.33	4.25	18.41 (Very High)
3	**IT Infrastructure**	Technology	4.50	3.92	17.64 (Very High)
4	**Confidentiality / Data Security**	Technology	4.08	4.08	16.65 (High)
5	**Changing Nature of Healthcare**	Strategic	3.42	4.25	14.54 (High)
6	**Adequate Protocols, Controls & Policies**	Operational	3.42	3.92	13.41 (High)
7	**Cost Management**	Financial	3.08	4.08	12.57 (High)
8	**Recruiting & Retention**	Human Capital	3.50	3.50	12.25 (High)
9	**Safety & Security**	Operational	3.58	3.33	11.92 (High)
10	**Business Model / Services**	Strategic	3.17	3.75	11.89 (High)
11	**Facility & Equipment Management**	Hazard	3.83	2.92	11.18 (High)
12	**Employee Engagement**	Human Capital	3.17	3.50	11.01(High)
13	**Competition**	Strategic	2.92	3.75	10.95 (High)
14	**Quality of Care**	Patient Safety	3.17	3.42	10.84(High)
15	**Skills & Capabilities**	Human Capital	3.17	3.17	10.05 (High)
16	**Conflict of Interest**	Operational	3.42	2.92	9.99 (Medium)
17	**Population Health**	Strategic	3.17	3.08	9.76 (Medium)
18	**Support Staff / Staffing Levels**	Human Capital	2.91	3.08	8.97 (Medium)
19	**Capacity & Availability of Space**	Strategic / External	2.92	3.00	8.76 (Medium)
20	**Patient Needs**	Operational	3.08	2.75	8.47 (Medium)
21	**Compliance**	Operational	2.50	2.83	7.01 (Medium)

24

Likelihood also referred to as frequency or probability,[25] refers to the number of times an adverse event or occurrence (a risk) will happen. This dimension is expressed in terms of a number or ratio.

Impact also referred to as severity, refers to the anticipated outcome of the risk if it occurs. Impact is most often referenced in financial terms (dollars $) and can also be referred to as “vulnerability”, “consequences”

or "costs". In some healthcare organizations, impact also refers to the level of harm (or potential harm) to a patient.

An additional or third dimension that is often used to further evaluate and assess risk is velocity. Velocity, also known as "the time to impact", refers to the speed of action or of an event occurring, time in which you have to take action, realize the outcome of a risk occurring or the duration of the event. As an example, contrast the velocity of an earthquake and a hurricane. Earthquakes offer no warning and there is little time in which to respond making contingency planning imperative. With an impending hurricane, weather forecasters give the public time to respond by offering appropriate warning and a watch notices.

Risk Scales refer to a numerical scoring system used to rank or prioritize risks based on the key dimensions usually likelihood and impact. Other dimensions in addition to velocity can include the impact on reputation, brand and/or market share. Risk scales can be developed for individual domains (i.e., finance, patient safety, human capital, etc.) or organization-wide based on risk appetite. A Likert scale ranking of one (1) to five (5) is most often used. With 1 being the lowest, least likely to occur, or least impactful. Using the range of 1 to 5 for both dimensions the highest ranking is 25. If velocity is used as a third dimension, a Likert scale of 1 to 3 is most often used with 3 being the least amount to time to respond, or minimal advance warning or longest period of time to recover. As an example, a hurricane may be a 2 on the risk scale while an earthquake would be a 3.

Risk Scores are generated for each significant risk and prioritized in numerical order. To determine the ranking the likelihood score is multiplied by the impact score to determine the risk score.

Likelihood x Impact = Risk Score

If velocity (time to impact) is added to likelihood and impact as a third dimension to generate a risk score the formula is:

Likelihood + Velocity x Impact = Risk Score

A Risk Map is a graphical display of risks and accompanying risk score plotted on an "X" and "Y" axis utilizing the above two key dimensions of frequency and severity. It is sometimes referred to as a "heat map" because of the color display of risk (red – critical, yellow – medium risk and green – risks that are less significant). See Graphic #3: *Sample Risk Map*

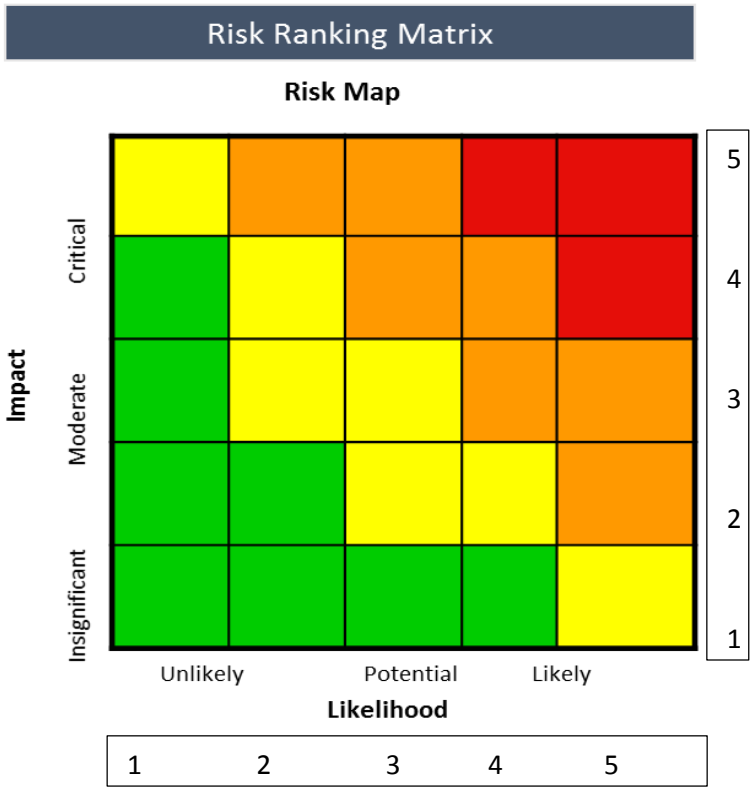
After the risk scores have been entered on the risk inventory tool and prioritized by order of significance (risk ranking), and graphically depicted on a risk map/heat map, many risk management professionals will make a more comprehensive assessment of the top 20 to 25 risks that offer the potential to effect strategy and the attainment of objectives. This furthers analysis is captured on what is referred to as a "risk register." Besides information already populated from the risk inventory tool, additional information depicted on a risk register might include: risk drivers both internal and external to the organization, risk response including value preservation (risk control and risk financing), and opportunities for value creation and enhancement.

Other data elements that could be added to the risk register include: the effectiveness of risk mitigation efforts, what mitigation efforts are needed, challenges and benefits, responsible party, action plans and

implementation timelines. Keep in mind that these templates (risk list, risk inventory and risk register) are tools to assist in the recording of information, in and unto themselves they offer no value.

It is the effective and efficient use of the information contained within these tools that is of importance and will be helpful in developing an appropriate and specific ERM program for your organization.

GRAPHIC #3 SAMPLE RISK MAP



26

Risk Rankings	
Risk is ranked as…	***…if the product of Impact & Likelihood is…***
VERY HIGH	Greater than ***17.0***
HIGH	Greater than ***10.0***, but less than ***17.0***
MEDIUM	Greater than ***5***, but less than ***10.0***
LOW	Less than ***5.0***

Table #5 offers an example of what a simple risk register might look like.

TABLE #5			Risk Register					
Risk Name	Category / Domain	Risk Defined	Likelihood (L), Frequency, numbers #, Probability	Impact (I), Financial severity $, harm index	Risk Score (RS) L x I = RS	Risk Drivers (Internal & External)	Risk Response (in place & needed)	Opportunity to Create, Enhance Value
1.								
2.								
3.								

Risk evaluation and assessment brings clarity to the decision-making process and is necessary to assist organizations in allocating appropriate and effective resources for strategic risk response strategies. Determining which risks require attention and how to promote value are important aspects of this step in the risk management decision-making process.

Strategic Risk Response

Once an organization identifies, analyzes, and assesses the risks it encounters and identifies the potential for creating value, the next step is to take action by the development and implementation of effective and efficient risk response strategies. There is no one technique that if employed will manage all risks offering both value protection and value creation. A combination of techniques is necessary and includes both risk control and risk financing strategies. See Table #6: *Techniques to Manage Risks*. Together these techniques offer the protection of valuable assets while recognizing value and are considered to be both proactive and reactive.

TABLE #6	Techniques to Manage Risks
Risk Control Techniques	**Risk Financing Techniques**
1. Avoidance 2. Prevention 3. Reduction 4. Segregation 5. Non-Insurance Transfer	1. Retain – Self-insure 2. Transfer – Insurance 3. Non-Insurance Transfer

A major difference between a traditional risk management program and the organization-wide ERM programs is the effort to create and recognize value. Previously, the majority of effort was spent on value protection and other reactive strategies to mitigate risks. Little knowledge of the effect of uncertainty on value was understood and therefore not captured or enhanced. Value if created was serendipitous, unplanned and solely by chance. ERM programs change that dynamic and consider value creation, recognition and enhancement on the same level as value protection.

The appropriate deployment of strategic risk response solutions becomes a critical function given limited resources and other competing priorities many of which are unfunded and unstaffed. The minimization of variability in care practices, reduction in duplicate efforts by differing units and departments, and a decrease in the volume of work to be redone can all help improve efficiency.

When dealing with uncertainty, the ability to make informed decisions supportive of the organization's strategic goals and objectives is tantamount to success. Quantitative support for decision-making and project implementation is becoming an essential ERM skill set. It is incumbent upon risk management practitioners to develop these skills or identify those with decision-analysis expertise and to partner with them.

Decision Analysis

"Rules of thumb, intuition, tradition, and simple financial analysis are often no longer sufficient for addressing such common decisions as make-versus-buy, facility site selection, and process redesign. In general, the forces of competition are imposing a need for more effective decision making at all levels in organizations."[27]

Decision analysis takes many forms and has differing schools of thought. Simply put, it is the ability to make rational decisions by understanding and analyzing the benefits (rewards/value) and disadvantages (cost/risks) of taking a particular action as compared with the benefits (rewards/value) and disadvantages (costs/risks) of not taking a particular action. In this manner, alternatives are evaluated and decisions are made that are guided, informed and structured.

A few factors should be noted:

- There is one decision maker (someone has the final decision)
- Decisions involve action on the part of the decision maker
- Decision analysis involves probabilities and outcomes
- There are often many alternatives to analyze and from which a course of action is chosen
- Better decisions have better data/information
- Consideration of the organization's Guiding Principles should be part of decision analysis
- The anticipated (and real) return on the decision is considered the payoff
- Decisions and payoffs should be measurable
- Understand the importance that emotion has in decision making, particularly when dealing with those who impact patient safety. Can something be legally right and morally wrong?
- Decisions should be analyzed in both the short and long terms (organization to determine timeline)
- The risk manager is usually the decision analysis facilitator outlining alternatives and benefits

Cost-benefit analysis and risk-reward analysis are familiar terms to most risk management professionals. With a cost-benefit analysis the decision analyst takes into account the total anticipated cost of a project as compared with the projected or perceived benefit/value. Similarly, under a risk-reward scenario, the risk inherent in undertaking a project is evaluated and quantified in relation to what the expected reward or payoff is in terms of dollars. Both techniques are used in healthcare to assist in making more informed decisions.

Data analytics and the use of big data support healthcare efforts to create value, drive decisions, improve outcomes, and offer a competitive advantage — all value propositions. Healthcare organizations for the most part have the capacity within their systems to accommodate vast amounts of data. As early as 2001, analyst Doug Laney described three characteristics that made data "big" and called them the 3 V's: volume (amount of data); velocity (the speed at which data is produced or generated); and variety (types of data generated

and produced).[28] Current descriptions of "big data" include additional characteristics not previously described and include.[29]

- Validity — Addresses reliability
- Venue — Describes complexity from a high diversity of data sources
- Visualization — Putting complex data sets into actionable form
- Value — Realizing real business value on a repeatable basis

A human capital concern with decision analysis, data analytics, and the use of big data for business intelligence is the paucity of professional skills in this area. Data scientists and data professionals skilled in healthcare and IT are few and far between and very much in demand.

Armed with informed, deliberate, well thought out strategic risk-response solutions, the risk management professional can then oversee their implementation.

REVIEW/EVALUATE/MONITOR

The final step in the risk management decision-making process is the continuous review, evaluation and monitoring of the ERM program. Embedded in this step is the recognition of value that is created throughout the process. Routinely addressing the following questions will simplify the more formal annual review of the program:

- Is the program meeting current needs?
- Is there an assigned professional responsible for the ERM program?
- Are current strategies evaluated in light of emerging or previously unknown risks?
- Have significant risks to the organization been identified and addressed?
- Have you had any major, unanticipated risks occur for which you were unprepared?
- Have lessons learned been incorporated into new strategies for improvement?
- Do all employees know their role and do they all participate in the ERM program?
- Do all strategies and solutions developed to address risks have criteria built in by which their success or failure will be evaluated?
- Do all implemented strategies have an assigned responsible party?
- Are all strategies reviewed periodically to determine whether the strategy is still appropriate for the risk?
- Is the ERM program tied in with strategic planning?
- Are all strategies and solutions reviewed for value-creation opportunities?
- Has the organization created a competitive advantage, improved market share, enhanced morale, improved community reputation or realized other value from implementation of the ERM program? Are these shared on a real-time basis with employees?
- Are the Board and senior leadership team routinely apprised of ERM program status?
- Are risk controls evaluated and modified if necessary in light of organizational (mergers, acquisitions or divestitures) or environmental (terrorism, pandemic, competition) changes?
- Are risk appetite and tolerance statements developed; and is adherence ensured?
- Are Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) developed and reviewed as monitors for the ERM program? [30]

Answering these questions will help you to evaluate your ERM program's implementation — and to make mid-course changes, if necessary. On a more formal basis and for internal and external reporting most ERM programs are evaluated at least yearly. This evaluative report will offer status on:

- Risks identified
- Progress on, and results of, risk-response strategies and solutions implemented
- Barriers and challenges to the success of the ERM program
- Improvement opportunities
- Program changes
- Lessons learned
- Goals and objectives for the next year

Business case scenarios are an additional tool and are valuable in delivering the message to wide internal and external audiences. Of particular interest and a feature specific to ERM programs is the report section on value creation and recognized opportunities to enhance benefits and rewards while reducing risks and costs.

CONCLUSION

The Framework — as described and developed by ASHRM for the development and implementation of healthcare Enterprise Risk Management programs — offers a flexible structure to guide and support risk management professionals as they tackle the task of advancing and evolving traditional risk programs into sophisticated, organization-wide, ERM programs. This Framework identifies key structural components and will assist with the planning and design of ERM programs focused on value protection and creation.

END NOTES:

[1] *Accountability is one of the major keys to attaining desired results. Lack of clarity around a project, responsibilities, or goals often leads to inadequate communication, inefficient results, and unmet goals. Accountability involves assigning clear responsibilities and ownership around all parts of a project or risk, not just at the senior executive level, but also pushed down through the business unit, the business process or the function, to the risk owner.* "Add Spreadsheets to Your Inventory". July 2009 available online at: www.irmi.com

[2] As stated in A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000. @AIRMIC, Alarm, IRM: 2010 "*Risk Management should be a continuous process that supports the development and implementation of the strategy of an organization*" p.6

[3] Carroll. RL, *Enterprise Risk Management: The Impact on Healthcare Organizations*, Ch11, 115, in Principles of Risk Management and Patient Safety, Barbara Youngberg ed. (2011) Jones & Bartlett Learning

[4] The terms "Governing Body" and "Board" are used throughout this paper and are meant to refer to the collective body (also known as Trustees, Governing Council, and Authority) responsible for setting the ERM Strategy, approving the ERM Plan and Framework, and ERM Program Oversight. The Governing Body can be elected or appointed, and be voluntary or paid positions.

[5] Developed by ASHRM's ERM Task Force (now an Advisory Committee) and adopted by the Board of Directors Sept. 19, 2012.

[6] COSO (Committee of Sponsoring Organizations of the Treadway Commission) is a voluntary council with members from five accounting organizations representing a cooperative effort between the American Institute of Certified Public Accountants, American Accounting Association, the Financial Executives Institute, the Institute of Internal Auditors, and the Institute of Management Accountants. For more information, go to http://www.coso.org. COSO defines ERM as "a process, affected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

[7] Carroll RL. *Enterprise Risk Management – What's It All About*? In Carroll RL editor in-chief, Nakamura PLB, Rose R, editors. Enterprise Risk Management Handbook for Healthcare Entities. 2nd ed. Washington (DC):
AHLA/ASHRM; 2013:6 AHLA in the Enterprise Risk Management Handbook for Healthcare Entities, 2nd edition offers a definition of ERM as: "…an on-going business decision-making process instituted and supported by the healthcare organization's board of directors, executive administrative and medical staff leadership. ERM recognizes the synergistic effect of risks across the continuum of care, and has as its goal to assist the organization reduce uncertainty and process variability, promote patient safety and maximize the return on investment (ROI) through asset preservation, value creation, and the recognition of actionable risk opportunities

[8] RIMS defines enterprise risk management as a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio. RIMS Executive Report *The Risk Perspective "*An Overview of Widely used Risk Management Standards and Guidelines" 2011

[9] ISO 31000:2009 Risk management "Risk management is an integral part of all organizational processes". "[It] is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes."
Source: Council of Standards Australia on Nov. 6, 2009 and the Council of Standards New Zealand on Oct. 16, 2009. From a Presentation "Enterprise Risk Management: COSO, New COSO, ISO 31000" prepared by:
Dr. Hugh Van Seaton, Ed. D., CSSGB, CGMA, CPA

[10] Tim Scott, Russell Mannion, Huw Davies, Martin Marshall. *The Quantitative Measurement of Organizational Culture in Health Care: A Review of the Available Instruments.* Health Services Research (HSR) June 2003; 38(3): 923-946

[11] Rapid Business Intelligence Success. A definition of Business Strategy available at: http://www.rapid-business-intelligence-success.com/definition-of-business-strategy-html

[12] SMART goals first appeared in a November 1981 issue of Management Review (vol. 70, issue 11) (AMA- FORUM) pp 35-36, in an article titled 'There's a S.M.A.R.T. way to write management's goals and objectives.' by George Doran, Arthur Miller, and James Cunningham.

[13] COSO Strengthening Enterprise Risk Management for Strategic Advantage, 2009

[14] Formal Methods – Systems, processes, programs, methods, reports and/or policies and procedures for which the primary purpose is the early identification of adverse or unexpected patient outcomes and hazards and value opportunities. Informal Methods – Systems, processes, programs, methods, reports and/or policies and procedures for which the identification of adverse patient outcomes or hazards and opportunities to create value are not the primary purpose.

[15] The four methods to identify risk are: Retrospectively = Based on Information from past events, Prospectively = Based on an analysis of likely potential exposures, Concurrently = Based on real-time monitoring of situations and events, Pre-interventional = Based on information collected in relation to a specific situation just prior to commencing action or treatment.

[16] Failure Modes and Effects Criticality, Analysis (FMECA) is a systematic, proactive method for evaluating a process to identify where and how it might fail, and to assess the relative impact of different failures in order to identify the parts of the process that are most in need of change.

[17] National Quality Forum (NQF), Serious Reportable Events In Healthcare—2011 Update: A Consensus Report, Washington D.C., NQF; 2011

[18] "A sentinel event is an unexpected occurrence involving death or serious physical or psychological injury, or the risk thereof. Serious injury specifically includes loss of limb or function. The phrase, "or the risk thereof" includes any process variation for which a recurrence would carry a significant chance of a serious adverse outcome. Such events are called "sentinel" because they signal the need for immediate investigation and response". For more information see Sentinel Events at: http://www.jointcommission.org/sentinel event.aspx

[19] Institute for Healthcare Improvement Global Trigger Tool available at: http://www.ihi.org/resources/Pages/Tools/IHIGlobalTriggerToolforMeasuringAEs.aspx Site accessed July 15, 2014

[20] Adopted from ASHRMs Risk Management PEARLs #1 *Enterprise Risk Management – The Foundation*. Chapter 3 The Eight Risk Domains of ERM pp 20-23. 2013 Edition

[21] "…the person performing the task fails to see what should have been plainly visible, and later, they cannot explain the lapse" ISMP Acute Care - ISMP Medication Safety Alert. Feb. 26, 2009 Issue available at: http://www.ismp.org/Newsletters/acutecare/articles/20090226.asp Site accessed July 15, 2014

[22] Nassim N. Taleb, Daniel G. Goldstein, Mark W. Spitznagel. *The Six Mistakes Executives Make In Risk Management*, Harvard Business Review October 2009 pp 78-81

[23] Developed for the ASHRM Essentials Module Program by Roberta Carroll – Reprinted with permission

[24] Developed for the ASHRM Essentials Module Program by Roberta Carroll – Reprinted with permission

[25] Probability when used in this context is subjective, not quantifiable

[26] Developed for the ASHRM Essentials Module Program by Roberta Carroll – Reprinted with Permission

[27] Professor Hossein Arsham. *Tools for Decision Analysis: Analysis of Risky Decisions* available online at: http://home.ubalt.edu/ntsbarsh/business-stat/opre/partIX.htm, Site accessed Aug. 18, 2014

[28] Doug Laney *3D Data Management: Controlling Data Volume, Velocity and Variety*. Application Delivery Strategies. Meta Group. Feb. 6, 2001

[29] Deloitte Tech Trends 2013 – *Enablers Finding the Face of Your Data* available at: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Services/Consulting/uk-con-finding-face-of-data.pdf

[30] For more information on RPIs and KRIs read the three ASHRMs PEARLS on ERM. To purchase go to www.ashrmstore.org or call 800- 242-2626