ASHRM
AMERICAN SOCIETY FOR HEALTH CARE RISK MANAGEMENT

# ENTERPRISE RISK MANAGEMENT: Implementing ERM

**Editors**:

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

Ann Gaffey, RN, MSN, CPHRM, DFASHRM

**Contributors:**

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

Franchesca J Charney, RN, MS, CPSO, CPPS, CPHRM, DFASHRM

Jeffrey Driver, JD, MBA, DFASHRM

Michelle Hoppes, RN, MS, AHRMQR, DFASHRM

Teresa Kielhorn, JD, LLM

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

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

Barbara J. Youngberg, BSN, MSW, JD

AHA Data & Insights

The American Society for Health Care Risk Management (ASHRM)
of the American Hospital Association
155 North Wacker Drive, Suite 400
Chicago, IL 60606
(312) 422-3980

ASHRM@aha.org
www.ASHRM.org

To view additional ASHRM white papers, visit www.ASHRM.org/whitepapers

ASHRM provides this document as a service to its members. The information provided may not apply to a reader's specific situation and is not a substitute for the application of the reader's independent judgment or the advice of a competent professional. Neither ASHRM nor any author makes any guarantee or warranty as to the accuracy or completeness of any information contained in this document. ASHRM and the authors disclaim liability for personal injury, property damage or other damages of any kind, whether special, indirect, consequential or compensatory, that may result directly or indirectly from use of or reliance on this document.

## TABLE OF CONTENTS

**Abstract:** Health care 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 adopted an ERM definition and an ERM Framework for use in health care. This framework is based on that developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2017. This white paper will graphically display the Framework and describe key structural components necessary in any health care  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

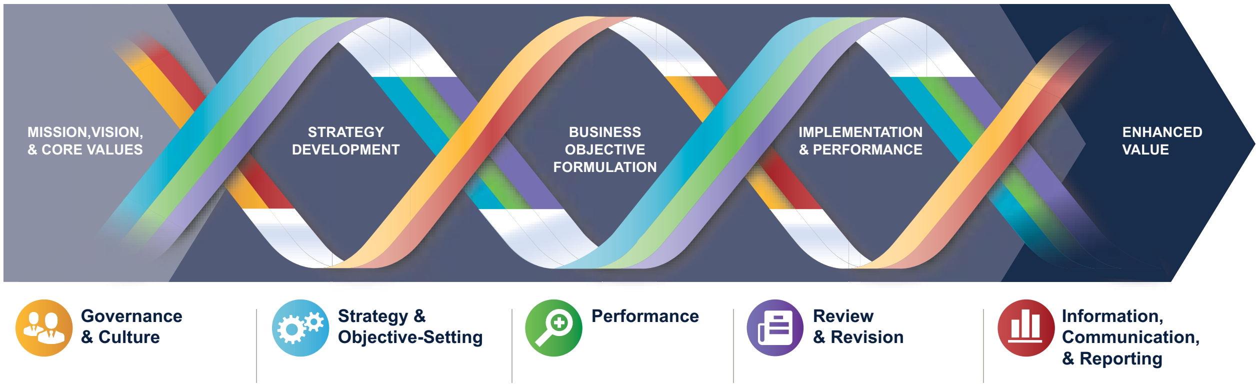
The advancement of Health Care  Enterprise Risk Management is a key initiative in ASHRM's Strategic Plan for 2019-2021. The implementation and maturity of ERM programs in health care organizations—while making significant strides—still lag behind organizations in other industries; most financial services organizations and most public companies. Although many health care 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 adoption 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 health care organizations. It outlines the COSO framework, which ASHRM aligns with, and highlights structural components to support a solid foundation, promote program credibility and success, and advance ERM principles throughout your health care  organization.

## FRAMEWORK

The Framework, as illustrated in this paper (See Figure 1) COSO 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 and principles shown in the sample Framework are relevant to any health care 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 risk management professionals 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 health care ERM program. Once a Framework to address the specific needs of the organization is developed, creating program success building blocks can be developed and implemented following reporting.

Figure 1: COSO ERM Framework


MISSION, VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

## GUIDING PRINCIPLES

**Governance & Culture**

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

**Strategy & Objective-Setting**

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

**Performance**

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

**Review & Revision**

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

**Information, Communication, & Reporting**

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

*Source: ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.*

## GOVERNANCE AND CULTURE

The Governing Body of each health care 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 of risk appetite and assessing risk capacity
- Establishing ERM operating and reporting structure
- Approving the ERM plan, including plans for ERM education and communication
- 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 health care 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." Developed by ASHRM's ERM Advisory Committee and adopted by the ASHRM Board on September 19, 2012

Other credible organizations such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO), The American Heath Lawyers Association (AHLA), the Risk and Insurance Management Society (RIMS), and the International Organization of Standardization – ISO 31000:2009 have all defined ERM, albeit differently. See the Endnotes for those definitions. See Figure 2 for terms and complimentary descriptions.

Figure 2: Terms & Complimentary Descriptions

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

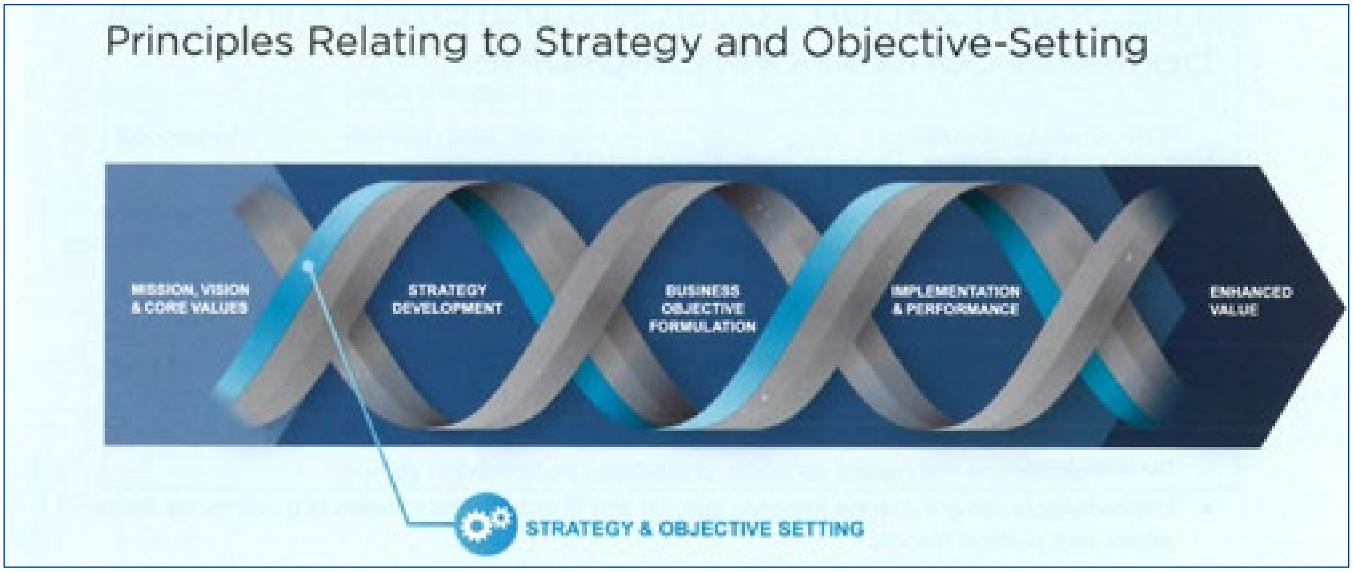
Culture is a key element in program implementation and organizational readiness. The Governing Body is responsible for "setting the stage" to ensure the organization's culture will support the ERM program. Organizations that adopt fear as a practice, engage in tactics that are not conducive to a learning 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 to quality outcomes, performance and employee satisfaction. However, no culture assessment instrument measures all three dimensions easily.[1] 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 in pursuit of an organization's mission, vision and core values.[2] In years past, an organization's Board of Directors, in concert with senior leadership, may have drafted a 5-10 year strategic plan. With the growing complexity and rapid changes to health care delivery models, technological innovation and regulation. Organizations may plan only two to three years ahead and focus on only the next few month's operations. They rely on committees, engage additional staff, 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 Figure 3: Strategy and Objective-Setting).

Figure 3: Strategy and Objective-Setting


Principles Relating to Strategy and Objective-Setting
MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
STRATEGY & OBJECTIVE SETTING

*Source: ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.*

**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[3] goals.

The acronym SMART describes the five key attributes of effective objective setting:

- **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?

**Risk Appetite and Risk Capacity**

Appetite refers to a broad-based description of the desired level of risk that an entity will take in pursuit of its mission.[4] Set by the board and senior management, risk appetite is inextricably linked with the organization's strategic plan and is a key component of an ERM program. Risk appetite reflects the size and mission of the organization, organizational culture and financial position and describes the amount and types of risk that the entity is willing to accept to achieve its strategic aims and business objectives and may be described in qualitative and/or quantitative terms. Risk capacity is an assessment of the total composite amount of risk from all sources that an entity is capable of assuming. Risk appetite and risk capacity are related, although somewhat independent concepts; some organizations are capable of taking a significant amount of risk (high risk capacity), but may elect to assume much less (low risk appetite) based on their culture or mission. Other organizations may be less risk averse and willing to accept significant uncertainty in pursuing their strategies and objectives (high risk appetite), but unable to do so because their risk capacity is more limited, due to poor financial performance, high levels of existing debt or the previous assumption of considerable amounts of risk. Risk appetite and risk capacity statements are most often expressed as statements accompanied by qualitative and quantitative parameters. As with other program components, risk appetite and risk capacity statements require continuous monitoring and may need revision to sync with current or changing strategy or financial position. Risk appetite statements and risk capacity analyses, which is a tactic to outline of what needs to be done to ensure certain deliverables are met, typically may be made specific statements can address the organization as a whole, or be specific to an individual strategy, unit or division of the organization.

### ERM Structure & Plans

The Governing Body should review and approve the ERM plan and advise on the framework and structure, offering input where necessary. The ERM plan identifies 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 such as: the Chief Risk Officer (CRO), Chief Financial Officer (CFO), Chief Digital/Information Officer (CDO/CIO), and the Chief Executive Officer (CEO). In addition to the ERM Plan, many health care organizations develop a task-specific annual ERM Work Plan, detailing individual action items to be completed in implementing and developing the ERM process with target competition dates. While both types of ERM plans should be reviewed at least annually, the ERM Plan may remain relatively static absent major changes in program organization or reporting structure while ERM Work Plan activities, which is a tactic to outline what needs to be done to ensure certain deliverables are met, tend to vary more widely year-to-year, especially in the early stages of ERM program development and implementation. Which is a tactic to outline of what needs to be done to ensure certain deliverables.

### 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 the risk management principles to identify and manage uncertainty. The risk management principles used in ERM programs is the same as that used in traditional risk management programs, except now the risk management professional looks to create value and optimize risk opportunities not just preserve assets and risks outside of clinical and patient safety concerns and insurable exposures are considered. 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 and can be retrospective, concurrent, prospective, and pre-interventional.

The following are a few of the various identification methodologies 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)
- Peer review and quality outcome data
- Questionnaires
- Brainstorming
- Focus Groups
- Interviews
- National Quality Forum's (NQF) serious reportable events (SREs)
- The Joint Commission Sentinel Event Alerts
- Patient satisfaction surveys
- IHI Global Trigger Tool

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.

## KPI's, Performance Measurement, KRI's and Tolerance

Performance measurement is a key concept in ERM programs. Key performance indicators (KPIs) should be developed for each risk identified on the risk list to measure whether the organization is meeting its strategic goals and important business objectives on an on-going basis. By measuring actual performance against performance targets, gaps to be closed and corrective action required to be taken can be revealed. Such performance monitoring and measurement helps the organization to avoid the risk of not meeting important objectives required to keep the organization on track to successfully implement its strategic aims and ultimately fulfill its mission. It is often helpful to specify risk tolerances for each KPI, indicating the acceptable amount of variation from target performance that is allowable before corrective action is required or the objective is deemed not to have been met. For example, an organization may have a strategic goal of maintaining 30% market share in a specific geographic area. While a market share of 29% might not be deemed to be particularly problematic, anything below 25% may trigger an analysis of why the entity is failing to achieve its market share goal and the implementation of additional strategic initiatives aimed at improving its performance.

In addition to concurrently monitoring KPI results and implementing and measuring the success of subsequently taken corrective actions, ERM programs typically include an analysis of multiple key risk indicators (KRIs). KRIs are predictive in nature and aim to monitor developments likely to drive changes in the likelihood or impact of a given risk. In the above market share example, a key risk indicator may be the entrance of new competitors into a given market, which would likely dilute the organization's market share in the given geographic area. The emergence of new competitors may force the organization to develop additional strategies to maintain its existing market share or to reduce its market share targets to a more realistically achievable level. Like KPIs, KRIs may employ risk tolerances to determine significance. In the market share example, the opening of a small clinic by a competitor within the specific geographic area may not warrant additional action, while the competitor's building a new hospital in the area may trigger a greater response.

The risk manager should seek to utilize the expertise of the Board of Directors, senior leadership and other subject matter experts within the organization, as well as available outside expertise, to develop KPIs and KRIs and monitor performance. While the role of risk managers in ERM is to educate organizational leaders about performance measurement and to develop a process for data collection and reporting of KPIs and KRIs, risk managers themselves need not have the expertise to develop specific KPIs and KRIs or establish appropriate risk tolerances for every identified risk area.

### Domains

Risk domains, also referred to as categories or areas of risks, are simply a method used to segregate similar risks into manageable groupings. See Figure 4: ERM Domains developed for health care by ASHRM. 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

Figure 4: ERM Risk Domains

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

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 of 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.

Figure 4 identifies the eight ASHRM supported domains with accompanying definitions and examples. These domains represent typical categories of risks specific to health care. 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: resource availability (or lack of), distraction from task (employee fatigue, inattentional blindness, 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,[5] "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 well-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 Figure 5: Sample Risk List.

Figure 5: Sample Risk List

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

**Risk Inventory**
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. 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.

**Likelihood** also referred to as frequency or probability, 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 over a specific period of time.

**Velocity** is an additional or third dimension that is often used to further evaluate and assess risk. 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**

While the formula is helpful in providing a general assessment of risk priority, it needs to be employed with a certain amount of common sense. Risks that are almost certain occur, but are of very little consequence to the organization's strategic success, such as lost patient hearing aides and dentures, would typically have a risk score of 5 (Likelihood of 5 X Impact of 1=5). A risk with potentially catastrophic outcomes, but that is very unlikely to occur, such as a bioterrorism attack on a health care facility, would also likely receive a score a 5 (Likelihood of 1 X Impact of 5 =5). Obviously, most organizations would view these risks quite differently despite their having the same risk score. Due to the low risk score (5 out of a possible 25), neither risk would likely merit much consideration in an ERM context, however, most organizations would be more concerned about the bioterrorism risk because, even though very unlikely, it could potentially have devastating consequences for the organization should it occur, while the lost hearing aides and dentures, no matter how frequently they occur, hold no such potential.

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 Figure 6: 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." See Figure 7: sample 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.

Figure 6: Sample Risk Map/Heat Map/Risk Matrix

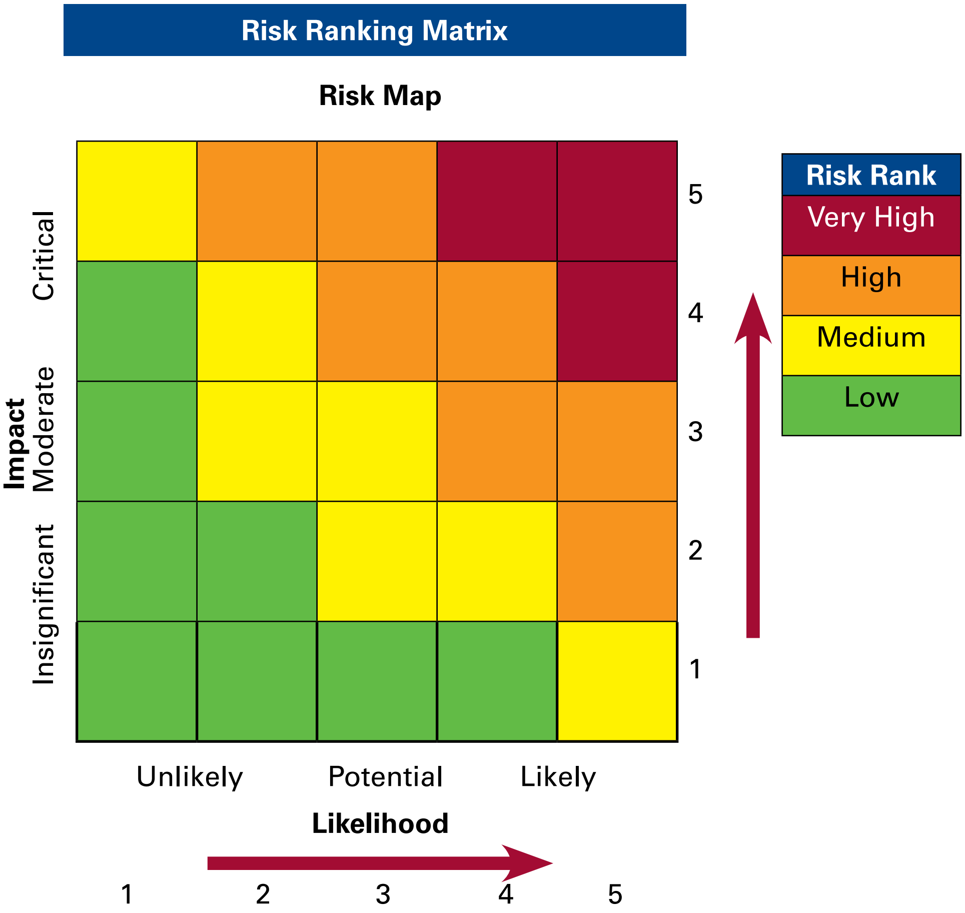


Figure 7: Sample Risk Register

**Risk Register**

| Identified Risk | Category/ Domain | Risk Description | Likelihood | Impact | Severity | Existing Risk Controls | Total | Contingent Actions | Owner | Status |
|---|---|---|---|---|---|---|---|---|---|---|
| | Hazard | Fire hoses are not present next to ER entrance | 4 | 5 | 3 | 4 | 16 | Budget item | Larry Smith | Open |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

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 Figure 8: 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.

Figure 8: Techniques to Manage Risks

| Risk Control Techniques | Risk Financing Techniques |
|---|---|
| 1. **Risk Avoidance:** Actions taken that will absolutely prevent the risk from occurring.<br>2. **Risk Prevention:** Actions taken to reduce the likelihood of a risk occurring. (Typically available only for risks internal to the organization).<br>3. **Risk Reduction:** Actions taken to reduce the impact of a risk. (May apply to internal risks, but may also be the only response available to external risks).<br>4. **Segregation:** Dividing assets among multiple locations or having back-up assets away from a main location.<br>5. **Non-Insurance Risk Transfer:** Avoiding, preventing or reducing a risk through contract or agreement with another party. | 1. **Retain or Self-Insure:** Bearing the costs related to a risk occurring with the organization's own funds, whether general funds, specific funds set aside for this purpose or borrowed funds<br>2. **Transfer-Insurance:** Paying a premium to an insurance company in exchange for the company's promise to cover the costs related to the risk, should it occur.<br>3. **Non-Insurance Transfer:** Contracting with a party other than an insurance company to cover the costs related to the risk, should it occur, in exchange for other consideration. |

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. ERM acknowledges the risk of missed opportunities as a risk to be identified and managed.

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. ERM acknowledges the risk of missed opportunities as a risk to be identified and managed. 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.[6]

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).[7] Current descriptions of big data include additional characteristics not previously described and include:

- 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 health care 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?
- Has a risk appetite statement been adopted and a risk capacity analysis performed? Are they routinely reviewed and revised as the organization or context change?
- Has a risk appetite statement been adopted and a risk capacity analysis performed? Are they routinely reviewed and revised as the organization or business context change?
- Are Key Performing Indicators (KPIs) and Key Risk Indicators (KRIs) developed and reviewed as monitors for the ERM program?

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.

## INFORMATION AND COMMUNICATION

Information is necessary for the health care organization to carry out internal control responsibilities to support the achievement of its objectives. Both external and internal sources are needed for management to support the organizations' internal controls. Communication needs to flow throughout the organization and is a continual, iterative process (a process for arriving at a decision or a desired result by repeating rounds of analysis or a cycle of operations) providing and sharing necessary information.

Dissemination of internal communication requires the ability of communication to flow up, down and across the entire organization. Communication allows personnel to receive a clear message from executive leadership and identifies crucial topics and focus. External communication is twofold; "it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations."[9]

Organizational success with any initiative requires deep commitment in its ability to be effective in information collection and communication.

## CONCLUSION

The Framework — as described and developed by COSO and described and adopted by ASHRM for the development and implementation of health care 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 integrated care and telebehavioral health methods. It is important that outpatient providers are competent to manage patients effectively, comply with the standard of care, take steps to reduce overall risk and when necessary, obtain outside consultation. Outpatient providers also need to be aware of relevant regulations such as duty to warn/protect and mandated reporting. Because behavioral health care is a specialized area of practice, providers may need to obtain consultation from a risk management or legal professional when questions arise.

# REFERENCES

1. ASHRM Health Care Enterprise Risk Management Playbook, second edition – An ERM Guide for health Care. 2020. pp 147- 148.
2. Courtney, Hugh, What is Business Strategy; World Economic Affairs, Spring 1998. https://www.mcgill.ca/economics/files/economics/what_is_business_strategy.pdf. Accessed November 3, 2020.
3. Mind Tools, SMART GOALS – How to Make Your Goal Achievable. https://www.mindtools.com/pages/article/smart-goals.htm. Accessed November 2, 2020.
4. COSO; *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). 2017.
5. 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.
6. Professor Hossein Arsham. Tools for Decision Analysis: *Analysis of Risky Decisions* available online at: http://home.ubalt.edu/ntsbarsh/business-stat/opre/partIX.htm, Accessed November 13, 2020.
7. Patgiri, Ripon; Ahmed, Arif; Big Data: The V's of the Game Changer Paradigm; Computer Society; 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems., https://www.researchgate.net/publication/311642627_Big_Data_The_V's_of_the_Game_Changer_Paradigm. Assessed November 13, 2020.
8. Deloitte; COSO – *Information and Communication & Monitoring Activities; The management of an entity need to evaluate the internal control of the firm to determine whether the components are not only present but also functioning.* https://www2.deloitte.com/ng/en/pages/audit/articles/financial-reporting/coso-information-and-communication-monitoring-activities.html. Accessed October 2, 2020.

This whitepaper was made possible by the American Society for Health Care Risk Management.

It was developed to support efforts to advance safe and trusted health care through enterprise risk management.

Visit www.ASHRM.org/membership to learn more and become an ASHRM member.

ASHRM

AMERICAN
SOCIETY FOR
HEALTH CARE
RISK
MANAGEMENT