Gallagher

Insurance | Risk Management | Consulting

Health System Boards and Cultures That Support Effective Enterprise Risk Management

A discussion paper by James Rice, Gallagher; Kevin Poole, Artex; and John Ergastalo, Gallagher.

Preface

This paper has been developed from discussions at the recent Cayman Captive Forum organized by the Insurance Managers Association of Cayman (IMAC). Requests at the Forum for materials that might help stimulate health systems boards to enhance the effectiveness of their enterprise risk management encouraged the authors to assemble and share this collection of ideas and insights about governing modern risk management strategies and structures.

Introduction

The common law and regulatory climates of North American health systems have been shaped by an Anglo-Saxon heritage regarding the role of the corporation. This view of the corporation has, in turn, shaped the role and responsibilities of corporate boards as they perform certain key fiduciary duties wisely.[1] At the 2018 Cayman Captive Forum, our session on governance trends and best practices for risk management sought to position the role of boards to not so much be experts in risk management, but ***to be enablers*** of a superior risk management culture that supports talented executives and risk management professionals to master and continuously enhance the use of modern Enterprise Risk Management principles, policies and practices.

Ernst & Young asserts that organizations with mature risk management practices outperform their peers.[2] At Gallagher and Artex, we believe that boards embracing the "**Q Factor**" is central to these modern practices; that is, asking the right questions at the right time to challenge assumptions, identify risks, understand their potential impact and then manage to minimize the total costs of such risks (TCOR).

The Q Factor is a mindset for health sector board members to adopt that enables them to ask wise questions that cannot be answered by a simple yes or no. They ask questions that require the board and senior management to engage in strategic thinking and conversations that stretch their strategic planning and decision-making to higher levels of performance. They pose questions that encourage their leadership to journey into some uncharted and risky waters of community accountability and value for money contracting with payers, and expanding regulatory oversight.

At the recent **Cayman Captive Forum**, participants were invited to share key questions they believe wise boards should be asking if they want to continuously strengthen their risk management practices and cultures for the coming decade. The top 20 questions identified were:

[1] OECD, "Board Practices: Incentives and Governing Risks, Corporate Governance," 2011.
[2] Ernst & Young, "The critical role of the board in effective risk oversight," 2013.

1. What are the key risks we are likely to face in the coming two to three years, and how can we best quantify their impact on our operations and plans?

2. What are the qualifications of a world-class chief risk officer, and how can they best be recruited and retained?

3. How can we best develop and conduct an effective annual risk assessment process?

4. What should be the charge, work plan and composition of a board-level Risk Management Committee?

5. What knowledge, skills and attitudes should new board members (at the parent organization, as well as our offshore captive) need to understand to optimize the effectiveness of their fiduciary role and responsibilities?

6. How should offsite strategic planning and education sessions best be developed to focus directors, officers and key service providers on innovations to address strategic opportunities and risks?

7. How should we encourage our directors/trustees to understand and embrace change as our constant partner for success and vitality?

8. How should we best anticipate and prepare contingency plans for the “unintended consequences” of our plans, actions, and investments?

9. How can we develop and manage positive media relationships in good and challenging times?

10. How can we ensure we are committing adequate financial and human resources to our risk management processes?

11. How can we monitor the degree to which we have, at every level of the organization, a culture of ownership, responsiveness, peak performance, and wise communications?

12. How should we be inviting in speakers from our staff and advisers to stay informed about the changing landscape of U.S. health regulations for physician compensation and contracting, patient privacy, as well as compliance with payers’ billing and collection practices?

13. How should we be partnering with our managers and advisers to be more proactive in our risk mitigation strategies and systems?

14. How are we using the results of our risk assessments to shape our plans and investments for future growth and financial vitality?

15. What are examples of our risk management work that have generated positive results, and which ones had negative results?

16. How can board members best shift the conversations about risk from the downsides to the upside of opportunity when we manage the risks wisely?

17. How should we be investing in board education and development about modern Enterprise Risk Management?

18. What are the cloud/IT/system technologies that can best support the effectiveness and efficiency of our risk management strategies and staff?

19. Are our Total Costs of Risk (TCOR) and how do we compare to national benchmarks and our competitors?

20. How must we continuously align our risk management process to our business model in light of the changing policy and competitive landscape?

The challenge, however, is to define how best to map a path for boards to pose and answer these questions with the executive teams and external advisers. This paper is designed to be a discussion guide for boards and their executives to explore practical ways to strengthen their risk management processes and investments into sensible staff and systems for the coming decade. Work by Ernst and Young provides a series of challenging additional questions that boards can pose and answer with their managers, and is displayed in Appendix 2.

The *Risk Management Handbook for Healthcare Organizations* observes…

"The medical culture that silently taught the ABCs as Accuse, Blame, and Criticize is fading. Rising in its place is a safety culture emphasizing blameless reporting, successful systems, knowledge, respect, confidentiality, and trust."[3]

However, boards now understand that risk management needs to move beyond clinical risk to business, regulatory, reputational and payer risks.

[3] American Society for Healthcare Risk Management (ASHRM), "Risk Management Handbook for Health Care Organizations, Sixth Edition" 2011.

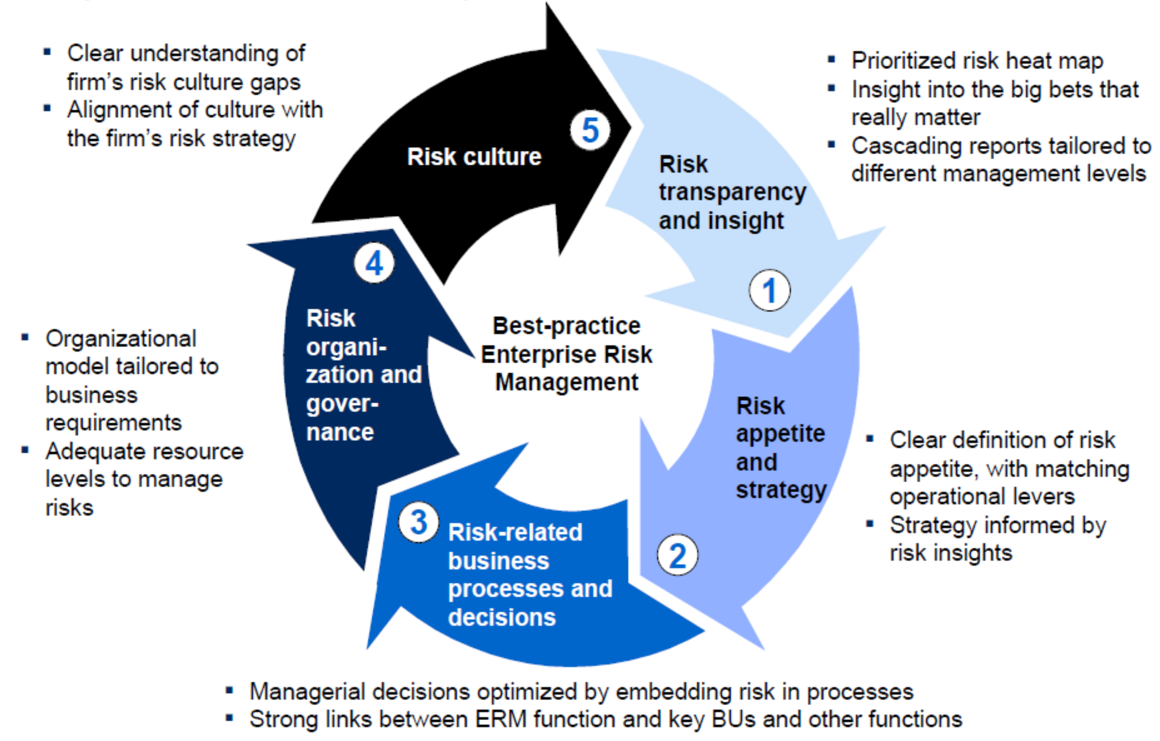
Conceptual Model for Board Focus on Strategic Risk Management

McKinsey studies indicate that there are five dimensions of Enterprise Risk Management (ERM) in which boards must become more knowledgeable:

1. Risk Transparency and Insight
2. Risk Appetite and Strategy
3. Risk Related Business Processes and Decisions
4. Risk Organization and Governance
5. Risk Culture

A graphic summary of these dimensions and their related concerns is shown below.[4]

Best-practice ERM delivers capabilities across 5 dimensions


5
Risk culture
1
Risk transparency and insight
2
Risk appetite and strategy
3
Risk-related business processes and decisions
4
Risk organi-zation and gover-nance
Best-practice Enterprise Risk Management

- Clear understanding of firm's risk culture gaps
- Alignment of culture with the firm's risk strategy

- Prioritized risk heat map
- Insight into the big bets that really matter
- Cascading reports tailored to different management levels

- Clear definition of risk appetite, with matching operational levers
- Strategy informed by risk insights

- Managerial decisions optimized by embedding risk in processes
- Strong links between ERM function and key BUs and other functions

- Organizational model tailored to business requirements
- Adequate resource levels to manage risks

Source: McKinsey

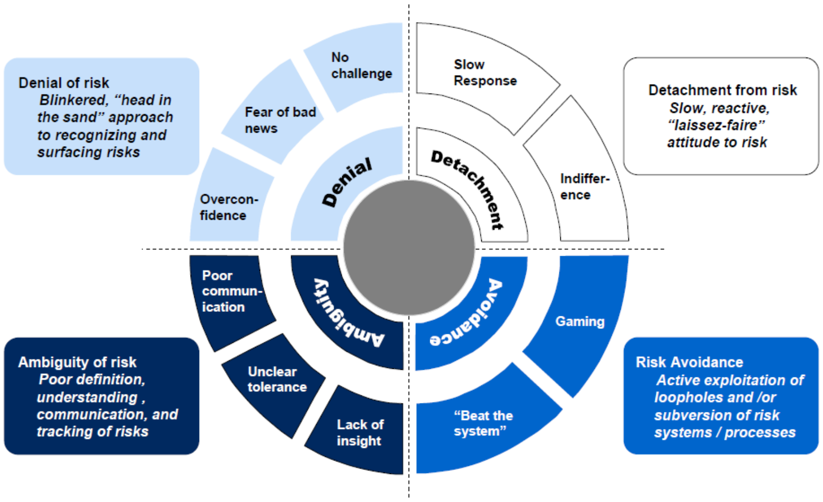
[4] Exhibit from "A board perspective on enterprise risk management", February 2010, McKinsey & Company, www.mckinsey.com. Copyright (c) 2019 McKinsey & Company. All rights reserved. Reprinted by permission.

To assess your organization's preparedness to embrace and accomplish these five dimensions of risk management, we encourage health system boards to annually assess the degree to which they are making progress against McKinsey's eight key principles:

- Strong and visible commitment from all members of the top team
- Central oversight of risk management across the enterprise (including subsidiaries and corporate functions)
- Separation of duties between policy setting, monitoring and control on the one hand; and risk origination and risk management execution on the other
- Clearly defined accountability
- Risk appetite and strategy clearly defined by top management and the board
- Full ownership of risk and risk management at business-unity level
- Business units formally involved and view risk function as a thought partner
- Robust risk management processes reinforce organizational design (e.g., incentive systems incorporate risk-return considerations)

Answers to such an annual assessment can enable a board to encourage its members and its executive team to avoid the four common behavior flaws described by Lamarre, Levy and Twining[5] – Denial, Detachment, Avoidance, Ambiguity:

Flaws in risk culture


Denial of risk
Blinkered, "head in the sand" approach to recognizing and surfacing risks
No challenge
Fear of bad news
Overcon-fidence
Denial
Slow Response
Indiffer-ence
Detachment
Detachment from risk
Slow, reactive, "laissez-faire" attitude to risk
Poor commun-ication
Unclear tolerance
Lack of insight
Ambiguity
Ambiguity of risk
Poor definition, understanding , communication, and tracking of risks
Avoidance
Gaming
"Beat the system"
Risk Avoidance
Active exploitation of loopholes and /or subversion of risk systems / processes

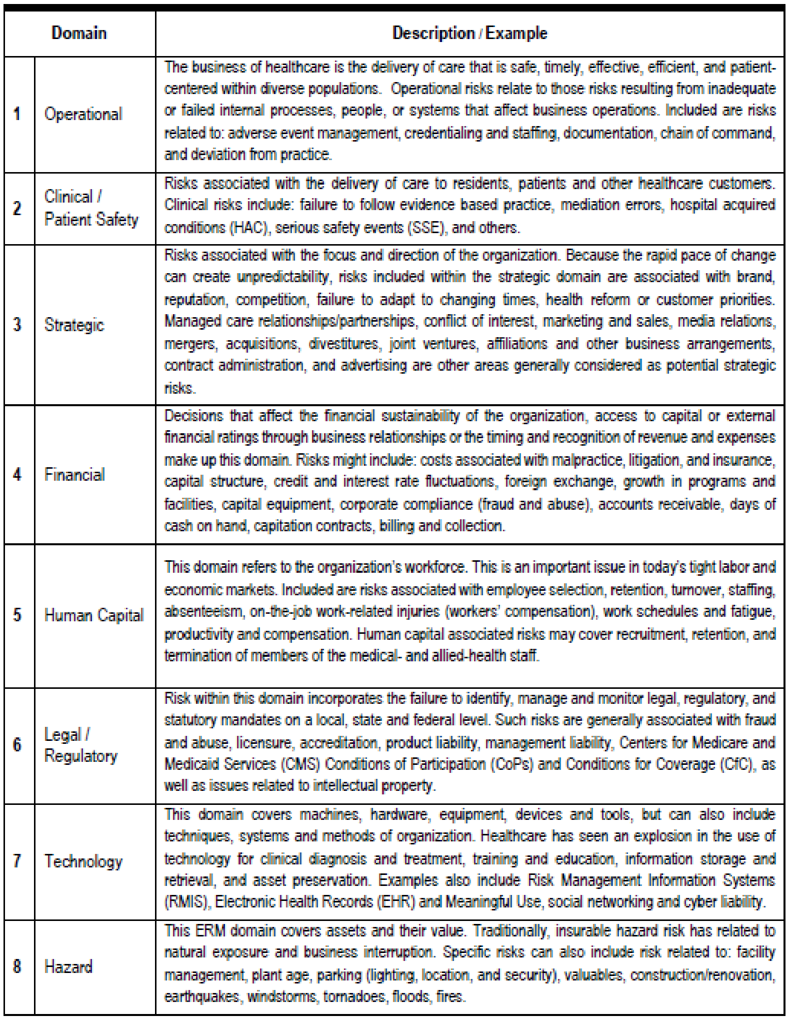
Source: McKinsey

[5] Exhibit from "Taking Control of Organizational Risk Culture "A board perspective on enterprise risk management", January 2010, McKinsey & Company, www.mckinsey.com. Copyright (c) 2019 McKinsey & Company. All rights reserved. Reprinted by permission.

Where Should Boards Look for Risks?

The Health Care Compliance Association published a profile of ten areas in which boards should ask for both an annual assessment and a Risk Management Plan to address the scope and nature of strategic risks in ten spheres of concern. (See next section)

The American Society for Risk Management (ASHRM), however, describes eight domains in which boards should be asking certain strategic questions to guide the organization's Annual Risk Management Plan.[6] The ASHRM Framework for Success is illustrated in the following exhibit.



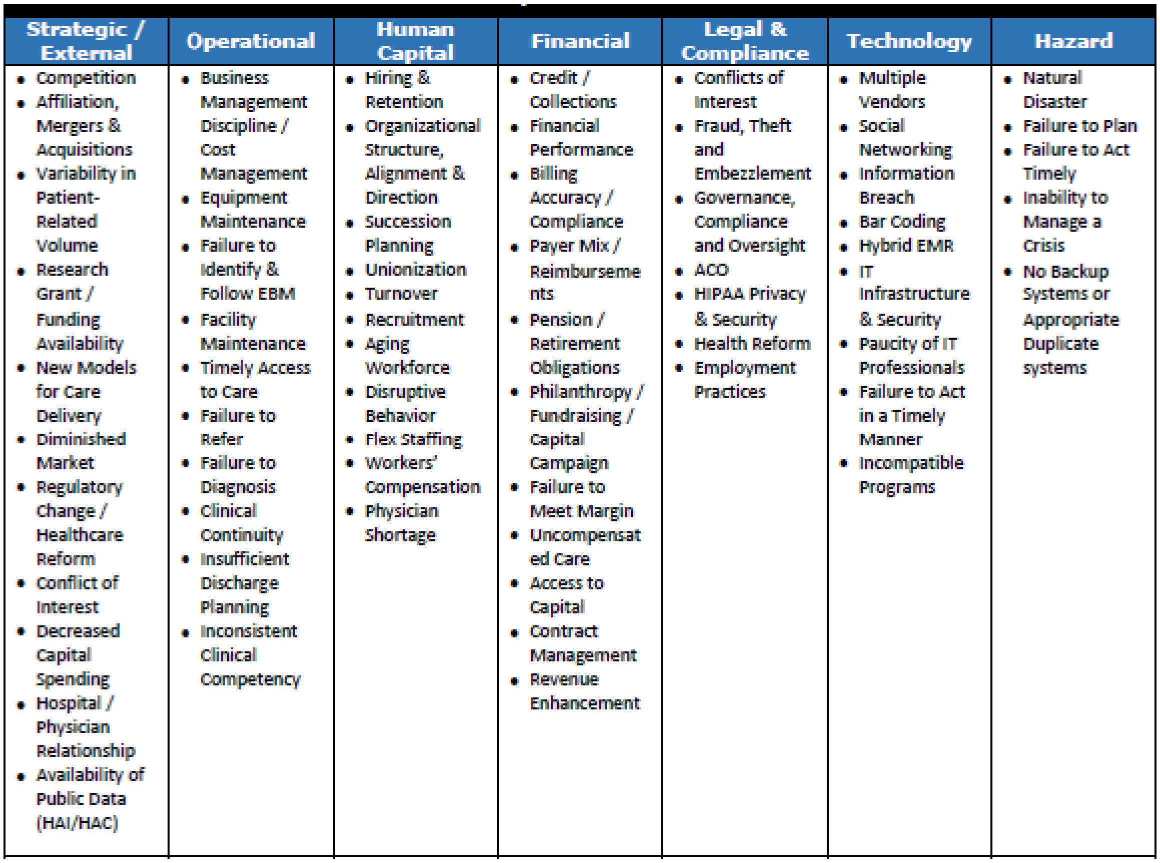
Domain		Description / Example
1	Operational	The business of healthcare is the delivery of care that is safe, timely, effective, efficient, and patient-centered within diverse populations. Operational risks relate to those risks resulting from inadequate or failed internal processes, people, or systems 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.

[6] ASHRM, "Enterprise Risk Management White Paper," August 29, 2014.

Gallagher

Insurance | Risk Management | Consulting

Risks within these domains are shown here:



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

Ten Regulatory Risk Categories from Health Care Compliance Association

Boards can ask questions about how their organizations are addressing these risks:

1. Quality of care - Subcategories may include: medical necessity, deficient care, practitioner qualifications and accuracy of quality-reporting data.
2. Anti-kickback and Stark - Subcategories may include: physician arrangements, joint ventures, leasing arrangements, physician recruitment, professional courtesy and safe harbors.
3. Emergency Medical Treatment and Active Labor Act (EMTALA) - Subcategories may include: stabilization, signage, physician on-call response, transfer, medical screening exam, and medical emergency response to areas outside the hospital buildings and non-clinical areas within the hospital.

4. Cost reports - Subcategories may include: bad debts, credit balances, wage indices, discounts, and disproportionate share hospital.
5. Claims development and submission - General subcategories may include: billing, coding, admissions and discharges, Charge Description Master, Advanced Beneficiary Notice and medical records. Specific subcategories may include: evaluation and management; outpatient observation services; three-day stays; and incident-to services.
6. Laboratory services - Subcategories may include: documentation, lab requisition forms, standing orders, physician notification, customized profiles and lab administration.
7. HIPAA privacy and security - Subcategories may include: privacy, security, information technology and documentation.
8. Physicians at Teaching Hospitals - Subcategories may include: billing, documentation, education and oversight.
9. Research - Subcategories may include: time and effort reporting; financial support from other sources; principal investigator conflict of interests; patent, trademark, and copyright under federal funds; human subjects' research; and animal subjects' research.
10. Compliance program effectiveness - Subcategories may include: compliance officer, corporate compliance, and board oversight; written standards of conduct; policies and procedures; training; enforcement; auditing and monitoring; and investigation and remediation.

It is critical to establish a simple framework to successfully manage the hundreds of risk areas prevalent in the current compliance environment.

Whether you are preparing for a government audit by a Recovery Audit Contractor (RAC), Medicare-affiliated contractor (MAC), Zone Program Integrity Contractor (ZPIC), or conducting your annual internal assessment, the HCCA believes that the correct use of these ten categories and their respective subcategories can guide you through the four compliance steps (risk assessment, risk remediation, risk monitoring and auditing, and risk response and reporting) that are essential to an effective compliance program and Risk Management Plan.

How can The Board Understand Risk Priorities?

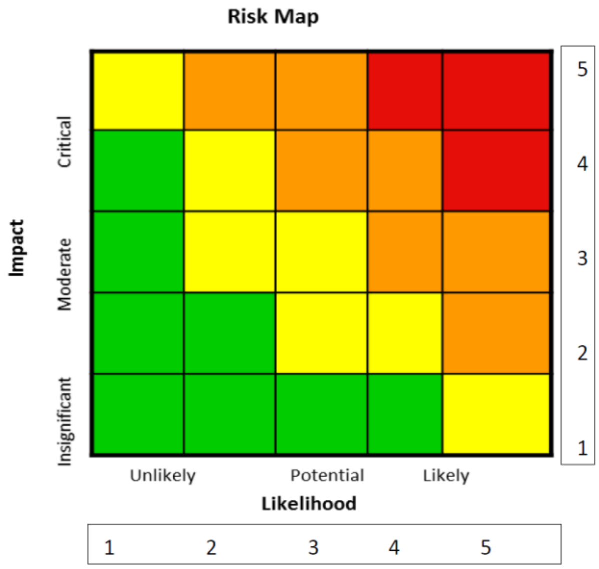
Wise boards ask their executive and risk management teams: “What is our process to assess the likelihood and the impact of all of our risks?” Nine processes are suggested as a framework for such a process of assessment:[7]

- Identify Risk: Since risk management involves managing uncertainty and new risk is constantly emerging, it is challenging to recognize all of the threats a healthcare entity faces. However, through the use of data, institutional and industry knowledge, and by engaging everyone — patients, employees, administrators and payers—healthcare risk managers can uncover threats and potentially compensatory events that otherwise would be hard to anticipate.
- Quantify and Prioritize Risk: Once identified, it is vital to score, rank and prioritize risks based on their likelihood and impact of occurrence, then allocate resources and assign tasks based on these measures. To accomplish this, risk matrices and heat maps can be deployed that will also help to visualize risks and promote communication and collaborative decision making.
- Investigate and Report Sentinel Events: Coined by the Joint Commission, Sentinel Events are “any unanticipated event in a healthcare setting resulting in death or serious physical or psychological injury to a patient or patients, not related to the natural course of the patient’s illness.” When a sentinel event occurs, quick response and thorough investigation address immediate patient safety issues and reduce future risk. Having an established plan in place promotes calm and measured response and transparency by staff and ensures that corrective actions can be implemented and evaluated. Sentinel events are not always the result of errors. However, achieving transparency and thorough evaluation requires healthcare organizations to establish an atmosphere of respect, trust and cooperation between staff and leadership.
- Perform Compliance Reporting: As with the Joint Commission, federal, state and other oversight bodies mandate reporting of certain types of incidents including sentinel events, medication errors and medical device malfunctions. Incidents such as wrong-site or patient surgery, workplace injuries, medication errors, etc., need to be documented, coded and reported.
- Capture and Learn “Near Misses and Good Catches”: When mistakes or adverse events are avoided due to luck or intervention, “near misses” and “good catches” occur. These are often the best way to identify and prevent risk. Healthcare providers should develop a culture that encourages reporting so that prevention measures and best practices can be instituted.
- Think Beyond the Obvious to Uncover Latent Failures: Active failures are obvious and easily-identified — when a nurse gives the wrong medication dose to a patient for example. Latent failures, on the other hand, are often hidden and only uncovered through analysis and critical examination. Did poor lighting make it hard to read the patient’s chart? Was the nurse rushing because he/she had too many high-acuity patients? When exploring the causes of an unfavorable episode, consider underlying and less-readily-apparent reasons.

[7] NEJM Catalyst, “What is Risk Management in Healthcare,” April 25, 2018

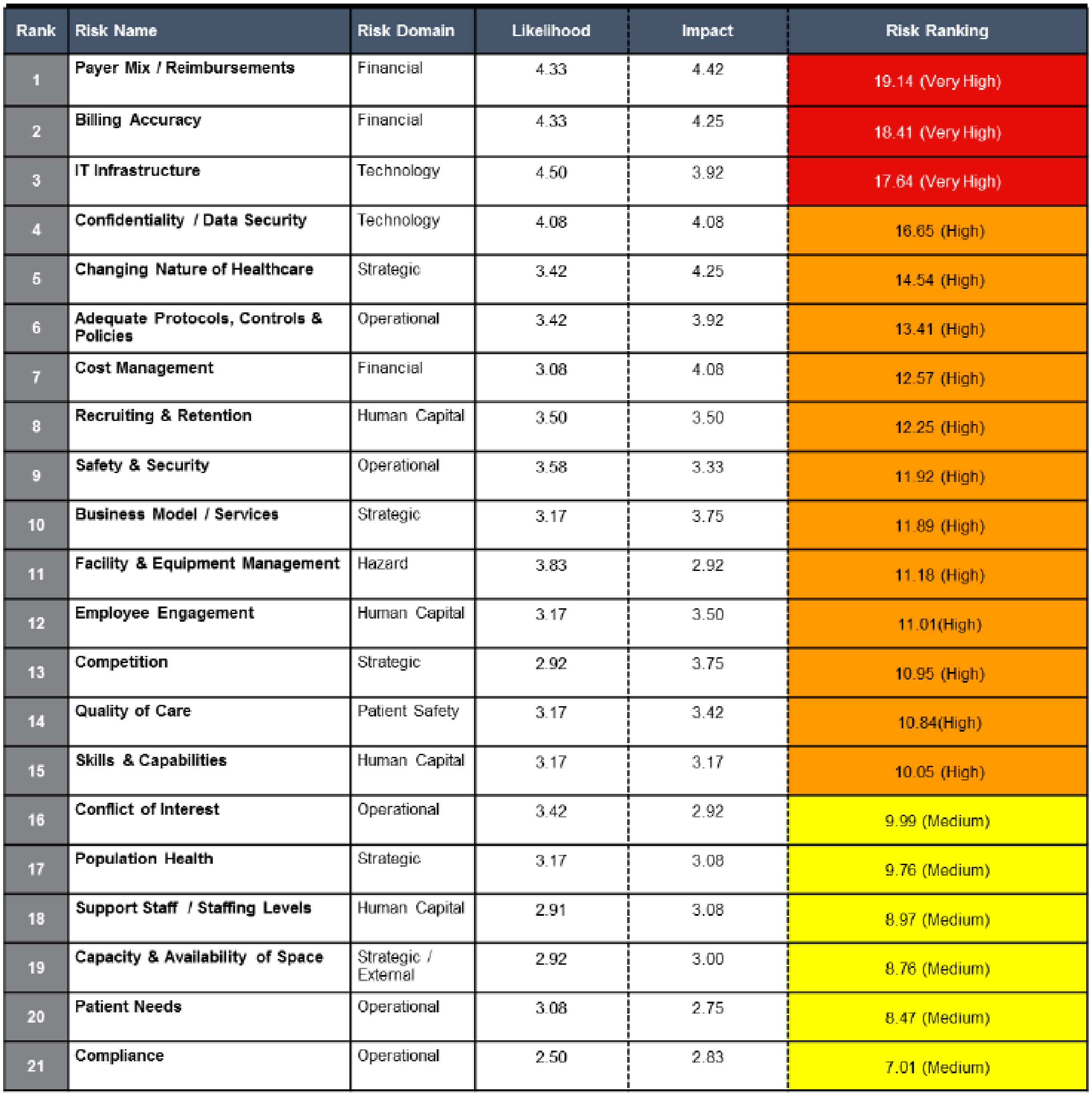
- **Use Proven Analysis Models for Incident Investigation**: Models for analyzing accidents are used to understand latent failures and causes as well as relationships among risks. For example, understaffing and fatigue often lead to medical errors. Applying well-established models improves risk management effectiveness and efficiency. Two accident analysis models used in healthcare risk management are the Sharp and Blunt End Evaluation of Clinical Errors model; FMEA or Failure Mode and Effects Analysis. These, as well as Root Cause Analysis, are also deployed and involve detailed frameworks to help uncover the causes and effects of medical mistakes.
- **Invest in a Robust Risk Management Information System (RMIS)**: Multiple platforms for reporting and managing risk are on the market. These systems provide tools for documenting incidents, tracking risk, reporting trends, benchmarking data points and making industry comparisons. Reports can be generated for losses, incidents, open claims and lost work time for injured employees to name a few. RMIS can greatly enhance risk management by improving performance through available and reliable systems while providing overall cost reduction by automating routine tasks.
- **Find the Right Balance of Risk Financing/Transfer/Retention**: Risk financing involves an organization's methods for efficiently and effectively funding loss that results from risk. It includes risk transfer usually through insurance policies and risk retention such as self-insurance and captive insurance.

The HCCA encourages use of a **Risk Map** which 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 below:



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***

A sample Risk Assessment Framework Report[8]



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)

[8] ASHRM, "Enterprise Risk Management White Paper," August 29, 2014

How can Boards Define Components of a Good Risk Management Plan?

The Risk Management Plan becomes the guiding document for how an organization strategically identifies, manages and mitigates risk. Hospital leadership and all department heads should be aware of and involved in the development and ongoing evaluation of the plan. Healthcare risk management plans communicate the purpose, scope and objectives of the organization's risk management protocol. They also define the roles and responsibilities of the risk manager and other staff involved in risk mitigation.

The format of a Risk Management Plan varies by organization and is contingent on the analysis of existing systems and historical data as well as the unique characteristics of each healthcare entity. That said, there are seven fundamental components that belong in all healthcare risk management plans:[9]

- Education and Training: Risk management plans need to detail employee training requirements which should include new employee orientation, ongoing and in-service training, annual review and competency validation, and event-specific training.
- Patient and Family Grievances: To promote patient satisfaction and reduce the likelihood of litigation, procedures for documenting and responding to patient and family complaints should be described in the Risk Management Plan. Response times, staff responsibilities and prescribed actions need to be articulated and communicated.
- Purpose, Goals and Metrics: Risk management plans should clearly define the purpose and benefits of the healthcare risk management plan. Specific goals to reduce liability claims, sentinel events, near misses and the overall cost of the organization's risk should also be well articulated. Additionally, reporting on quantifiable and actionable data should be detailed and mandated by the plan.
- Communication Plan: While it is critical that the healthcare risk management team promote open and spontaneous dialogue, information about how to communicate about risk and with whom should be provided in the healthcare risk management plan. Next steps and follow-up activities should be documented. It is essential as well that the plan detail reporting requirements to departments and C-suite personnel. Furthermore, the plan should promote a safe, "no-blame" culture and should include anonymous reporting capabilities.
- Contingency Plans: Risk management plans also need to include contingency preparation for adverse system-wide failures and catastrophic situations such as malfunctioning HER systems, security breaches and cyber-attacks. The plan needs to include emergency preparedness for things like disease outbreaks, long-term power loss, and terror attacks or mass shootings.

[9] NEJM Catalyst, "What is Risk Management in Healthcare," April 25, 2018

- **Reporting Protocols**: Every healthcare organization must have a quick and easy-to-use system for documenting, classifying and tracking possible risks and adverse events. These systems must include protocols for mandatory reporting.
- **Response and Mitigation**: Plans for healthcare risk must also include collaborative systems for responding to reported risks and events including acute response, follow-up, reporting, and repeat failure prevention.

Conclusions

As many captive boards are aware, guidance has been issued by the Cayman Islands Monetary Authority in relation to board responsibilities. This means that, at least annually, a captive board should review its Corporate Governance and Risk Management Frameworks and update these as necessary. This paper helps identify some of the tools and techniques that can be used to help enhance these frameworks as well as hopefully provide some food for thought.

About the Authors

James A. Rice, PhD, FACHE
Managing Director & Senior Advisor, Governance and Leadership
800.327.9335
jim_rice@ajg.com

Kevin Poole
Client Services Director, Artex
345.914.2265
kevin.poole@artexrisk.ky

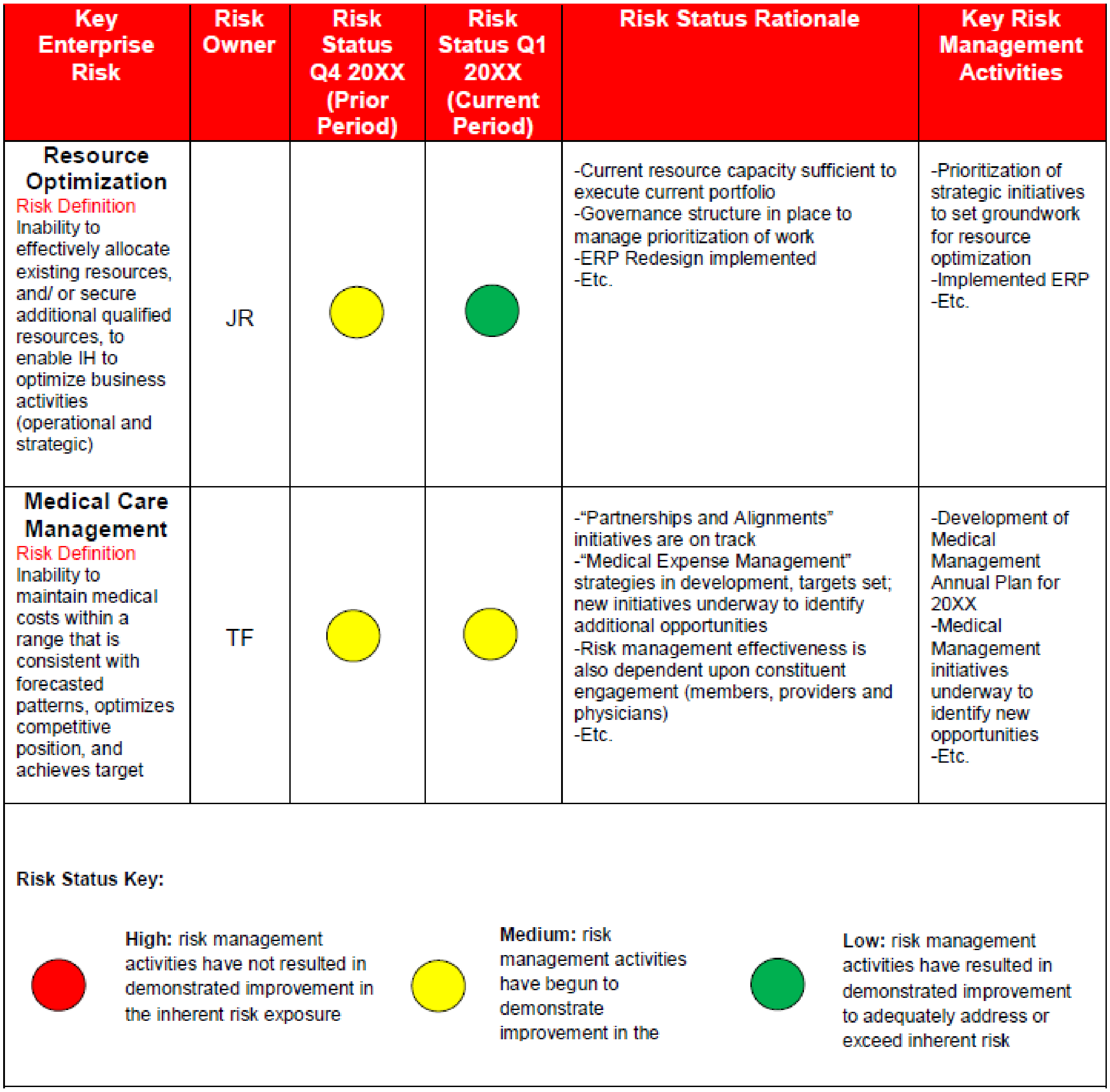
John Ergastolo
Area Executive Vice President, Management Liability Practice
312.803.7426
john_ergastolo@ajg.com

Consulting and insurance brokerage services to be provided by Gallagher Benefit Services, Inc. and/or its affiliate Gallagher Benefit Services (Canada) Group Inc. Gallagher Benefit Services, Inc. is a licensed insurance agency that does business in California as “Gallagher Benefit Services of California Insurance Services” and in Massachusetts as “Gallagher Benefit Insurance Services.” Neither Arthur J. Gallagher & Co., nor its affiliates provide accounting, legal or tax advice.

Appendix 1: Sample Board Report on Risk

REPORTING KEY RISK INFORMATION TO THE BOARD OF DIRECTORS

Figure 1: Risk Dashboard (Example)



Key Enterprise Risk	Risk Owner	Risk Status Q4 20XX (Prior Period)	Risk Status Q1 20XX (Current Period)	Risk Status Rationale	Key Risk Management Activities
Resource Optimization Risk Definition Inability to effectively allocate existing resources, and/ or secure additional qualified resources, to enable IH to optimize business activities (operational and strategic)	JR	🟡	🟢	-Current resource capacity sufficient to execute current portfolio -Governance structure in place to manage prioritization of work -ERP Redesign implemented -Etc.	-Prioritization of strategic initiatives to set groundwork for resource optimization -Implemented ERP -Etc.
Medical Care Management Risk Definition Inability to maintain medical costs within a range that is consistent with forecasted patterns, optimizes competitive position, and achieves target	TF	🟡	🟡	-"Partnerships and Alignments" initiatives are on track -"Medical Expense Management" strategies in development, targets set; new initiatives underway to identify additional opportunities -Risk management effectiveness is also dependent upon constituent engagement (members, providers and physicians) -Etc.	-Development of Medical Management Annual Plan for 20XX -Medical Management initiatives underway to identify new opportunities -Etc.

Risk Status Key:

🔴 **High:** risk management activities have not resulted in demonstrated improvement in the inherent risk exposure

🟡 **Medium:** risk management activities have begun to demonstrate improvement in the

🟢 **Low:** risk management activities have resulted in demonstrated improvement to adequately address or exceed inherent risk

Gallagher

Insurance | Risk Management | Consulting

Appendix 2: Sample Questions for Board Members for Risk Planning

Ernst & Young's "The critical role of the board in effective risk oversight" offers six pages of questions which can be helpful for board members to stimulate discussion with organizational leadership.