Enterprise Risk

A Toolbook for Healthcare Boards and Executives

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

A Governance Institute Strategy Toolbook **Fall 2022**

A SERVICE OF

nrc HEALTH

The Governance Institute®

The essential resource for governance knowledge and solutions®

1245 Q Street, Lincoln, NE 68508
(877) 712-8778

GovernanceInstitute.com
/The Governance Institute
/thegovinstitute

The Governance Institute is a service of NRC Health. Leading in the field of healthcare governance since 1986, The Governance Institute provides education and information services to hospital and health system boards of directors across the country. For more information about our services, please call toll free at (877) 712-8778, or visit our Web site at GovernanceInstitute.com.

The Governance Institute endeavors to ensure the accuracy of the information it provides to its members. This publication contains data obtained from multiple sources, and The Governance Institute cannot guarantee the accuracy of the information or its analysis in all cases. The Governance Institute is not involved in representation of clinical, legal, accounting, or other professional services. Its publications should not be construed as professional advice based on any specific set of facts or circumstances. Ideas or opinions expressed remain the responsibility of the named author(s). In regards to matters that involve clinical practice and direct patient treatment, members are advised to consult with their medical staffs and senior management, or other appropriate professionals, prior to implementing any changes based on this publication. The Governance Institute is not responsible for any claims or losses that may arise from any errors or omissions in our publications whether caused by The Governance Institute or its sources.

Acknowledgements

This toolbook was compiled from a collection of Governance Institute resources written by the following contributors, faculty members, and advisors (listed in alphabetical order; see the resource list at the end of this publication for more details and links):

James W. Blake, Cofounder, *JMP Ventures, LLC*

David Burik, Partner, *Guidehouse*

Bob Chaput, M.A., Founder and Executive Chairman, *Clearwater Compliance*

Danielle A. Dyer, Partner, *Guidehouse*

Ryan S. Gish, Managing Director, *Kaufman Hall & Associates, Inc.*

Marian C. Jennings, M.B.A., President, *M. Jennings Consulting, Inc.*

Eric A. Jordahl, Managing Director, *Kaufman Hall & Associates, Inc.*

Kenneth Kaufman, Chair, *Kaufman Hall & Associates, Inc.*

Daniel K. Zismer, Ph.D., Managing Director & Cofounder, *Castling Partners*

The Governance Institute

The Governance Institute provides trusted, independent information, tools, and resources to board members, healthcare executives, and physician leaders in support of their efforts to lead and govern their organizations.

The Governance Institute is a membership organization serving not-for-profit hospital and health system boards of directors, executives, and physician leadership. Membership services are provided through research and publications, conferences, and advisory services. In addition to its membership services, The Governance Institute conducts research studies, tracks healthcare industry trends, and showcases governance practices of leading healthcare boards across the country.

Table of Contents

Introduction

Board members' fiduciary duties encompass oversight of enterprise risk management (ERM). To do so, board members, in collaboration with senior leadership and championed by the CEO, must identify the most significant risks to their organizations and decide how to allocate resources to mitigate those risks. Healthcare enterprises face many different kinds of controllable and non-controllable risks related to:

- Clinical quality of care and patient safety
- Financial stability
- Emergency preparedness
- Legal and regulatory compliance
- Merger and acquisition (M&A) activity
- The privacy and security of patient data/protected health information

Traditionally, ERM within hospitals and health systems has primarily focused on compliance and efforts to improve margins. However, today's ERM strategy demands the nimbleness of leadership to respond to the "next normal" by predicting, identifying, and monitoring risks and then ensuring responses are aligned and coordinated.

This is an approach that has long been deployed by organizations in the high-tech, manufacturing, and energy industries. Doing so will help leaders combat economic and operational uncertainty while strengthening stability in this era of transformative change.

Disrupting Traditional Thinking around Risk

A recent Guidehouse analysis found that health systems have diversified their risk-based payment strategies with a broader array of business lines, and nearly 60 percent of health systems plan to advance into risk-based Medicare Advantage models in 2022.[1] Leaders are increasingly viewing risk models as a lever for revenue growth—critical given decreased demand for inpatient care.

Pre-COVID, leaders demonstrated an emphasis on growth, seeking opportunities not just to shore up market share, but also to expand key capabilities and gain access to scale. Growth was considered strategic, so there was minor focus on measuring the ROI of these pursuits beyond revenue. Merger and acquisition (M&A) deal volume reached historic proportions in 2017, and a rise in megadeals captured headlines from 2017–2018. Deals weren't limited to hospitals and systems. Physician practices also drew strong interest, with hospitals acquiring 3,200 physician practices from 2019–2020 alone.

But as hospitals and systems paid high prices for assets, leaders often had little experience in—or the stomach for—integration and margin creation. Without a clear vision for what an integrated system would look like and a path forward for achieving

1 *2021 Risk-Based Healthcare Market Trends*, Guidehouse, November 8, 2021.

this vision, organizations often struggled to meet post-transaction goals two years after a merger.[2]

Healthcare boards need a process for systematically structuring their organization's best strategic thinking around ERM. Comprehensive ERM uses a dual approach to risk assessment through:

1. Quantitative corporate finance tools, which identify risk factors and assess their impact through financial and economic models. This step involves identifying organization-specific rules around risk management, taking into account the organization's risk tolerance/appetite and the internal and external challenges that could affect performance.
2. Scenario planning, which is the more qualitative, broad-thinking approach to envisioning the future. This step involves determining key metrics that will give boards clear insight into the risk pressures their organizations face.

2 Christopher Cheney, "M&A Study: Acquired Hospitals Often Struggle to Meet Financial Goals," *HealthLeaders,* October 12, 2017.

Step 1. Applying Quantitative Corporate Finance Tools to ERM

A mature ERM program supports the organization in the evaluation and treatment of risk. It should be structured and analytical, focused on identifying and mitigating the financial impact and volatility of a portfolio of risks. Effectively managing risk requires shared beliefs. An important first step is to identify and understand the risks your organization is facing and develop a foundation of shared beliefs around those risks to unify the board and leadership team, binding them to a risk management plan they all own together.

Understand Where You Are Starting

Start by reviewing your current compliance and ERM approaches and address key questions. Are today's approaches siloed or coordinated? Is your approach more proactive or reactive? How do you measure the success of your compliance or ERM program? Have you agreed on which major risks should be shared with senior management, the compliance committee, or the full board? How aligned are your ERM approaches with your strategic plan? The answers to these questions will help your board identify a framework that guides what rules should be in place regarding risk management for your organization.

The critical building blocks of ERM:

1. An integrated strategic and financial plan
2. The cataloging of baseline risks
3. Scenario planning

Adopt an Enterprise Risk Management Framework

If you have not already done so, adopt a framework that comprises more than just compliance. Start by recognizing that there are three categories of enterprise risk:[3]

- Preventable risks: typically internal and a primary focus of corporate compliance (e.g., fraud and abuse, HIPAA requirements, etc.).
- Strategic risks: often external, these arise related to your strategic decisions or positioning (e.g., investing in new urgent care centers to compete with a

3 Robert S. Kaplan and Anette Mikes, "Managing Risks: A New Framework," *Harvard Business Review*, June 2012.

CVS health hub or new risks associated with sponsoring your own health plan, etc.).
- External risks: these arise from events outside your organization and often are beyond your influence or control (e.g., a pandemic, ransomware attack, major cut in Medicare payments, etc.).

Don't fall into the trap of believing one category of risk is worse than another. A "preventable" risk is no less dangerous than a "strategic" risk. Any category of risk could substantially harm the organization and its reputation.

Equally important is to recognize that risk can occur across multiple domains: clinical, operational, strategic, financial, legal, technology, and hazard. Any category of risk (prevention, strategic, or external) could occur in each of these domains, and the ERM plan must take each into account.

Determine Your Risk Appetite and Tolerance[4]

Risk appetite is the total level of risk an organization is willing to accept while pursuing its objectives, and before any action is determined necessary in order to reduce the risk. It is related to the longer-term strategy of what needs to be achieved and the resources needed to achieve it. Factors to consider when determining risk appetite include:

- Organizational culture
- Competitive position
- The nature of the objectives being pursued (e.g., how aggressive are they?)
- Financial strength and capabilities (the more resources an organization has, the more willing it may be to accept risks and their associated costs)
- Ability to continue to fulfill the mission

Risk tolerance is more granular and affects individual risks; it reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the organization is seeking to achieve. Your ERM framework should include a risk score for each individual risk that calculates the benefits vs. potential costs if the risk or worst-case scenario occurs. This is discussed in more detail in the next section.

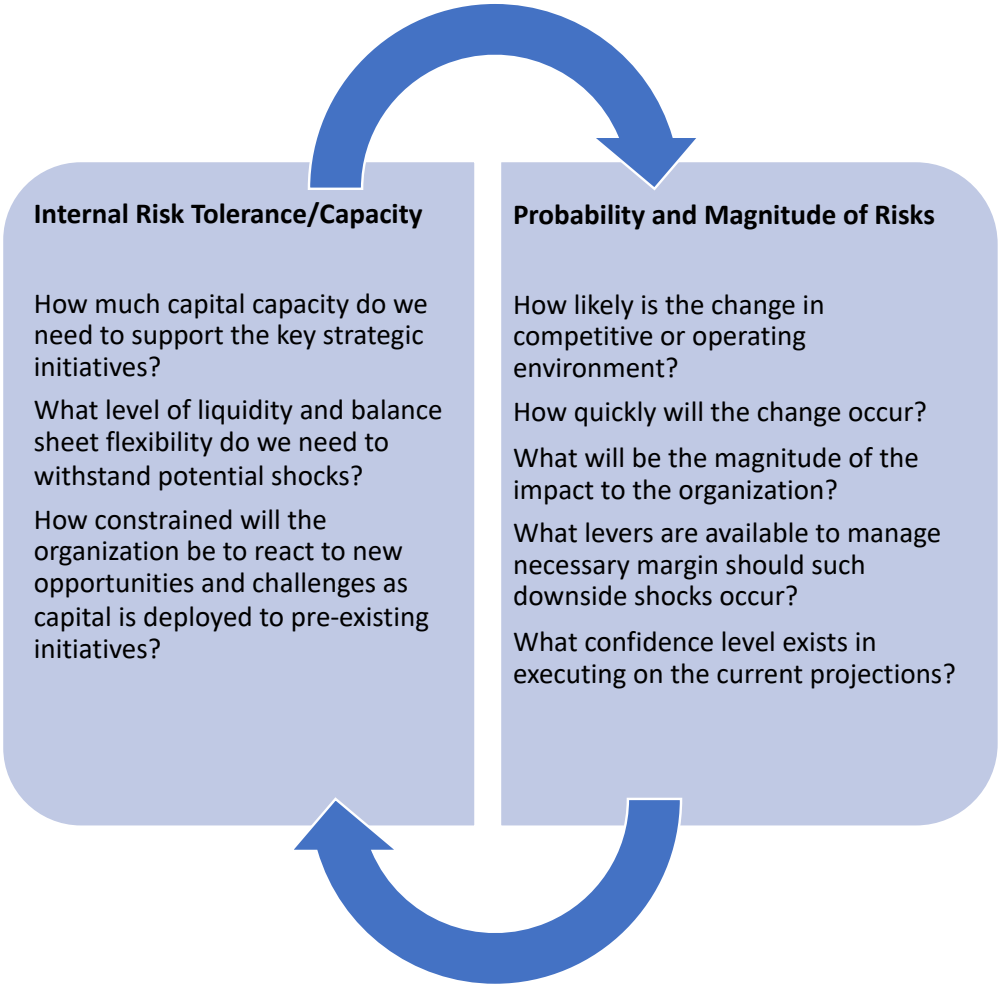
4 Jean-Gregoire Manoukian, "Risk Appetite and Risk Tolerance: What's the Difference?," *Expert Insights,* Wolters Kluwer, September 29, 2016.

Strategic Investment Example

ERM must use a corporate finance approach *plus scenario envisioning* based on an integrated strategic and financial plan. Identifying the strategies or initiatives that will enable the hospital or health system to achieve market strength, differentiation, and sustainable competitive financial performance involves finding the balance between strategic needs and financial capabilities. The equilibrium lies in a "corridor of control" where the organization balances two opposing goals:

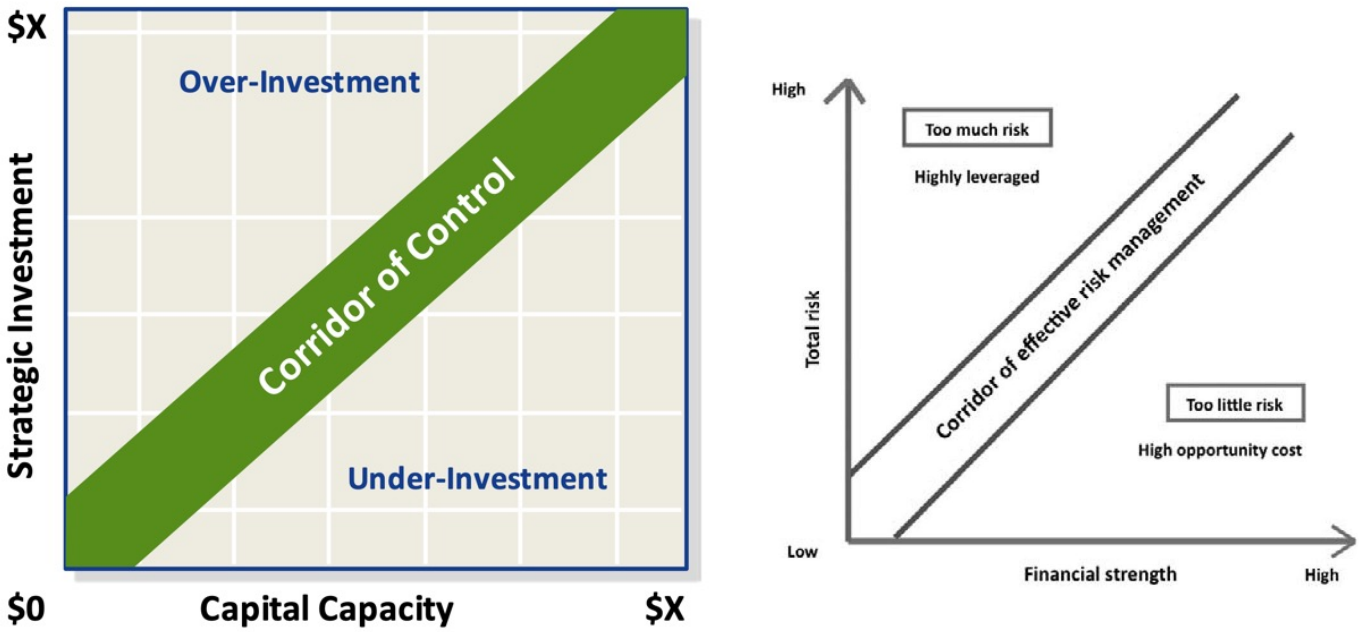
- Compete as effectively as possible, which requires aggressive investment of capital and commitment of operating dollars, but
- Respect the fiduciary role of management and the board to maintain the long-term financial integrity of a community asset.

Exhibit 1. Risk Tolerance vs. Probability and Magnitude of Risks



Source: Kaufman, Hall & Associates, LLC

Exhibit 2. A Comparison: Investment Corridor of Control and Risk/Reward Continuum



Source: Kaufman, Hall & Associates, LLC

Identify Risks of Both Action and Inaction

Ensure that the board understands the financial, strategic, reputational, or internal political risks associated with being proactive. Equally important, ensure understanding of the risks associated with a "wait and see" approach.

If an organization falls above the corridor of control, its financial need or strategic capital appetite exceeds it financial capability. In the extreme, this can cause liquidity crisis and trigger a debt default. More commonly, the organization puts itself in a position where it is unable to respond to opportunities and threats because its available capital is fully committed and its financial performance precludes access to additional capital.

An organization whose position appears below the corridor of control might have a fair amount of money but lacks a strategic plan that outlines how to grow and spend that money. It may be at risk of losing relevance in its community because it is not investing sufficient capital to pursue strategic opportunities to meet new needs. Over time, underinvesting leads to a loss of profitable business, which erodes operating performance, which reduces capital capacity, which diminishes the level of strategic investment that can be made.

Step 2. Scenario Planning and Determining Key Metrics

Scenario planning provides the broadest-possible thinking about what might occur in the future. All strategies have varied degrees of associated risk, and risks are not fixed variables. They can be prospectively mitigated to increase the chance of success. An ERM plan will identify risks in the following categories: clinical, operational, strategic, financial, technology, or hazard. Often a risk will span more than one category. Then, scenario planning will envision all of the possible events around each risk and the related impacts.

Examples of risks healthcare organizations are currently facing include:

- Declining demand for hospital-related services (financial)
- High inflation, supply chain gaps, and increased labor costs (clinical, operational, financial)
- Business disruption (clinical, operational, strategic)
- Dramatic increase in cyber attacks (technology)
- Increase in extreme weather events such as floods, wildfires, hurricanes, and extreme heat (hazard)

Develop a Risk Inventory

While risk events may occur individually, the enterprise's overall risk is cumulative. A risk inventory includes risks across all domains and categories. Importantly, this risk inventory also needs to assess both the potential impact on the organization and the likelihood of each risk event. For example, a potential $20M risk event with a likelihood of five percent results in an "expected impact" of $1.0M. This is the same expected impact as a $5M risk event with a 20 percent likelihood. Recognize that the likelihood assessment is an assumption and needs to be based upon the best available, credible data—and considered the most likely case, not the worst or best scenario.

Develop Scenarios and Contingency Plans

The next step is for the management team to envision all of the possible scenarios and develop contingency plans and "trigger points" for each risk in the inventory.

Scenario planning is often a facilitated process in which boards and senior leaders ask the biggest "what if" questions about alternative future states. Descriptions of potential macroeconomic impacts, business model transformation, competitor moves or responses, and regulatory changes can start the process. The analysis includes anticipated hidden weaknesses and potential inflexibilities in the organization's strategy, as well as "common-denominator" strategies that would be successful under all of the scenarios.

Though exact quantification may not be possible, scenario planning can also be helpful in the identification, scale, directionality, and likelihood of risks. A solid contingency plan identifies the major actions that the organization would need to take should this industry disruption occur (akin to the disaster planning that you already undertake for local or regional physical disasters/disruptions).

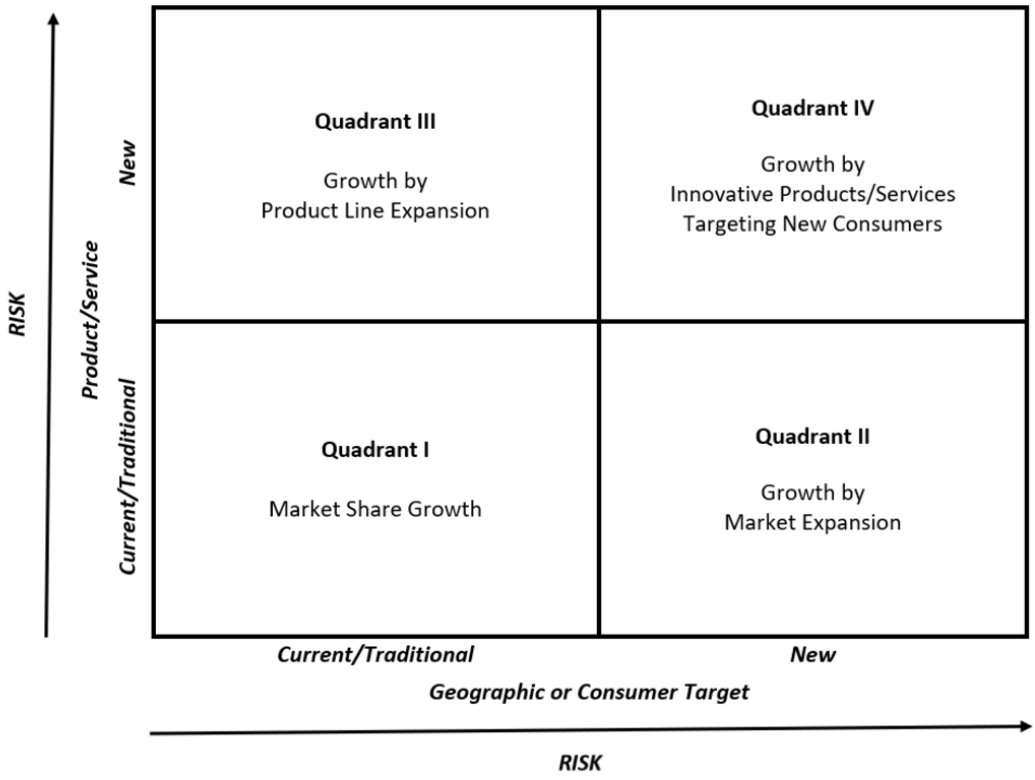
"Trigger points" are like the canary in the coal mine: that is, they are early indicators of potential change. Leaders should identify and constantly monitor these trigger points. Federal payment changes, as an example, often can be foreseen years before they are enacted. Such predictable changes need not come as a surprise, although many hospitals and health systems scramble to adapt once implementation is imminent.

The scenario planning and resulting analysis are then incorporated into the risk inventory with the trigger points and specific mitigation (or prevention) strategies that could reduce the likelihood of the risk event, and actions to take to reduce the impact if a risk event occurs. Finally, the list of risk events, ranked by greatest expected impact, are compiled into an inventory that presents the overall cumulative portfolio of risks.

Align ERM with Strategic Goals and Related Risks

ERM plans must also align with the strategic plan and its objectives, identifying the related risks of not achieving or underperforming on strategic goals. The two-by-two matrix in **Exhibit 3** is a schematic representation of the Growth Opportunity Matrix. Conceptually simple, it is a useful analytical framework for identifying growth opportunities worth pursuing, along with their relative risks and key success factors.

Exhibit 3. Relative Risk of Growth Strategies



Source: M. Jennings Consulting, Inc.

Quadrant I: Market Share Growth

This is where the low-risk growth strategies lie, such as targeted growth in primary or secondary service areas through clinical innovation, satellite facilities' distributing physician and/or ancillary services art convenient locations, and new patient-centered primary care models with greater alignment between your primary care providers and specialists.

Focusing solely on this quadrant will not yield sufficient growth for most organizations.

Quadrant II: Growth by Market Expansion

A realistic market expansion strategy must be built on solid market and consumer research. Successful geographic growth requires offering a distinctive consumer experience. The risks associated with this quadrant are moderate, and may yield unpredictable results.

Quadrant III: Growth by Product Line Expansion

Growth in this quadrant occurs by successfully introducing new products or services to consumers in your service area/market. Competition in this quadrant can be fierce. The risks associated with activities in this quadrant are moderate to high based on both how innovative your new product would be and the size of your organization.

Quadrant IV: Growth by Innovative Products/Services Targeting New Consumers

Growth in this quadrant occurs primarily by breakthroughs in clinical and/or information technologies and is seen most frequently in the private sector or in large corporations, including insurers or academic medical centers and their research spinoffs. Competition in this quadrant is fierce and the associated risks are high; most competitive players expect that many of these strategic initiatives are likely to fail.

Step 3. Putting the ERM Plan into Action

Mitigate Risk and Measure Progress[5]

This phase is about systematically resolving the risks identified in the previous stages. Important questions the board can ask senior leadership to ensure that risks are being appropriately mitigated include:

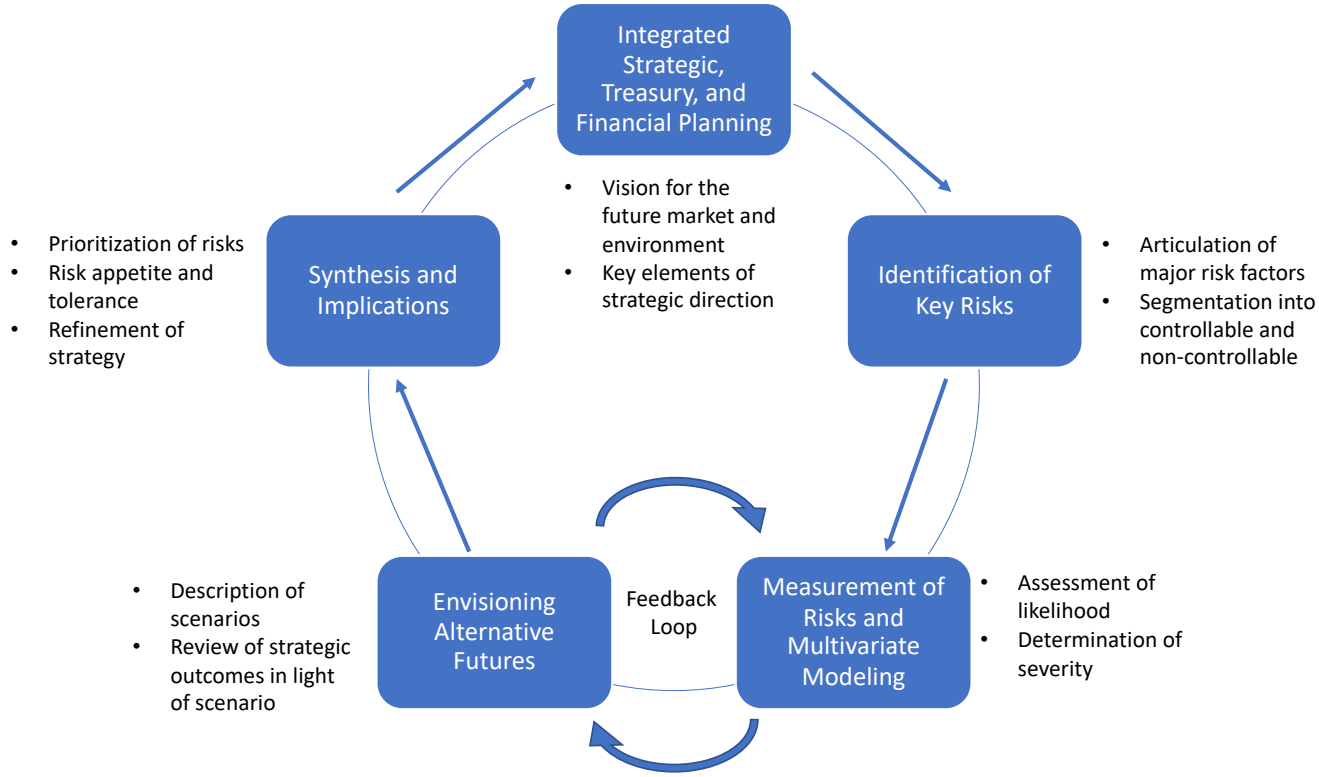
- Now that we have identified the risks, how are we addressing them?
- What controls and procedures have we currently established that address our risks?

Senior leaders responsible for ERM implementation can use a simple action plan template that includes the following for each risk identified:

- What phase of implementation it falls in the ERM plan
- The probability of that risk occurring and its impacts to the organization
- Mitigation response
- Desired outcome
- Owner(s)
- Timeline
- Progress

Organizations can't take actions to mitigate risks until they are made aware of the areas of exposure. Measuring and reporting on the progress of the ERM program builds awareness and visibility into the existing hazards, provides a performance review of ERM implementation steps, and helps the organization respond to new risks that arise and anticipate new areas of opportunity to improve risk exposure.

Exhibit 4. Putting ERM into Action



Source: Kaufman, Hall & Associates, LLC

5 Andy Marker, "Guide to Enterprise Risk Management Implementation," Smartsheet, September 16, 2021.

Step 4. Go beyond Compliance

Effective enterprise risk management is much broader than compliance alone. As part of its fiduciary duties, a board is required to review the adequacy of the organization's risk management processes and can play a key leadership role in moving beyond traditional reactive and siloed risk prevention approaches.

Update Your Compliance Committee Charter and Membership

Review your compliance committee charter (see the Appendix for a sample ERM committee charter and policy) to ensure that it incorporates all desired elements of ERM. Consider changing the committee name to "Compliance and Enterprise Risk Management" and using this committee as the board's locus for a robust, multidimensional, and coordinated approach. (For some boards, maintaining separate committees is preferable to combining the two. For boards that feel they need to develop a brand new ERM program or revamp an existing one, a temporary committee focused on this work might be appropriate, and then the Compliance and ERM committee would be tasked with monitoring progress and periodic updates of the ERM program once it is in place.)

Additionally, identify the competencies needed on such a committee. If needed, add or replace members of today's committee—and consider whether the board itself needs to recruit new members to lead or serve on this committee.

Questions to Consider:

What if several of our major risks occurred simultaneously? Could we remain viable?
Are we spreading ourselves too thin?

Ensure that Your Board's Culture Supports Effective ERM

It is critically important that the board create a culture of safety that encompasses all enterprise risks. Leaders need to encourage transparency when an adverse event occurs in any domain.

The board must be courageous and willing to consider a "stress test" scenario. Encourage willingness to ask "what-if" questions around potential disruptors that, even if unlikely, could substantially harm the organization.

The Board's Leadership Role

The board can play a key leadership role in moving the organization to a more robust, multidimensional, and coordinated approach to overall enterprise risk management (ERM):

- Ask questions about today's approaches and adopt an ERM framework that differentiates between preventable, strategic, and external risks.
- Determine the best committee approach to help the board fulfill its risk management responsibilities.
- Carefully link strategy development and implementation with organizational mission and ability to tolerate and manage risk.

Conclusion

Now is the time for the board to establish a multidimensional, coordinated, and proactive enterprise risk management approach. While recognizing myriad risks may feel uncomfortable or even overwhelming, anticipating these events today allows the organization to identify mitigation approaches in advance of an untoward event.

Maintaining a Future-Focused View

As the business model evolves in healthcare, the use of ERM in hospitals and health systems will contribute to new success models. These models will be created when organizations identify, pursue, and achieve opportunities that otherwise might have been missed due to focusing, instead, on fixing broken pieces of their strategy, operations, or capital structure.

Time spent envisioning alternative futures, evaluating their non-controllable risk factors, and stress-testing the impact, help develop a deeper understanding of the organization. All of this makes organizations more nimble when something inevitably happens, even if it's not exactly what was considered.

Across the industry, healthcare leaders are pondering what care delivery will look like going forward. One thing is certain: this future state will not include a return to the status quo—not with the level of disruption and change that has already occurred. By hardwiring a measured response for enterprise risk management, healthcare boards can strengthen resilience and better position their organization to successfully manage volatility in a COVID-transformed environment.

Discussion Guide for Board Members

1. What is the organization's portfolio of enterprise risk?
2. What is the organization's "risk budget"—in total and within vertical silos?
3. If one of these risks or some portfolio of them is realized, what will be the impact on the organization's financial position/reputation/compliance/market strength/etc. and its ability to execute strategy and succeed?
4. How can leadership's approach to ERM enhance and drive the organization's success?
5. Where does the organization "own" outsized risk?
6. Does the return justify such risk?
7. Can some controllable risk be taken off the table?
8. If various risks are realized, how long will the organization be able to incur such risks before experiencing significant harm?
9. Might the organization be experiencing a new level or "normal" for enterprise-wide risk that is materially more challenging than in earlier years?

Resources

The information in this toolbook has been compiled from the following Governance Institute publications:

Marian Jennings, "Focused Growth: A Strategic Framework," *Hospital Focus,* August 2022.

David Burik and Danielle A. Dyer, "To Manage Volatility, Sharpen Your Enterprise Risk Management Strategy," *E-Briefings,* Vol. 19, No. 1, January 2022.

Bob Chaput, *Enterprise Cyber Risk Management: A Toolbook for Healthcare Boards and Executives,* The Governance Institute, Summer 2021.

Marian Jennings, "Enterprise Risk Management: Moving beyond Compliance," *BoardRoom Press,* Vol. 31, No. 6, December 2020.

Daniel Zismer, "Managing Strategic Risk Effectively Requires Shared Beliefs," *BoardRoom Press,* Vol. 30, No. 3, June 2019.

Marian Jennings, "Navigating Strategic Uncertainties: The Board's Role," *BoardRoom Press,* Vol. 28, No. 6, December 2017.

Kenneth Kaufman, *Focus on Finance: 10 Critical Issues for Healthcare Leadership* (2nd Edition), The Governance Institute, 2016.

James W. Blake, Ryan S. Gish, and Eric A. Jordahl, *Managing Enterprise Risk to Achieve Sustained Success in the New Healthcare Environment* (white paper), The Governance Institute, 2011.

Appendix 1. Sample Enterprise Risk Management Committee Charter

This committee charter was adapted from a sample corporate risk committee charter based on leading practices developed by Deloitte, with input from Hunterdon Healthcare and ***ACCORD*** *LIMITED. If applicable, these responsibilities can be combined with the compliance committee.*

Purpose

The principal purpose of this committee is to task management with the development of a risk management program, oversee and approve the organization-wide risk management practices, and assist the board in ensuring that the risk management infrastructure is capable of addressing risks faced by the organization.

Responsibilities

In fulfilling its charge, the enterprise risk management committee is responsible for the following activities and functions:

- Help to set the tone and develop a culture of the enterprise vis-à-vis risk, promote open discussion regarding risk, and integrate risk management into the organization's strategic goals and compensation structure.
- Provide input to management regarding the enterprise's risk capacity and tolerance and approve the statement of risk capacity and tolerance developed by management.
- Monitor the organization's risk profile—its ongoing and potential exposure to risks of various types.
- Approve the risk management policy, plan, infrastructure, and framework developed by management. The risk management plan should include:
  - The organization's risk management structure
  - The risk management framework and/or approach
  - The standards and methodology adopted¾measurable milestones such as tolerances, intervals, frequencies, frequency rates, etc.
  - Risk management guidelines
  - Details of the assurance and review of the risk management process
- Review the risk management plan at least once a year.
- Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products or service lines), and transactions and exposures (e.g., by amount) and prioritize them prior to being sent to the board's attention.
- Regularly review information provided by the Chief Information Security Officer (or top executive responsible for cybersecurity) to assess the organization's risk profile for cyber attacks and sufficiency of management's handling of data storage, security protocols, and response to cyber attacks.
- Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities.

- Oversee and assess the risk program/interactions with management and obtain regular assurance from management that all known and emerging risks have been identified and are being mitigated/managed.
- Periodically review and evaluate the organization's policies and practices with respect to risk assessment and risk management, including the effectiveness of management's corrective actions for deficiencies that arise, and annually present to the full board a report summarizing the committee's review of the organization's methods for identifying, managing, and reporting risks and risk management deficiencies.
- Monitor governance rating agencies and their assessments of the company's risk and proxy advisory services policies, and make recommendations as appropriate to the board.
- In coordination with the audit committee, understand how the organization's internal audit work plan is aligned with the risks that have been identified.
- Perform an annual committee self-assessment; review the committee charter and advance recommendations for any changes to the board for approval.

Composition

The risk committee will comprise three or more directors as determined by the board. The membership will include a combination of executive and non-executive directors. The committee may include non-directors as members. Each member will have an understanding of risk management expertise commensurate with the organization's size, complexity and capital structure. The chief risk officer or senior executive in charge of risk will serve as staff for the committee.

Recommended skills and competencies:

- Laws and regulatory policy
- Legal implications related to risk management
- Enterprise risk concepts in relation to the healthcare industry and the organization itself
- Familiarity with identification of risk and insurance models
- Conflicts of interest and confidentiality

Meeting Schedule

Quarterly or as needed.

Appendix 2. Sample Enterprise Risk Management Policy

Policy No.: _____
Title: Enterprise Risk Management
Policy Date:
Approval Date:

Definition:
Enterprise risk management (ERM) is an ongoing strategic process that is applied systemically across the organization. It closely links the organization's strategy, operations, finance, and treasury,[6] which together define the totality of a healthcare organization's risk-bearing chassis. The ERM process is designed to identify potential events and risks that may affect the organization and to help prioritize and then manage those risks in the most appropriate manner given the organization's defined risk "appetite."

Recommended Approach:
- A process of thinking about and actively managing risk across the entire enterprise in order to achieve the highest possible business success
- An optimal way of thinking about the organization's most significant risks and opportunities, matched against the organization's ability to carry such risks and achieve such opportunities
- A process used to integrate strategy, operations, finance, and treasury activities in the organization
- The "heart" of a vibrant and enterprise-wide ongoing strategic process that is applied systemically and horizontally across the organization, closely linking strategy, operations, finance, and treasury

Purpose:
The board is responsible for approving and monitoring the organization's enterprise risk policy, plan, infrastructure, and framework developed by management.

Policy:
The organization's ERM process and plan will:
1. **Be CEO-championed.** The CEO has direct responsibility for "driving" the approach, with engagement and approval by the board and involvement of managers across the organization.
2. **Be guided by an assessment of controllable and non-controllable factors**, and applied across the whole organization. Controllable factors are internal to the organization, emanating from its business activities. Examples include service line offerings, physician integration strategies, and staff compensation models. Non-controllable factors are external variables that can impact

6 "Treasury" management is the management of the non-operating assets and liabilities of a business or organization.

the organization independently of how it is operating its businesses, such as regulation, worldwide capital markets, and payment systems. Mapping controllable and non-controllable risk (measuring risk on a "severity of impact" and "likelihood of occurrence" grid) can provide a visual representation of identified risks in a way that easily allows ranking and prioritizing.

3. **Use a corporate finance approach** plus **scenario envisioning.** The corporate finance approach provides the quantitative discipline and specific tools needed for analytic work. Tools include a credit analysis, integrated strategic-treasury-financial plans, sensitivity analyses, financial models, and asset-liability management analyses. Scenario envisioning or planning is a forward-looking, more qualitative approach that asks the broadest possible "what if" questions.
4. **Be defined as a critical organizational success factor.** An organization's long-term financial success will be linked to how well its leaders understand and ensure the application of ERM enterprise-wide. Accomplishing far more than helping to manage or mitigate risk, ERM guides organizations toward identifying, seizing, and achieving opportunities

Procedure:

Supported by the CEO, the organization's management team uses ERM to closely monitor risks, according to defined risk-tolerance guidelines that emerge from comprehensive assessments. The team also uses ERM to track trends and issues with strategic and financial implications, and devise and implement effective plans to address the challenges.

The board (or appropriate board committee responsible for enterprise risk) will:

1. Review the risk management plan at least once a year.
2. Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products or service lines), and transactions and exposures (e.g., by amount) and prioritize them.
3. Oversee and assess the risk program/interactions with management and obtain regular assurance from management that all known and emerging risks are being identified and mitigated/managed to the board's expectations.