ENTERPRISE RISK MANAGEMENT

Part One:

Defining the concept, recognizing its value

FOREWORD

This three-part monograph series Enterprise Risk Management is available as three PDF documents on the Web site of the American Society for Healthcare Risk Management (www.ashrm.org, Resources).

INTRODUCTION

Today's health care organizations are complex entities facing new challenges and emerging risks that pose threats to their financial and operational well being. Enterprise risk management (ERM) is taking root – spurred by globalization of business and financial markets, increased integration of capital markets and the insurance industry, development of sophisticated tools for risk modeling, increased regulatory controls, and greater interest in corporate governance.

ERM provides a new approach to identifying and treating risks and to gaining advantage in the health care delivery marketplace through management of risks found across the organization. These risks go beyond the traditional focus of medical liability or safety issues. Indeed, these risks are as diverse and fundamental as the business operations of the health care organization itself. They are every bit as hazardous as unmanaged clinical risk.

However, when risks are successfully recognized, managed and mitigated through a well-orchestrated ERM approach, they become key elements in a strategic plan and offer forward-thinking organizations a tool for achieving business success.

WHAT IS ENTERPRISE RISK MANAGEMENT?

ERM, as defined in the *Risk Management Handbook for Health Care Organizations* (4th ed.), is a structured analytical process that focuses on identifying and eliminating the financial impact and volatility of a portfolio of risks rather than on risk avoidance alone. Essential to this approach is an understanding that risk can be managed to gain competitive advantage.

ERM utilizes a process or framework for assessing, evaluating and measuring all of an organization's risks. In essence, it is integrated risk management. ERM quantifies risks to determine significance, groups them into components or "domains" looking for either inter-relatedness or inter-dependency and devises strategies to manage each.

Two key principles

The first essential principle of ERM is that it recognizes a broad range of risks confronted by the organization and acknowledges that those risks represent either sources of capital or potential for losses.

When recognized as "capital," risks can be viewed as having either a negative (that is, having only potential to adversely effect the organization) or a positive (or upside) potential. This recognition is central to the ERM premise because it stresses management of risk to exploit the upside possibilities of risk.

The second essential principle is that a comprehensive, or "holistic," approach is critical to managing diverse risks. An enterprise-wide view recognizes all of the potential threats to the organization's business and strategic objectives. As explained in a Dec. 1-6, 2002, ECRI Risk Management Reporter article titled "Enterprise Risk Management takes hold in health care," this view requires awareness that risks are not isolated. While entities tend to organize themselves operationally into silos, their associated risks do not exist in isolation. For example, the Emergency Department and the Legal or Finance Department share easily crossed barriers. The risk of one is inter-related to, and possibly inter-dependent on, other areas as well as to the organization's overall strategic plan.

The inter-relatedness of these risk exposures is easily seen in the emergency department (ED). Emergency Departments face significant regulatory and legal issues such as EMTALA on a daily basis and also

continued on next page

represent the single largest source of admissions to most hospitals. The ED can put a health care organization at risk for fines and penalties for failing to meet the requirements of applicable laws and regulations. When operations in the ED do not run efficiently, waiting times can become extended and increase the risk that urgent care is not delivered promptly or worse, not at all. Patients who leave without treatment cause potential professional liability exposure as well as loss of revenue – significant financial impact in both short- and long-term views.

Organizational philosophy

Understanding a health care organization's current view of risk is a good orientation for ERM's broader perspective. The organization's overall approaches to risk management and risk tolerance are key factors. Determining whether an organization views risk as something to be tackled proactively or responded to or reacted to gives a good indication of its core philosophy toward risk management.

Risk tolerance is another indicator of how organizations view risk. Healthy, profitable organizations may be willing to tolerate more volatility than a less profitable organization. This can often be expressed in levels of self-insurance and retentions. Health care organizations with a low tolerance for risk – i.e., risk averse – are apt to limit their exposure by limiting the degree of risk retention or being aggressively proactive about mitigating risk.

Risk domains

The variety of risks facing a health care organization today can be appreciated by looking at the domains (detailed in the *Risk Management Handbook for Health Care Organizations*) that ERM recognizes:

- **Operational:** Derived from the organization's core business, including its systems and practices. Examples include clinical services and outpatient care.
- **Financial:** Risks related to the organization's ability to earn, raise or access capital as well as costs associated with its transfer of risk. Examples include bonds and insurance premiums.
- **Human:** Relates to the risk related to recruiting, retaining and managing its workforce. Examples include worker's compensation, employee turnover and absenteeism, unionization and discrimination.
- **Strategic:** Risks related to the ability of the organization to grow and expand. Examples include joint ventures, mergers, profitability, customer satisfaction and financial performance.
- **Legal/Regulatory:** Risks related to health care statutory and regulatory compliance, licensure and accreditation. Examples include HIPAA compliance, OSHA regulations, Medicare-deemed status and JCAHO accreditation.
- **Technological:** Risk associated with biomedical and information technologies, equipment, devices and telemedicine. Examples include clinical information systems such as computerized physician order entry and radiology picture archiving and communication systems and off-site monitoring of critical care units.

ERM VS. TRADITIONAL RISK MANAGEMENT

Traditional health care risk management takes a clinically focused approach and examines risks individually. This model defines risks in terms of the probability that adverse events will occur and result in financial losses. The risk manager's responsibility under such a model is focused on protecting the assets of the organization.

Risk management activities center on ways to mitigate the impact of adverse events on operations and finances. The risk manager works to implement techniques to avoid, control, reduce or contractually transfer financial losses. Through the use of risk financing techniques, financial losses resulting from adverse events are retained or transferred. This theory, outlined in the *Risk Management Handbook for Health Care Organizations,* maintains that risks are best managed within the functional silos of finance, insurance, human resources and safety, and holds that shareholder value is maximized through partial or full risk transfer.

However, this approach fails to appreciate relationships among risks and lacks the optimization of collective risk evaluation and management through an enterprise approach. It also lacks a common definition of risk and universal measurements to gauge the effectiveness of risk management efforts. Instead of handling risk in functional silos where measurements of success are variable, ERM strives to use common metrics across risk domains to determine the effectiveness of risk management approaches.

With an integrated, enterprise-wide view of risk, the risk manager has a much more strategic position, focusing on opportunities as well as risks. The growth of ERM has resulted in the emergence of the chief risk officer (CRO, as detailed in Part 3 of this monograph) as the executive responsible for leading the team of senior managers from operations, finance, human resource and other key areas in aligning risk management strategies with the organization's business strategies aimed at maximizing shareholder value. Under ERM, managers as well as front line staff understand and promote a common organizational risk management strategy as the way of doing business. It is incorporated into the culture of the organization as a shared set of beliefs necessary to achieve its mission.

The following example contrasts one aspect of risk management – risk identification – using a traditional with an integrated approach under ERM. It exemplifies the advantages of the latter using new technology in the shift from a silo-centric, reactive focus to an integrated, proactive one.

Risk identification under ERM

Event reporting and trending has been a keystone element of risk management in the identification of events and incidents that expose the organization to the risk of loss, especially liability losses. Traditionally, event reporting systems have been used to notify the risk manager of adverse and potentially compensable events and to catalog reported events.

With the continuing development of electronic event reporting systems comes the ability to generate aggregate reports of events for

trending purposes. While aggregate data report support monitoring of the frequency of events, pertinent event-specific information or trends may or may not be available in a timely manner to those in the best position to analyze and act on the information. This results in a time lag between the event's occurrence and the interventions necessary for mitigation of future adverse effects. In addition, the benefit of multiple perspectives on implications of adverse events and trends across the organization is not realized.

New technologies such as real-time, electronic risk management identification systems (RMIS) can be employed in an integrated, enterprise-wide risk management program allowing information to be shared across functional disciplines. With multiple perspectives from diverse individuals and support for collaboration between groups, more effective management of risks across the organization can be attained.

For example, the patient complaint handling process presents a key opportunity for risk management across the enterprise through service recovery and prevention of similar complaints in the future. The use of an integrated RMIS to report, communicate and act on a patient complaint involving a delay in notification of diagnostic test results can alert involved clinicians and departments as well as key individuals to a problem. The complaint can be evaluated for risk potential (Was there a delay in diagnosis?), quality and safety impact (Was inappropriate care provided?) and service improvement opportunity (Who should communicate [disclose, apologize] to the patient?) Further analysis may reveal system issues involving how diagnostic test results get reported. The diagnostic test reporting process as it is currently should then be evaluated against how it could be. Improving such a process involves multiple people, departments and systems – in short, multiple perspectives.

Using patient perception of safety as another example, a January 2005 study linked patient concerns about medical errors in the ED to lower patient satisfaction ratings and a reduced willingness to return for care and reduced likelihood that patients would recommend the hospital to others. (Burroughs, T.E., Waterman, A.D., Gallagher, T.H., et al., "Patient concerns about medical errors in emergency departments," Academic Emergency Medicine.) Taking an enterprise view of risk, patient complaints and concerns represent not just exposures to loss, but rather, they also present key opportunities to improve satisfaction and to increase market share through repeat ED encounters, increased visits and the hospital's good reputation in the community. Patients who are more satisfied with their care are less likely to initiate malpractice claims.

Accordingly, patient satisfaction affects many of the risk domains of ERM, including operational, human and strategic. Therefore, information on events and patient concerns and complaints arising from the ED should not be limited to the risk manager and ED staff, but rather should be shared with multiple disciplines to capitalize on broader perspectives for correction and improvement. Improving care and patient satisfaction in the ED is interdependent upon such things as clinical competency of the ED staff, physical access and environment, patient identification procedures and systems for medication administration, to name a few. Improvement involves individuals and systems far beyond the walls of the ED, too.

ERM as a management philosophy

The use of a "confluence of perspectives" for defining and solving problems in an ERM model was described in a presentation at ASHRM's 2004 Annual Conference as utilizing a common frame of reference to evaluate data and integrating the management of problem-solving through process management. (Hajek, M.A., Robins, M., "The enterprise management of risk and safety: TRQS2 Model.") When all are evaluating the same set of circumstances collectively, multiple perspectives on an identified problem converge, and thus a broader definition of the problem and how it can be solved emerges. Viewing a set of circumstances from a common frame of reference allows managers and staff with previously departmentalized perspectives to see the connection between departments and the broader implications for the organization as a whole.

CONCLUSION OF PART ONE

For reasons described above, risk managers are in a unique position to initiate change and move the organization toward an ERM model. Armed with an understanding of ERM concepts, executive support for a positive transition to ERM can be garnered through education, the setting of objectives and alignment of risk strategies with the organization's overall mission, goals and strategic objectives – the subject of the second part of this monograph: "Enterprise Risk Management: Getting an ERM program started."

RESOURCES

Journal of Healthcare Risk Management, American Society for Healthcare Risk Management: Berkowitz, S.L., "Enterprise Risk Management and the health care risk manager," Winter 2001; Hoyt, R. E. and Hall, E .B., "Enterprise Risk Management: Evidence shows changing role of health care risk managers," Spring 2003.

The Risk Management Reporter, ECRI, "Enterprise Risk Management takes hold in health care," Dec. 1-6, 2002.

Essentials of the Risk Management Process, Head, G.L., Horn, S. Insurance Institute of America, 1985.

Risk Management Handbook for Health Care Organizations (4th Ed.) Carroll, R., editor. Jossey-Bass, 2003.

ENTERPRISE RISK MANAGEMENT

Part Two:

Getting an ERM program started

INTRODUCTION

When the decision has been made to incorporate enterprise risk management (ERM) within an organization, a major ideological shift is required. The ERM model requires organizations to think systematically and eliminate functional silos.

ASSESSMENT

One of the first steps involved in implementation is to educate all appropriate staff about the ERM concept and why it is the right approach. This education is essential to garner the support necessary to make for a successful transition. Executive cooperation is necessary, because this type of change will require a significant commitment of time and human and financial resources. Leaders have considerable influence over the internal corporate environment and their support sets the "tone from the top" which is essential for culture change. They can influence progress and encourage the evolution.

RISKS AND OBJECTIVE-SETTING

Without clearly stated objectives, using ERM to set risk priorities is destined to fail.

An organization must know its goals and objectives before management can identify events that might interfere with those objectives. Objective-setting is applied in the ERM context when an organization evaluates and develops its risk strategy in the context of its mission, values and strategic objectives. It involves understanding how corporate objectives and risks interrelate and affect the achievement of goals. This alignment of purpose comes with taking a "portfolio view" of risk in the organization as a whole and in the individual business units.

One example of objective setting would be if a health care organization determined that a major strategic goal is to develop a reputation as the leading provider of neonatal intensive care services in the region. This new focus would require expanding the scope and depth of services it already provides. By necessity, the resources to meet this goal would significantly affect the resources available for all other strategic objectives.

Risks may be categorized into six major risk domains that are explored in the process of objective setting. These domains, which were detailed in Part One of this monograph, are strategic, operational, financial, legal/regulatory, technology and human capital risks.

Setting objectives while evaluating all risks allows the organization to define its risk tolerance, the amount of risk exposure or potential for adverse events the organization is willing to bear, and its risk tolerance, which is the level of acceptable and unacceptable exposure from a single risk on a particular corporate objective. Once the exposure rises above the acceptable threshold, internal risk management systems would be implemented.

Event identification: Risk or opportunity?

During event identification, an organization examines all internal and external events that could affect the achievement of its goals. It then differentiates between risks and opportunities.

A risk is an observable event with potential for a negative impact on goals and objectives. A risk event that an organization might consider when developing strategy would be the arrival of competitors in the same community. This would have the potential for negatively affecting market share and revenue generation.

An opportunity is an event that may have a positive impact; once identified, opportunities are incorporated into management's strategy or objective-setting. An opportunity might take the form of a strategic alliance with a competitor.

Causes of risk to any organization come from people, corporate culture, systems and processes in place, or decisions made by management. Risk events can include a loss of assets, business interruption, employee work actions, professional liability, environmental or safety breaches, and fraud and abuse. These can affect the organization in the areas of reputation in the community as well as creating financial, legal and regulatory exposure. By dissecting possible events and identifying their impact and causes, an entity can better assess the likelihood and severity of impact of each. The process of event identification should be continuous.

Risk assessment: Inherent or residual?

This phase involves the evaluation of all potential events to determine their impact and likelihood of occurrence. This enables an organization to understand how these potential events can affect goals and objectives, and to determine how to manage them.

Evaluation promotes an understanding of the interrelationship of the risks across the entity, which is necessary to prepare a proper organizational response plan. Risks can then be prioritized so that those with the highest potential impact, for which the organization is the least prepared, are addressed first. Risk assessment should be a continuous part of business planning

Risk likelihood and consequences can be evaluated on an inherent or a residual basis. Inherent risk is viewed without consideration of any of the mitigating controls an organization has in place. Residual risk considers risk in conjunction with existing control mechanisms. Control assessment examines what controls are in place, and how effective they are to manage the identified risks.

For example, an organization might identify that extended negotiations with a particular labor union have been unproductive, and a strike appears likely. If this risk were to materialize, depending on how long it lasted, the consequences would have the potential for a major hit on short- and possibly long-term strategic growth objectives, financial performance and operations across the continuum. The leadership would evaluate this possibility and estimate the costs that might arise across all of the risk domains.

Risk response

Once the risk assessment is complete, focus moves toward identifying, evaluating and developing options to deal with risk. Management evaluates its options based on the organization's risk tolerance, a cost-benefit analysis of the possible responses, and the degree to which the options would affect the impact and/or likelihood of risk occurrence.

Risk handling solutions usually fall into one of four categories: risk avoidance, acceptance, reduction or sharing. Responses are developed to align with the amount of risk the organization is willing to tolerate and what it can afford in light of strategic goals and objectives.

In this phase, the organization would determine its willingness to risk the negative impact that a strike by union workers would have on the bottom line. The decision might then be made to avoid the risk entirely by agreeing to union demands, attempting to reduce the risk by taking a more conciliatory negotiating stance and offering to make some concessions, or accepting the risk and preparing for the potential of a strike.

Portfolio view

The portfolio review of risk permits the leadership to catalog all the risks that exist across the board. Leaders would look at the totality of organizational risks involving, for example, implementation of new technologies, regulatory compliance, human capital, expansion and growth opportunities, insurance and contracting for services. Then an analysis of the entire cross section of risks would take place, evaluating each risk for likelihood of occurrence and the severity of impact. Prioritization of risks to be addressed would follow.

ROLES AND RESPONSIBILITIES

In the ERM framework, risk management becomes everyone's responsibility. It relies on an interdisciplinary approach, with no place for a hierarchical or silo approach to risk management. There are defined roles for certain senior management positions.

Chief risk officer

The leading coordinator of the process is the chief risk officer (CRO). This person is responsible for identifying and quantifying risks and managing the process, analyzing risk strategically. He or she is the facilitator of the activities of the interdisciplinary risk management team, and a liaison and support person for the CEO, CFO and senior management team as well as middle management. The CRO develops organizational policies and procedures, works on concept development and implementation, tracks and trends key risks, and facilitates continuous risk assessment.

This role is a global one, dealing with the overall risk of the organization. (See Part Three of this monograph for a detailed view of the CRO role.)

Board of directors

The board of directors should provide oversight of ERM, understanding its key elements and regularly discussing organizational risks with senior management. It should receive information about significant risks and how management plans to handle them.

Communication with senior leaders, the CRO and other management personnel is essential.

Chief executive officer/president

The chief executive officer (CEO) or president is ultimately responsible for molding the corporate culture and making sure that ERM functions effectively. He or she should assess the organization's ERM capabilities and champion "thinking outside the box." Once the organization's risk philosophy is developed and risk tolerances identified, the CEO should communicate these concepts on a consistent basis throughout the organization, and insist on cooperation from all levels. He or she should communicate regularly with the CRO and CFO to track the implementation and success of the ERM model and report to the board.

continued on next page

Along with other members of the senior leadership team, the CEO continuously reevaluates risks facing the organization and modifies strategy accordingly.

Chief financial officer

The chief financial officer (CFO) provides the analytical insight to determine the organization's risk appetite, looking across the multiple units of the entity to help develop and implement the portfolio view of risk. This individual has the greatest degree of knowledge of the financial condition of the organization and the demands and performance of the individual entities, divisions and departments. With the assistance of senior leadership and the CRO, the CFO views the prioritized list of risks and determines what resources are available to address them. If necessary, financing options would be explored to fund important strategic initiatives.

Senior management is responsible for managing risk in their areas of responsibility. They should establish risk tolerances in line with the corporate limits. These leaders rely on the CRO to develop policies and procedures to implement the ERM model, but they make sure that their departments implement them and comply.

As new risks become apparent through continuous risk assessment, it is the CFO's role to communicate with the CRO. If a new risk is compelling, the entire team, along with the CEO and CFO, would assess the impact on the achievement of existing goals and plan accordingly.

Health care risk manager

The health care risk manager remains on the front lines of the risk management effort and focused on daily operations. He or she develops risk management strategies in line with the business goals and objectives communicated by the CRO and senior leaders. The risk manager also nurtures alliances with other departments to develop a broader understanding of the risks within the organization and adjust risk management policy in response.

The risk manager should continue to regularly report to senior management and the CRO about ongoing or newly identified risks, and be a reliable resource for staff at all levels. Education of staff about enterprise risk management would be another responsibility for the risk manager.

Middle managers and others

Middle managers and other employees are expected to understand those risks for which they are accountable and manage them within the entity's approved risk tolerances. However, they must receive education about the interrelatedness of risk within the organization, learn to think more globally and participate in the atmosphere of open communication.

TRANSITIONING TO ERM

The success of the ERM transition is dependent upon education. The change agent, whether coming from the senior management level, or the risk management level, utilizes education to promote recognition of the need for change for the good of the business enterprise. This education is ongoing and does not cease once the ERM program is implemented.

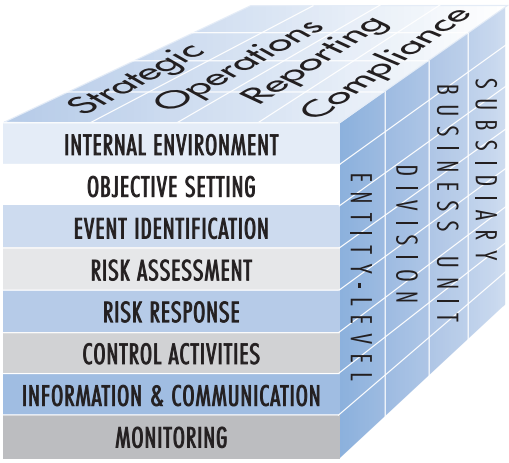
As the change agent, the CRO must sell the program to enterprise stakeholders. In essence, a stakeholder is any person, group or entity who can place a real or potential claim on the organization's resources, attention or output. A stakeholder can be internal or external, management, an employee, customer/patient, a board member, a shareholder, an outside vendor or a person from the community. Stakeholders tend to drive decision-making and risk appetite.

Approaching ERM from a holistic vantage point in a consistent, coordinated global process is the basis of development and rollout of a successful risk management program throughout the organization. While risk management is actually everyone's responsibility, it is more integrated within the ERM model. One way to get people to buy into a concept is to demonstrate how it can be a "win-win" situation for all. ERM should be portrayed as a positive process that is ongoing, flowing through the enterprise and beneficial. This is the challenge for the CRO as the foundation for change is laid.

A generic model ERM

The COSO ERM Framework

- Is a process
- Is effected by people
- Is applied in strategy setting
- Is applied across the enterprise
- Is designed to identify potential events
- Manages risks to be within risk tolerance
- Provides "reasonable assurance"
- Supports achievement of key objectives



Transition to any new program is a challenge and requires a framework to guide the changes. The Commission of Sponsoring Organizations of the Treadway Commission (COSO) developed a generic model ERM program that can be utilized and adapted to the unique needs of the health care organization.

Some of the program's key processes to be addressed are:

- **Setting objectives** (management objectives applicable to all levels)

1. Strategic – linkages among the organizational mission, vision, values and business plan.
2. Operations – roles, responsibilities and assignments; criteria for consistent risk identification and handling.
3. Reporting – concurrent risk monitoring and identification processes; formal communication processes; parameters of accountability.
4. Compliance – monitoring of interventions and other treatments of risks.

- **Achieving structure and organization** (the process components)

1. Risk committee composition – consisting of senior management level decision-makers, business unit (BU) and department level managers, and representatives of front-line workers (See the "ERM Committee" section on page 18.)
2. Responsibilities and authorities – while everyone in the organization has some responsibility in ERM, the board and ultimately the CEO assume ownership.
3. Performance metrics – using established methods of performance related to risk identification and treatment.

- **Employing methods, information and reports**

1. Reduction of operational surprises and losses.
2. Enhancement of risk response decisions – rapid communication and response mechanisms to identify and implement business controls and risk management treatment to bring risk exposure to acceptable level (as determined by the organization's risk appetite).
3. Event identification – analysis and ranking of exposures that threaten not only the business as a whole, but any BU or department.

- **Establishing information technology infrastructure** – the basis of prompt communication throughout the organization; support of rapid reporting analysis and ranking of risks and interventions.

1. Accommodation of predetermined information recipients and pathways.

- **Recognizing roles and responsibilities** – implementation of ERM from the top down and across all domains and business units. Those responsible for the following areas may be unique in the BU, while methods and responsibilities are redundant depending on the risk and ranking:

1. Risk response – as discussed on Page 15.
2. Mitigation – to reduce severity.
3. Strategic plan – action focused on attaining a goal.
4. Exposure and control activities – handling identified risks, such as avoidance, transfer.
5. Transaction level – the predetermined and delegated level responsible to carry out ERM activities to address identified risks.

- **Monitoring** – the ongoing activity undertaken on all levels of the organization with:

1. Early identification of risks.
2. Mitigation and intervention and effectiveness of control activities.
3. Ongoing education and other activities to keep the involvement and sensitivity ongoing and effective.

TOOLS AND TECHNIQUES/BEST PRACTICES

As the ERM program is implemented, the organization's risks are identified, analyzed and prioritized.

Risk mapping

A risk map is a visual aid to depict the frequency of occurrence and possible severity of an organization's risks.

The first step in developing a risk map is to identify the risks to be analyzed. Mapping those risks involves correlating each risk to all others based on these elements. These correlations are set out to depict the significance and relevance to the entire set. In an ERM program, all types of risks and components/elements of the risks can be mapped to assist in identifying and comparing key risk indicators.

Key risk indicators are based on the value drivers of the enterprise, which are an organization's business goals. They must be broken down to the most basic levels that relate to the ERM program and then evaluated.

Developing the threshold of acceptable exposure is the next step: What level of risk is the organization willing to tolerate? This often varies based on the specific risk and relates to risk appetite. Consideration should be give to the likelihood that an event will occur (e.g., "not likely," "likely," "imminent" and "immediate"). Finally, evaluate the severity of impact if a risk event occurred and identify what percentage of the organization/enterprise would feel the impact.

(Risk mapping is detailed in Chapter 7 of the *Risk Management Handbook for Health Care Organizations,* 4th ed.).

continued on next page

Prioritizing risks

After mapping, determination of how to deal with these risks can be made using business mechanisms to address whether to retain and manage, avoid, or transfer the risk.

When prioritizing risks, it is important to keep the number manageable and initially focus on risks that are significant either for their frequency or severity of impact. It can be counterproductive to get bogged down with all conceivable risks at the same time. Less critical risks can always be addressed after more urgent risks.

Risk prioritizing cannot take place without strategic analysis, strategic dialogue and planning dialogue at the highest level of the organization. Depending on the overall level of corporate risk identified, the proper choice may be to refer a risk down to the relevant business unit to handle and report back rather than handle a particular risk on an enterprise basis.

ERM committee

A top-down, big-picture view of the ERM program is essential. Therefore, the ERM committee structure should begin with a senior level risk group that reports to the board. The culture of the organization will determine if a board member is a part of this committee, how often it meets and how often it reports to the board.

This committee should be made up of the CEO, chief operating officer (COO), chief nursing officer, CFO, CRO (and risk manager, if one exists), chief medical officer, chair of the investment committee and chair of the audit committee.

The committee would be responsible for ongoing, organization-wide identification and assessment of risk, as well as development and implementation of risk reduction strategies. The work of this committee must enhance – not impede – the risk management functions of individual BUs.

The local BU-based committees should collaborate with each other. Because there is interdependence among departments and facilities in an organization, the BU-based committee reinforces that departments and risks don't exist independently. For example, an operating suite is dependent on its customers (the nursing units), whose customers are the patients; the operating room staff relies on the materials management department to order, store and deliver supplies, and the biomedical department to handle preventive maintenance and repairs. Therefore, cross-functional representatives from these support services, or domains, can assist in addressing the risks that arise across these lines, contributing their unique perspective to any risk analysis.

Identified risks should be reported to the ERM committee, which will decide whether the risks are to be handled on an organization-wide basis or managed within the related departments.

CONCLUSION OF PART TWO

The transition or conversion plan from the traditional risk management program to an ERM program begins with education of senior management and the board as a basis of "selling" the need for the expanded program.

Once that decision is made, the CRO must lay out the steps to implement the plan. This entails still more education of all employees across the organization, and in all domains or silos, as well as creating an senior level ERM committee. It should not be forgotten that all employees and stakeholders have a role to play in the transition to an ERM program.

RESOURCES

"Enterprise Risk Management takes hold in health care," ECRI Risk Management Reporter. Dec. 1-6, 2002.

Carroll, R. *Risk Management Handbook for Health Care Organizations* (4th ed.) San Francisco: Jossey-Bass, 2003.

Berkowitz, S.L. "Enterprise Risk Management and the healthcare risk manager," Journal of Healthcare Risk Management. Winter 2001, pp. 29-37.

Aabo, T., Fraser, J., Simkins, B. "The rise and transformation of the chief risk officer: A success story on Enterprise Risk Management," Journal of Applied Corporate Finance. Winter 2005.

ASHRM Barton Certificate in Healthcare Risk Management Program Modules. www.ashrm.org.

Ching, W. "Enterprise Risk Management: A new risk paradigm." www.CaptiveGuru.com.

Gooch, C., Kaufman, C. "An urgent call to action: COSO, ERM and the role of the risk manager," Risk Financing & Claims Management INsights, ASHRM Risk Financing & Claims Administration Interest Network, Fall 2004. www.ashrm.org.

Carey, M., "Enterprise Risk Management and business continuity planning," and "Changed world, new risks." www.Delcro.com.

Berinato, S., "Risk's Rewards: Enterprise Risk Management," CIO Magazine, www.cio.com. Nov. 1, 2004.

"Enterprise Risk Management – Integrated Framework, " Commission of Sponsoring Organizations of the Treadway Commission (COSO) executive summary and complete report, available at www.aicpa.org. For details about COSO publications, contact AICPA at (888) 777-7077.

ENTERPRISE RISK MANAGEMENT

Part Three:

The role of the chief risk officer (CRO)

INTRODUCTION

The enterprise risk management model requires the leadership of an individual with a global perspective of the interrelationship of all risks within the entire organization. The chief risk officer (CRO) role has emerged from the ERM movement as the senior level professional best situated to shepherd the concept through the entire entity.

EMERGENCE OF THE ROLE

Industry trends

Interest in ERM arose after some high-profile financial scandals led to huge losses for shareholders and company employees. In the aftermath, there was a great demand for more responsible corporate governance, greater internal controls and risk oversight. This led to federal intervention in the form of legislation, regulations and standards.

It became evident that a paradigm shift away from the business practice of managing risk in functional silos was necessary, and that an enterprise risk management approach could be an effective solution. Boards of directors realized that they needed to be more informed and develop a more thorough understanding of key risks within their organizations and how these were being managed.

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an enterprise risk management framework to encourage and facilitate standardization of the process (detailed in Part Two of this monograph). The central figure in the framework is the CRO. While it does not define or expand upon how the individual business unit risk manager (long established in the health care setting, with varied responsibilities) can fit into and enhance the enterprise risk management process, the concept of ERM is gaining recognition within the health care sector. And as the business of health care grows in size and complexity, the importance of the CRO's role grows.

CRO or risk manager?

The health care risk manager's focus has a local perspective, generally geared toward individual divisions, entities or departments in an organization. Depending on the size and location of the entity, the job varies widely. Many small to medium health care organizations utilize the risk manager in roles including compliance, patient safety and quality. Such institutions often transfer their risk through an insurance program to cover losses, so the risk financing and claims management responsibilities are fewer. The risk manager in these settings is usually a highly visible resource, concentrating on loss control but closely allied with the clinical function. He or she collects, analyzes and trends data for risk identification, reduction and prevention.

In larger organizations, the responsibility for risk control and loss prevention increases with the volume of exposures. Additional staff may be hired to perform the quality, performance improvement and compliance functions, freeing the risk manager to fully assess organizational exposure and pay greater attention to pure risk management functions. Frequently, the role rises to the level of a director, with assistant risk managers reporting up. Larger organizations often employ alternative risk financing methods, providing the risk manager with the opportunity to play a greater role in claims management and risk financing as well as serving as an adviser in such areas as ethics, compliance, medical staff issues, credentialing and human resources.

So what distinguishes the chief risk officer from the risk manager?

In most traditional health care structures, risk is compartmentalized. The risk manager has a snapshot view of risk in specific sectors of the organization, but lacks the wider vision to see patterns and understand relationships. Risk managers are often not sufficiently involved with senior leadership to have input into strategic planning. Decisions are based on isolated issues or circumstances, which often affect the whole in ways that cannot be foreseen with this type of encapsulated perspective.

In the ERM model, the CRO has unlimited access to the other members of the senior management team. He or she is empowered to examine the workings of all departments and entities, has access to financial and operational data and is able ask the difficult questions about "the way we do business." In addition, the CRO is empowered

continued on next page

by leadership to think outside the box and create a picture of the entire organization's risk by connecting the dots among risks in all departments. This individual can design and implement policies and procedures to promote ERM organization-wide.

The CRO makes decisions based on the total picture of an organization's risks and opportunities, and works with other senior leaders to develop corporate goals and objectives in light of all that is known. The role is defined and distinguished by the ability to integrate knowledge and perspective.

OPERATIONAL ASPECTS/ ORGANIZATIONAL PREREQUISITES

Justification for position

Creating the position of CRO, even in an organization with a formal and successful risk management program, can be justified by the magnitude of the work. Changing from a traditional risk management model to ERM requires a tremendous effort in time and human and financial resources. This single individual spearheads the entire effort to centralize all risk management activities, develop an integrated risk management plan throughout the organization, and improve the flow of information and ideas about existing and future risks.

The first step in making the change is eliciting senior level support. The creation of a CRO position is a reflection of leadership's recognition of the strategic value of risk management to corporate goals and objectives. However, this does not mean that leadership understands all that is involved. The CRO must sell the concept by presenting a clear vision of how the organization can benefit from a coordinated, portfolio view of risk, and why it is worth the time and effort to reorganize corporate culture to remove existing functional silos. It might be beneficial to arrange for presentations from other companies that have successfully converted to ERM or consultants that can provide information on the benefits to be gained.

Organizing a department

The CRO should facilitate the ERM process by interviewing senior leaders and board members to identify business goals and objectives. These meetings should also be used to determine what the corporate culture is and learn what types of resistance are to be expected. A review of significant records that can help to develop a plan should follow.

Since ERM involves a systems approach, the next step would be to develop a cross-functional implementation team (ERM committee) with senior managers from operations, information technology, finance, human resources and risk management. Through collaboration, this team would analyze risks across the organization, as well as set strategy for the future in light of the results of the risk assessment. The CRO is the facilitator of this committee and coordinates its activities.

A subgroup of the ERM committee should reach out across the organization to explore what critical risks exist.

This information then goes back to the ERM committee for assessment and analysis, and for evaluation of the internal risk management infrastructure and capabilities. Once the ERM committee has completed its analysis, it can develop a thorough, prioritized list of organizational risk (a risk map). From this, the committee will set strategic goals and objectives, define risk tolerances and develop a plan for dealing with risk and allocation of resources.

With the organization's risk philosophy confirmed, the CRO must develop an educational program to publicize the ERM process and rationale. The CRO must also develop policies and procedures to standardize and operationalize the ERM process throughout the organization. To this end, educational committees composed of risk and other managers in each business unit can spread the ERM message. These committee members will receive ERM education from the CRO and then bring it to their departments or units. They also will continuously monitor risk within the individual entities and the success or failure of enterprise-wide risk management strategies. The CRO should be a liaison between these and the ERM committee, sharing information between them.

Managing risk issues

The nature of the CRO position requires an understanding and the ability to manage many diverse types of risk, and appreciate their interrelationship to the strategic goals and objectives of the organization. The role is a fluid one, with the CRO serving in an advisory capacity to both senior leaders and line staff. It involves supporting the CEO, CFO and board of directors by developing frameworks and processes for dealing with the identified and prioritized risks and assuring that the ERM educational program is rolled out throughout the organization.

With an expansive perspective on enterprise risk, the CRO is responsible for identifying and promoting new and creative means for managing risk, as well as managing and updating a catalog of all key risks. He or she must be able to broadly interpret the risk climate, both internal to the organization and external. The CRO manages the revision of risk profiles and facilitates ongoing risk assessments.

Visibility

The CRO must remain visible as the ultimate authority on risk throughout the entire organization. In order to constantly have a finger on the pulse of threats to the strategic goals and objectives, the CRO needs to be an ever-present source of information and perspective.

Communication with internal and external customers can be both formal and informal. Meetings are important for getting and keeping the message out, as are newsletters, phone calls, memos and e-mails. Formal periodic reports to the board and other senior leaders are another means. As risk managers have learned, one gets much more current information by keeping the lines of communication open and being available to members across the organization.

CHARACTERISTICS OF A CHIEF RISK OFFICER

Credentials and skills

Chief risk officers come from a variety of disciplines, including auditing, strategic planning, investor relations, line-operation management and hazard risk management. If there are state and federal regulatory drivers, the position may be viewed as a legal champion role.

The candidate's necessary credentials may vary depending on the size, strategic direction, and complexity of the organization. Organizations with insurance products or those with a high dependence on credit and bond markets may find that insurance, actuarial and accounting backgrounds are assets. CROs with a background in finance and accounting may find their role redefined to include the management of strategic, legal and operational risks. Due to the impact of state and regulatory actions including Sarbanes-Oxley, HIPAA, Stark, as well as the cost of malpractice litigation, it is common to find CROs with legal backgrounds in health care organizations.

There appears to be no single educational pathway to the CRO position. Instead, as the list of programs listed in the Resources section at the end of this monograph attests, a solid industry related degree coupled with progressive experience and excellent communication skills are the key to advance to this position.

The CRO is generally charged with three major tasks: coordinating all RM activities, introducing an integrated framework, and improving risk communication with internal and external partners. Key background skills center on math, finance, communication and accounting (as summarized in findings from the publication "A composite sketch of a Chief Risk Officer" by Karen Thiesson of the Conference Board of Canada, Brian Markley of Tillinghast-Towers Perrin and Robert Hoyt of the Center for Enterprise Risk Management at the University of Georgia). The ability to communicate effectively is key. From a governance perspective, the CRO must be able to distill strategic operational, financial and "reputational" risk management information in a manner that enhances the board's understanding.

A background or understanding of statistics and the use of quantitative tools is also important. In "The evolving role of the CRO," a survey published April 2005 by The Economist Intelligence Unit, the ability to measure and compare risk and reward and technical risk management skills (e.g., risk measurement, risk modeling, etc.) were rated second and fourth among skills and experience most important in an effective risk manager. The ability to understand business issues was rated as most important.

Experience and education

The CRO position requires an experienced professional; however, the CRO is not expected to be the expert in every area confronting the organization. CROs tend to have a broad health care and business background combined with the communication skills required to influence the board, managers and employees responsible for making day-to-day decisions.

There are opportunities for risk management professionals to move into the CRO role. Risk managers should supplement their experience and education where necessary. A Jan. 25, 2005 Business Insurance article titled "Risk managers shatter glass ceiling by expanding role, relationships" quotes a risk management recruitment and coaching firm president saying "a strong financial background is important for risk managers who want to go beyond the risk management department."

SAMPLE CRO JOB LISTING

"The right candidate for this position will have over ten years experience in increasingly responsible positions within Risk Management, Internal Audit/Compliance, Public Accounting or Consulting. Experience in Risk Management at an academic medical center is highly preferable, and the candidate will have led or helped lead an Internal Audit function that is organizationally broad and deep, engaged collaboratively with all parts of the organization, and seen as a true resource to management. He or she must be able to develop and build an organization-wide, service-driven Risk Management function that is proactive, progressive and collaboratively aligned with the many disparate organizational entities.

The right candidate is a true leader and builder. He or she must be able to work effectively with all levels of the organization in crafting the Risk Management function. Therefore the candidate must have the appropriate business experience, interpersonal and relationship building skills, as well as maturity and judgment. Success in the role requires the political sense to serve multiple constituencies, the vision and leadership credibility to build a state-of-the-art function, and the personal warmth to fit in with a leadership team of people with strong professional dedication."

-- Recruitment ad in ZD & Co. News, http://www.zurickdavis.com/zdnews.asp

TOOLS

Job descriptions

Job descriptions will vary according to the priorities and complexities of the organization. A survey by Tillinghast titled "Information technologies for support of Enterprise Risk Management" reveals most CROs report to the CFO, though in companies with an active ERM program, the majority report to either the CEO or the board. This is a complex position that, as Dr. Robert Mark said in April 2005 at a Chief Risk Officer Forum in Chicago, requires "the ability to efficiently integrate all components of risk as well as to effectively operate in markets while serving customers as well as satisfying regulatory requirements."

continued on next page

Sample job description components, taken from the Economist Intelligence Unit survey, include:

Chief Risk Officer: Develops and coordinates the organization's enterprise risk management framework. Provides the board with a clear vision of where enterprise risks lie, helps define a policy for distributing and offsetting those risks, and works to communicate that vision so that individual managers understand and support it. Reports to CEO or CFO. Direct reports include attorney, risk manager and compliance officer.

Key tasks:

1. Chairs the enterprise risk management committee
2. Develops a framework for the organization's risk management activities
3. Ensures that the organization is in full compliance with regulations
4. Policy assessment
5. Assures business continuity (ability to sustain operations in the event of a disaster) through risk assessment, planning, financing and risk transfer
6. Identifies and monitors emergent risks
7. Extends risk principles into the wider business strategy
8. Develops the data strategy required to build an accurate picture of operational risk; uses models to describe and quantify
9. Educates the investment community on the organization's risk management strategy
10. Disclosures (internal and external)
11. Informs the board of significant risk issues
12. Delivers an integrated picture of risk across the enterprise
13. Determines the organization's tolerance for risk
14. Evaluates insurance coverage
15. Develops alternative risk strategies
16. Trains and communicates with the workforce on risk management policies and structures.

CRO's role in the risk management structure

The CRO participates actively at multiple organizational levels to integrate risk management throughout the enterprise. The following are examples.

The board or a board risk review committee: Expects management (the CRO) to identify and review the major areas of risk. The committee approves and reviews compliance with policies implemented by the organization. Most often the CRO will report directly to the board or a committee.

Executive risk committee: May be chaired by Chief Risk Officer. Also includes CEO and CFO. This committee provides oversight of risk across the organization. Approves and reviews compliance with risk policies. Monitors breaches of risk tolerance limits and directs action. Sponsors review and analysis on risk exposures related to specific issues. Looks at risk from strategic perspective.

ERM committee: Comprising chief risk officer, corporate functional heads, (Operations, Planning, Human Resources, Finance, IT) and the organization's risk leaders from the main operations (CFOs, Legal etc). Serves to understand relationships between risks within the separate business units.

Organization risk leaders: Risk management, legal, human resources, finance at individual hospital or facility level. They may chair a risk management committee or report on risk management to the senior management team. (In smaller organizations, the organization's risk leaders will be part of the enterprise risk management committee.) In addition to developing policies and framework for this group, the CRO is responsible for training and, in some organizations, supervision of some members of this group. Managers make day-to-day decisions on what is or is not an acceptable risk according to a group policy and within the framework established by the CRO.

Management reports

As explained in Part One of this monograph, the CRO should participate in the preparation of reports and models to assist senior management in its risk evaluation and decision making. One challenge is to ensure there is a formalized process for discussion and debate of the risk/benefit analysis among the various business units to opportunistically increase their risk. One key to bring management together is a common terminology. According to Tillinghast-Towers Perrin's Jerry Miccolis, author of "The language of enterprise risk management: A practical glossary and discussion of relevant terms, concepts, models and measures," "An important aspect of ERM is the strong linkage between measures of risk and measures of overall organizational performance." The CRO needs to incorporate consistent definitions into the reports along with benchmarking information to enhance the common understanding among the management team.

One of the first products presented to the management team will be a detailed risk map. Risk mapping is an important tool that can be used to assist in the understanding, prioritizing and analysis of risk. Risk mapping results in a graphic display of relationships between the frequency and severity of exposures. The organization starts by identifying those assets in which it has a legal and financial interest. These assets are both tangible property and intangible, such as reputation or goodwill. This process may also identify how these losses are covered whether by insurance, shared risk or retained risk. As in many of the exercises, it is important that data sources and actuarial interpretations are used to construct the map wherever possible. (For details about risk mapping, see the *Risk Management Handbook for Health Care Organizations*.) The preparation of the initial risk map will serve to expose the CRO to all facets of the enterprise and foster positive ongoing relationships between the CRO and management team.

The CRO will provide for routine updates to executive management on key risk management issues. These will include reports by the CRO or other staff such as contract reviews, claims management, human resource reports, internal audit reports, compliance issues and regulatory reviews. Ongoing reports will also include the status of action plans, results of ongoing monitors, and organizational compliance with risk management policies.

Proactively, emerging issues will be identified and prioritized for further investigation. Additionally, the risk manager will evaluate risks associated with the organization's strategic planning initiatives.

Board reports

Reports to the board of directors will vary according to the nature of risks faced by the organization. Reports may be made to the board or to a confidential board committee. If no enterprise risk management committee exists, board committees such as compliance or audit can be expanded. At a very minimum the CRO should report at least annually to the board. However, in organizations that are more complex or where there is an active Enterprise Risk Management program, more frequent reporting is recommended.

One key report is the annual risk assessment. This starts with an environmental assessment from a risk management perspective. The risk map created earlier will be a starting point. This should be updated with information provided from multiple sources. Current activities to transfer and manage risk will be evaluated and action plans updated. Special attention should be paid to emerging risk. Risk modeling and other tools can be used to portray linkages and quantify impact.

The board reports should include recommendations for board action and broad policies to manage organizational risk. Additional reports could include updates on key risk management areas and compliance with action plans. Key risk management focus areas include major litigation, results of regulatory compliance surveys, patient safety, patient and employee satisfaction and clinical quality measures. As the April 2005 Economist Intelligence Unit survey predicts, the CRO will also be called upon to manage impact of such diverse issues as public relation crises, IT failures and impact of new regulations. Whether reporting on more routine matters or complex issues, the perspective the CRO brings to the board is one of organizational impact.

CONCLUSION OF PART THREE

Considering that the role of the chief risk officer is relatively new, it has rapidly achieved prominence not only in the financial sector where it began, but also in the health care arena. This role is evolving as the scope and cost of emerging risks changes. With ever increasing regulatory and legislative scrutiny of organizational compliance, the CRO has become an important member of the senior management team. The ability to view risk in the context of the "big picture" of an organization and to "connect the dots" across the entities, is invaluable to the success of any planning efforts. The need for these skills assures that demand for CROs will grow, providing an avenue for professional growth for risk managers in the future.

RESOURCES

Carroll, R. *Risk Management Handbook for Health Care Organizations.* San Francisco: Jossey-Bass.

Monroe, A. "Information technologies for support of enterprise risk management," presentation for Enterprise-wide Risk Management, a conference sponsored by International Quality and Productivity Council of Canada, Dec. 12, 2001, Toronto. http://www.riskinfo.com/seminars/Toronto-12-2001_files/frame.htm

Miccolis, J. "The Language of enterprise risk management: a practical glossary and discussion of relevant terms, concepts, models and measures." www.irmi.com/irmicom/expert/articles/2002/Maccplis05.aspx

Theisson, K., Markley, B., Hoyt, R. "A composite sketch of a chief risk officer." Risk Management Reports, November 2001. www.riskinfo.com/rmr/rmrnov01.htm

The following education programs are listed for information purposes and are not endorsed by ASHRM:

- Colorado Technical University offers a 15-month online program resulting in a master of science in management-project management that includes aspects of risk management (http://degrees.education.yahoo.com/pd?p=deg014002)
- St. John's University School of Risk Management, a division of the Peter J. Tobin College of Business in Bermuda, offers an off-shore program in risk management (http://www.stjohns.edu/academics/graduate/tobin/pr_uni_050601.sju.)

continued on next page

- Harvard School of Public Health through the Department of Health Policy and Management, offers degree programs in health policy and management and a master of science in health care management (http://www.hsph.harvard.edu/Academics/hpm/)
- Georgia State University offers a master of science degree with a major in risk management and insurance (http://www.rmi.gsu.edu/AcaProgs/Masters/MSPFP.htm)
- University of Wisconsin-Madison offers a degree in Actuarial Science, Risk Management & Insurance (http://www.bus.wisc.edu/asrmi/prospective/asiintro.asp)
- The Fox School of Business and Management at Temple University offers undergraduate and graduate classes in health-care risk management (http://sbm.temple.edu/)

REPRINTING THIS MONOGRAPH

2005 ASHRM MONOGRAPHS TASK FORCE

Chair
Rosemarie Braz, RNC, BS, FASHRM, CPHRM

Members
Denise Barger, BA, CPHRM, CPHQ
Karen Geller, RN, JD
Leilani Kicklighter, ARM, CPHRM, DFASHRM
Michael S. Midgley, BS, MPH, RN, CPHRM
Kathleen Shostek, RN, ARM, BBA, FASHRM
Evonne G. Ulmer, RN, MHA, JD, FACHE

Also contributing
Peggy L. Nakamura, MBA, JD, CPHRM, DFASHRM