ERM for health systems — Your questions answered

November 07, 2013

Guidance for health care internal auditors

In the fall 2013 webcast *ERM: Perceptions from Health Systems That Got It Right,* health care internal auditors learned the benefits of and successful methods for implementing an enterprise risk management (ERM) system.

The webcast prompted valuable questions. In response, the following insights are provided by Bailey Jordan, Grant Thornton LLP Governance, Risk, and Compliance partner; David Hughes, Hospital Corporation of America assistant vice president of ERM and business continuity planning; and Claire Meehan, Kaiser Permanente executive director of ERM.

Download the webcast presentation (PDF) and replay the webcast.

Q: How often do you cycle through the ERM process?

A: David Hughes (**DH**): Annually.
Bailey Jordan (**BJ**). Health systems with major changes in processes, systems and organization structure, and risk profile are updating the direction/movement of their top 10 risks and consider emerging risks on a quarterly basis. Some organizations are moving to six-month cycles. Again, it is driven by the number and complexity of changes in the health system.

Q: It seems you rely primarily on one-on-one meetings with officers and surveys. To what extent do you utilize facilitated discussions involving multiple executives at one time?

A: DH. Our facilitated discussions are conducted after the initial assessment. We present the results to the entire executive management team, and the results create the discussion. We also distribute the result to all of the interviewees and frequently are asked to present at their division or department leadership meetings.
Claire Meehan (**CM**). On a few occasions, ERM has facilitated a deeper dive on a specific risk, bringing in a cross-functional group with subject matter knowledge and understanding risk exposure from a variety of perspectives. The purpose is to understand the full exposure and consider what more the organization could do to increase the likelihood for success. The recommendations are then reviewed with the executive team.

Q: Do you conduct interviews in person or by questionnaire?

A: DH. Last year we did 52 of the interviews in person and 42 over the phone. We received 180 responses to our survey of the hospital and subsidiary leadership teams (about 70%).
CM. The interview of the executive team and other senior leaders is done in person, as part of the formal annual refresh of the ERM profile. The intent is to foster dialogue about the both the external risk landscape and internal capabilities to gain better understanding and insight of enterprise and emerging. We also conduct a survey of a broader set of management.

Q: Along the lines of facilitated discussions, have you utilized scenario analysis techniques in furtherance of ERM?

A: DH. Not formally.
CM. Strategic planning department uses scenarios in estimating risk/opportunity. ERM collaborates with strategic planning to tighten linkages between assessments of top enterprise risks with scenarios used in strategic planning.
BJ. This is becoming more prevalent, including stress testing of the scenarios.

Q: Approximately how many total risks do you rank in your surveys?

A: DH. There are about 170 risks in our risk universe. In any given year, there are about 25 to 35 risks that are mentioned in our interviews. We rank them and focus on the top 10.
CM. We survey on the top 10–12 risks, and then ask a couple open-ended questions about other risks of a similar magnitude, and areas of concern and such.

Q: Since both of your organizations have hundreds of different locations, do you try to identify risks relevant to any specific hospital location or is that outside of the enterprise risk management process?

A: DH. Our internal audit department uses a tool we developed to help risk-rank each of our hospitals, based on a number of factors. Operations leadership has reviewed the model and provided input to help validate it as to how they would also determine risk. It keys off many attributes like revenue size, earnings budget vs. actual, tenure of the CFO, time since last audit, audit results from last audit, etc.
CM. Enterprise risks are those that are material to the enterprise. Location and business unit risks are considered through interactive and planning processes. Risks are evaluated in the context of enterprise risks to see if the ERM profile needs to be updated to reflect or adequately characterized the risk. A risk in a particular area might be a "top risk" for that area but not a top risk for the enterprise. Looking at risk from various perspectives and scopes is very important.

Q: How does your organization identify risks in the operational/clinical areas?

A: DH. Primarily through our interviews/surveys with our clinicians and our operations leadership.

Q: What is your typical response rate when sending out the annual risk surveys to key leaders? What do you do to ensure leaders actually complete and return the surveys?

A: DH. Most of our information is gathered in face-to-face interviews or conference call interviews. Our surveys are sent to a sample of the hospital and subsidiary leadership teams. The surey is introduced with an email explaining what the process is all about, how the information will be used and why it is important for them to complete it. We get about 70% of them back, which is a little disappointing. I know someone else in health care that put together a brief webinar that covers why the survey is important and seemed to get a better response rate. We may try that next year.
CM. ERM conducts one-on-one interviews with each member of the executive team. A broader survey of management is conducted. It is focused, fairly brief. The request comes from the chief strategy officer. Respondents are given about two weeks to complete the survey, with two reminders. The survey was sent to slightly over 200 senior managers/leaders. Response rate between 50–60%.

Q: Once risks have been identified and prioritized, what is done? Do you conduct internal audits to look at controls to mitigate the risks?

A: DH. Yes, the internal audit plan focuses on the top risks that can be audited.
BJ. The top risks are assigned a risk owner. The risk owner is responsible for putting together a cross-functional team that has a primary stake in the risk; it includes one or two "independent" parties to balance the team and bring a different perspective. The risk owner should facilitate a discussion to take a deeper dive on the risk description, risk contributors, potential exposure, current risk mitigation, and further action needed by whom and when. The risk owner is also responsible for providing periodic updates (at least quarterly) to the risk committee or equivalent on progress to monitor and treat the risk.

Q: How do you identify metrics for top risks like "organizational culture," "leadership effectiveness," "communication effectiveness"?

A: CM. Some risks are less receptive to quantitative metrics; however, there are usually some proxy mesaures. For example, one measure may be an employee survey. At KP [Kaiser Permanente] there is an annual survey of all employees which has questions that are reflective of culture, employee engagement, confidence in the organization, leadership, as well as many other people factors such as having information/training needed to do a good job, etc. This is ongoing and continues to be enhanced and gives perspective year over year and by function/area/department.
BJ. Some examples include an ERM charter, clear risk management principles and guidelines that have been communicated to all departments. Senior management's compensation is linked to and dependent upon critical risk management metrics, the frequency the top risks are reviewed with executive management and the board, and feedback from risk owners during the annual risk assessment process. ERM is a continuous process. ERM is an integral part of strategic planning, and the ERM process encourages the consideration of both downside and upside risk/opportunities.

Q: When you present your high-risk areas to executive leadership and the board, do you base the definition of high risk on inherent risk or residual risk?

A: DH. Residual risk.
CM. We base it on residual risks because we are interested in highlighting/discussing areas of greatest exposure.

Q: Do you use the ERM risk assessment in creating your audit plan? Or do you continue to use a separate audit risk assessment? How are the two coordinated, if at all?

A: DH. We use the ERM risk assessment as a basis for our risk-based audit plan. There are other factors and discussions with management, but the assessment is the starting point.
CM. ERM information is one input into the internal audit work plan, and audits are mapped back to the ERM profile to look at areas of coverage.

Q: How does your organization ensure the ERM risk assessment is in alignment with the risk assessments performed in other areas of your organization (e.g., compliance, financial, information security)?

A: DH. We share our risk assessment with them, and they provide input to it. Our IT internal audit has a risk assessment that is more detailed than ours and is specific to IT. They used our format and share it with us.
CM: At KP, there is an "integrated" risk management approach which has been developed over the last couple of years. Currently there are several areas (high risk, high level of assessments) where a common and coordinated approach is used for assessment, risk ranking and developing assurance plans. As part of this work, a common risk language, framework and ranking criteria [have] been developed that [are] in synch with the ERM approach. The various groups (compliance, audit, technology risk and others) meet regularly to connect the work, and to evolve and enhance how we assess risks, and encourage teaming and relying with/on each other.

Q: You mentioned getting "bogged down in process risks." Would you be willing to share one or two of your enterprise risks? Generally trying to get a feel for how detailed/high level your enterprise risks are identified.
A: DH. Managed care pricing pressures, implementation of electronic health records and bad debts, growth in uninsured/underinsured.

Q: How much of your time is spent, on an annual basis, on ERM?
A: DH. I spend about 50% of my time on it. I also use two staff for about two months to help crunch the data and create the presentations.

Q: How big is your ERM team?
A: DH. For HCA [Hospital Corporation of America], it is just me. I have two staff that help me for about two months each year. The CAE also participates in most all of the interviews.
CM. At KP, the ERM program has one dedicated FTE (executive director of ERM). The program leverages the processes and works across other functions and business units, and reports to the chief strategy officer.

Q: What electronic tools do you use to aggregate and manage your ERM programs?

A: DH. We use Microsoft Office applications (Excel, Word, PowerPoint, Access) and Survey Monkey (upgraded version).
CM. The ERM program uses general MS Office tools — Excel, PowerPoint, etc., and it meets our current needs.

Q: What are some of the key areas to focus on when preparing an ERM program for a small company (100–150 employees, private company)?
A: DH. Start with the company's strategic goals and objectives, and focus on the high-level risks (both internal and external) that could impact those goals and objectives. Don't get lost in the detail processes. Create a risk universe specific to your company.

Q: What are the factors included in your risk appetite? How do you measure those factors?
A: DH. We tried to define our risk appetite and were not successful. It is a confusing concept to gain consensus on.
CM. We are in the process of developing a risk appetite as a set of qualitative statements related to our core strategic and business objectives.
BJ. We recommend reading the COSO's [Committee of Sponsoring Organizations of the Treadway Commission] *Enterprise Risk Management — Understanding and Communicating Risk Appetite,* published in January 2012, for practical guidance to implement the ERM elements of risk appetite and tolerance.

Q: Can you describe a specific risk the ERM prevented or identified early that would have cost you a loss, i.e., to justify the expense?
A: DH. Years ago, our bad debts started spiking up, and the hospitals starting seeing it first and showed it as a significant risk before it started showing up on the radar at corporate because the accounts had not aged out, and we had a more decentralized process at that time. More focus was put on the accounting and reporting, new policies were put in place to help address the increase, and process changes were made.

Q: What are challenges you still face in keeping ERM sustainable and valuable?
A: DH. We are on our fourth CEO since we started the program. We have been fortunate that all of them have seen value in the program. It must be driven from the top. We try to add something new to what we do every year.

Q: Should compliance be involved in ERM engagements?
A: DH. Not in my opinion, except to be interviewed and provide their input. It is not a compliance activity. If it becomes one, you are in real trouble. It should be strategic.

Q: Would optimal risk council membership be the C-suite or a level below that?
A: DH. I think it would be different for every company. In my opinion, at a minimum I would include the CEO (should chair it and own it), the CFO, the CAE, the head of strategy and the ERM leader. You may want to include operations, and legal should be consulted but not a driver of the ERM process.
CM. An overarching enterprise risk council should be C-suite at the corporate level. If the scope is for a particular function or business unit, the senior leader of that area and their leadership team should be engaged, informed and approve the risk profile and associated work.

Q: Are you performing and presenting the ERM under the direction of general counsel to ensure client/attorney privilege?
A: DH. No, per internal and external legal counsel, that is not really possible. You can try, but they don't believe it would hold up in court.
CM: It is not under general counsel; however, there are many mechanisms to ensure the privacy of information. The office of the general counsel does review all ERM documents — those presented to the ERM executive steering committee and the board of directors.

Visit grantthornton.com to read the article online.