INTERNAL AUDIT: PROMOTING THE VALUE OF ENTERPRISE RISK MANAGEMENT TO MANAGEMENT

By Jay B. Goldberg, MBA, CIA, CFSA

As a Chief Audit Executive or member of the Internal Audit department, you may have been thinking about or incorporating risk management into what you do for many years. Audit plans and programs should be incorporating risk to determine what areas to audit, what to test within each area, and how much to test. In industries like banking and financial services, Enterprise Risk Management (ERM) is second nature. There are Chief Risk Officers, risk committees, risk matrices, heat maps and a committee of the Board of Directors charged with overseeing risk at the company. Yet in many other industries, and in most small companies, there is no formal enterprise risk management process. Given the impact of global events like the accident at the Fukushima nuclear power plant in Japan, the global financial crisis, high unemployment and the risks companies may face because the US Government had its debt rating downgraded, every company should have some sort of ERM process. Knowing that your company needs formal ERM processes in place and knowing that many companies are keeping a tight rein on spending and hiring, how do you convince management to invest the time, resources and funds to properly implement ERM?

We Don't Need ERM Here

If you ask senior executives of companies that don't have a formal ERM process in place why they lack it, they would likely tell you it's because they don't need ERM at the company. If pressed, they might also say that they already understand the major risks within and facing the company and ERM would only tell them things they already know.They might also say ERM is too costly to implement.

Try this test to see if your company needs a formal ERM process. Meet separately with each of the top five or ten executives at the company and ask them to list, in order of importance, the top ten risks they see facing the company (don't let them collaborate). Then ask the Audit Committee members to do the same thing. If you don't get the same ten risks in the roughly the same order from everyone, then your company would benefit from a formal ERM process.

In fact, the differing perspectives on what the key risks are can provide a good starting point for a discussion with senior management and the Audit Committee about why ERM is important and why it is needed in the company.As you probably already know, it is important for everyone to agree on key risks facing the company and then to understand what is being done to address each of them. If management can't agree which risks are the most significant, how can they be in a position to understand them and develop strategies to address them?

The Audit Committee: Your Biggest Ally

If you are a Chief Audit Executive or otherwise have access to the Audit Committee, they can be your biggest ally in the quest to promote ERM to senior management. You should be regularly engaging them in a dialogue about risk. This discussion should include what the company is doing related to evaluating risk, managing risk and defining the risk tolerance for the company. Although they may not be the final decision makers about the company's risk tolerance, by engaging them and encouraging them to have these types of discussions at the Board level and with senior management, they can help drive management to take action and implement an ERM program. Remember, the company doesn't need to have defined its risk tolerance for you to start to implement an ERM program. When the risks and controls have been identified, the residual risk has been evaluated, and the key issues are brought to the Board level, that will drive the discussion about how much risk and in what areas the Board and management are comfortable taking.

Before bringing this issue to the Committee, you should have had a number of discussions with management and management should be aware of your concerns and the fact that you are going to elevate the discussion to the Board level. Explain that you are doing it because you feel it is in the best interest of the Company to have a formal ERM process and that although you have tried to get management to agree, you have not been successful and feel it is a significant risk to the company not to have this process in place. Management can then be prepared to discuss why they don't feel it is necessary.

What is Internal Audit's Role in theRisk Discussion? Well, it Depends…

What role Internal Audit plays in the ERM process depends on two factors:

1) What other functions in the company have the expertise or bandwidth to drive the ERM process, and
2) HowInternal Audit is viewed in the organization.

If the organization has a strong legal or compliance function already in place, they may be able to convince management of the need for ERM and drive, or help drive, the process once management sees the need for it. If neither of these functions is significant or mature, or if these functions are primarily outsourced, it will likely be up to Internal Audit to take the lead. Your success will be greatly enhanced, or inhibited, by how Internal Audit is viewed within the company.

How is Internal Audit Viewed in Your Organization?

In most companies, Internal Audit is viewed in one of four primary ways: compliance/governance focused, operationally focused, consulting focused, or risk management/strategically focused. If the Internal Audit function is viewed as compliance or governance focused, it will be seen as group that performs audits related to compliance with laws, regulations or company policy. This type of function is seen as basic with little value-add to the company. It is typically provided with minimal resources and the areas in which it operates are very narrow. Audit usually brings up issues that have happened after the fact and then provides recommendations in audit reports that are intended to fix issues going forward. Management will bring Audit in to assess the scope of a problem after they have discovered it, but Audit is not seen as a true business partner. If your audit department is viewed this way, it will be very difficult for you to convince management of the need for ERM since you are seen as a tool to "clean up" after the fact.

If the internal audit function is operationally focused, you are probably viewed as more of a business partner. Your department performs reviews of the processes within sales, marketing, and other non-financial areas (as well as financial areas, of course). You look at the efficiency and effectiveness of processes, as well as compliance with laws and company policy. Management is likely to call you in if they think there may be a problem, and let you determine whether there are actually problems and their extent. Being viewed in this way will make it easier for you to convince management of the need for ERM than if you are viewed primarily as a compliance function, but it may be harder for you to show that you can take the lead in developing the ERM process. The internal audit function is viewed as experts in process, but not necessarily experts in business risk. While you are seen to add some value, you may be missing some risks by not thinking strategically or not focusing at all on compliance and governance.

If Audit is a consulting focused function, it is willing to take on any project and the internal audit plan will be changed to accommodate most management requests. While viewed as a complete team player, the audit function is probably not seen as strategic in nature and will react to projects or assignments requested by management. While you may be seen as able to implement ERM, the reactive nature of the department may prevent you from educating management on its value since you may be seen by management as more of a follower than a leader.

Finally, if you are risk management and strategically focused, management sees the department as an asset because you understand the business, bring to light potential emerging risks and think about the company as a whole – not just as departments or functions. In this case, it will be easiest to both obtain buy-in from senior management on the need for ERM, as well as take a leadership role in facilitating its implementation.

Most Internal Audit functions provide a combination of services from several of these four areas. Think about your department. How are you primarily viewed by management and the Audit Committee?If you are primarily seen as a compliance function with some operational knowledge, you should develop ways to move the department to ensure that you participate in

some consulting opportunities, as well as trying to think strategically and point out emerging risks for the company. Incorporate these issues into your next audit plan. You will show management the kind of value internal audit can add, as well as show your leadership skills and make it easier to convince management of the need for ERM, since you will be viewed as knowledgeable on this topic.

There is one more question to consider when determining how easy it will be to convince management of the need for risk management. Would management turn to Internal Audit if there were a problem in the business? Not a problem with controls or segregation of duties or a process that seems inefficient, but something at a very high level that's related to the business. For instance, if the company were considering several strategic directions, would Internal Audit be asked to give an opinion or assessment on the various options? If so, Audit is strategically valued within the company and it should be relatively easy for you to convince management of the need for risk management. If not, you can still do it. It will just take more time and effort.

The First Step to Convincing Management: Think Small

Normally when one thinks about ERM (or any other large scale project) the temptation is to try to make great strides quickly to demonstrate success and show everyone why the project needs to continue. In the case of ERM, although the ultimate goal is for the entire company to participate (hence the name **enterprise** risk management), the short-term goal is to obtain management buy-in and get them to commit resources to the project. Therefore, trying to involve many departments or business units in the beginning is a recipe for failure. Managers will complain they don't have the time or support from their bosses to participate in something that will involve many meetings and a lot of time spent thinking and reviewing documents. After all, they have their regular jobs to do as well. A better approach is to select one area (a department or preferably a business unit) where you have a very good relationship with the senior manager of the area. You will use this area, and the successes that follow, as an example to demonstrate the value of ERM to the senior management.

Educate and Listen

When you first meet with the senior manager over the area you are going to use as a pilot for the program, you may need to educate him/her about what risk management and ERM are. This is a good time to review those definitions. Risk management is a systematic way to identify, categorize and measure the risks in, and facing, a department or company to help ensure that it achieves its business objectives. ERM is a way to do that across the company and ensure that the company understands the risks it is taking, and is taking as much risk at it will tolerate, but no more.

Once the business owner understands what risk management and ERM are, engage him or her in a conversation about the risks facing the department or business unit. What goals and objectives are they trying to achieve this year and in the future? How will success be measured (what are his/her objectives for this year)? What stands in the way of achieving the objectives? What things can be controlled? What things are out of the manager's control? Ask a lot of questions and really listen and take note of the answers.

At this point, explain to the manager that you want to help him/her achieve the objectives but in order to do that, you will need to engage his/her team in a risk management project. Explain that although the manager has identified many risks, you believe that a more complete set of risks, as well as how they can be or are mitigated, will be identified if you get input from a larger group.

Get Other Team Members Involved

With the blessing of the manager, it is time to involve other members of the team. Invite team members at almost every level of management within that area to attend a meeting where you discuss the objectives of defining what risks the department/business unit face; the likelihood, impact and velocity at which each could occur; what controls there are around each risk; and how much risk remains after the controls are factored in. You may need to have multiple introductory meetings if the group will be too large or the geographic or time zone differences make a single meeting logistically challenging.

As an internal audit professional, you may have already gone through this risk assessment process when you put together your audit universe and continue to do it as you update the universe after each audit or annually. You need to engage the department managers in this process and get them thinking about risk. Set up brainstorming sessions asking them to identify risks they see to their business, to achieving their objectives (as a department/division), and to the company as a whole. Most of their initial suggestions will probably be broad in nature (i.e., we might not sell enough product to achieve our sales goals for this year). It will be your job to get them to think both at a higher level and at a more granular level.

For instance, as it relates to the sales goal objective above, get everyone to think about why they might not achieve their sales goal. Do they have the right salespeople? Is there competition from another company and/or product? Is there a lack of innovation in the product? Is there adequate support from the credit department to grant new customers credit to purchase the product? Each of these is a specific risk under the sales goal objective and should be listed.

In addition, you should get them to think about the macro environment. What is happening in the business world that may affect their company? Is credit tight? Are interest rates low? What other things may affect the company and its ability to grow or its customers and their ability to purchase the product? Although this information will be used later, after senior management

has bought into the idea of ERM, it is important to try to gather the information now so that you don't have to repeat these sessions with this group.

Share the Internal Audit Risk Assessment

Once the group has come up with all the risks they can think of, make sure you share the internal audit risk assessment with them. Also share the list of risks you obtained through your discussion with the head of the division/business unit. In addition to making the internal audit process more transparent to them, they will gain valuable insight into what the head of their unit thinks. If the business unit leader is a good communicator, the list of goals, objectives and risks should come as no surprise. Usually it will be the basis of further discussion in the group and lead to a more complete understanding of what the business unit is trying to accomplish. It will also provide you with better insight into the accuracy of the risk assessment in your audit universe.

Risks: Likelihood, Impact and Velocity

Next you need to gain consensus for the likelihood, impact and velocity of each of those risks. How likely is it that this risk will occur? I have always used a rating of low, medium or high, although others like to rate using a 5 or 10 point scale. For impact, you need to determine what impact the risk would have on your business if it occurred. There are two pieces to this – quantitative and qualitative impact.

The easiest way is to assess the quantitative impact on the business unit is to assign a dollar value to it and, based on that amount, rank it as low, medium or high. Determine at what threshold, based on the size of your business, the impact goes from low to medium and medium to high. For instance, in a company or division that has only $2 million in sales, a reduction (or increase) in sales of $100,000 may be considered a medium impact event if it were to occur but in an organization of $50 million in sales, it would be a low impact event.

Because not all risks have a significant quantitative impact associated with it, you also need to consider the more subjective qualitative impact. Consider a situation where a web server is taken down by a virus and sales or customer data is compromised. It may not be too costly or take too much time to rebuild and restore the server and its data, but what is the impact on the company if that data is obtained by competitors? How would it impact the company's reputation if the media became aware of this breach? These are the types of qualitative impact that need to be considered and evaluated.

Finally, determine how quickly each event can become a reality (velocity). The faster something can occur, the more inherently risky it is because it is harder to forecast or foresee if it can occur quickly.

To most effectively determine likelihood, impact and velocity, I recommend getting a small group (3-5 people) together and working through each risk and coming to a consensus on these three attributes for each risk. Alternatively, you could have three to five people go through this exercise individually and then bring the group together to discuss the results and come to consensus (or a range where a consensus cannot be reached).

Once the group has reached a consensus, share the information with the larger group and invite everyone to comment or provide feedback to you. If the larger group has consistent comments, discuss them with the smaller group (3-5 people) and make changes as appropriate.

Identify Controls That Mitigate Risks

Now that you have a list of risks and agreement on the likelihood, impact and velocity of each, you need to look at the company and determine what controls you have in place that could mitigate those risks (the same way you would do for an audit). These controls might actually reduce the likelihood that the risk will occur, or it could also be an early warning indicator that a risk might be coming and that its likelihood or velocity is increasing.

Although you could assemble a small or large group of people to identify and evaluate the controls that are in place and how much they mitigate the risks, a better approach is for the Internal Audit department to attempt to initially list the controls and how much they mitigate risk. After all, Internal Audit should be the risk and control expert in the company. You probably already have a listing of controls, by area, and have also determined how effective each is. Using that information, and combining it with the list of risks, Internal Audit should be able to add controls and determine how much they mitigate the risk. Finally, the assessment process should attempt to estimate how much residual risk is left, after factoring in the controls and their effectiveness for each risk.

After Internal Audit has completed the draft, it too should be circulated to a smaller or larger group for feedback and agreement.

Aggregate Risks

Once you have the complete listing of risks and controls that mitigate them, you should go through the process of aggregation. You will probably have a list of over 100 risks and that list will only grow as you add other departments/business units into the process later. Examine the risks and try to group them by common themes or areas (i.e., risks to sales, cash and reputation). What you are trying to do is reduce the list of risks from the hundreds to maybe 50-100 categories, or groups of risks. With this smaller list, you can review the categories for trends and focus on the 10-20 themes that seem to have the most risk or are the most prevalent. These are the key ones you want to discuss with management and ensure that they have strategies in place to mitigate them.

Sometimes aggregation is more easily accomplished using a framework. A framework provides areas in which to put risks and can assist you in evaluating how many there are of each type. There are many frameworks out there and this, like the whole ERM implementation process, is not a "one size fits all." You should speak to other audit professionals, as well as industry experts, about what risk frameworks they can provide and use the one that best suits your company and approach.

Once the risks have been aggregated, the document including the key risks, their related controls, and the residual risk, is ready to be presented and discussed with the senior manager over the area (the one you met with to kick off the project).

Discussion with Senior Management

When you present the informationto the senior manager over the area, explain that because of his/her support and the collaboration from the team, both the process and the outcome was much more complete and accurate than if it was just developed by the Internal Audit Department or just one or two people from the area. Point out specific areas where the collaboration was helpful and discuss why it was so critical to get his/her support.

I am sure he/she will be surprised at how high the residual risk is in some areas. He/she may also be surprised that there is very little risk in others and feel that the department should be taking more risk. This is a good time for two discussions: How much risk is the manager comfortable taking (based on guidance from other senior managers and/or from the Board) and how can the company go about taking more risk in some areas? Discuss ways that some of the excessive risk can be mitigated (add additional controls to reduce it or transfer the risk to another party). He/she should be very pleased with the assessment and will have a better understanding of the risks in the department/business unit. The senior manager should also have a better understanding of where the department might be at risk for not achieving their objectives and what can be done to increase the likelihood of success. Once you have this senior manager's buy-in to the value of the ERM process, it will be much easier to get the rest of the management team to agree that it is worth investing in rolling it out company-wide.

Summary

Trying to convince management of the need for an ERM process at a company can be difficult. They may feel that they have risk management under control and that they know all of the important risks facing the company. While this may be true for the more obvious risks, it is the less obvious risks that management also needs to be aware of and needs to consider as the business moves forward.

As an internal audit professional, you are in a unique position to be able to facilitate an ERM process by starting with one business unit and demonstrating how a more collaborative and

broader effort can uncover less obvious risks which may put the company, and/or some of its business objectives, at risk. Through the process you may also show that while management is knowledgeable of many of the risks, they may have underestimated the how large the impact of these risks could be or the speed at which these risks could move from highly unlikely, to unlikely, to very likely, to actually occurring. You should also engage the Audit Committee and make sure it is comfortable with the risk level the company is taking and the areas in which it is taking those risks.

While most Boards of Directors and management are concerned if they are taking too much risk, they should be equally concerned if they are not taking enough. They may be missing out on ways to take additional risk within the company's risk tolerance and grow the business (or increase profitability). However, without knowing the level of risk the company is currently taking in each area, and without a defined risk tolerance for the company, it is impossible to know what risks or opportunities the company is inadvertently taking or missing out on.

Finally, make sure your Internal Audit Department is viewed in such a way that you can easily and successfully demonstrate the value of ERM to management and the Audit Committee.

Jay Goldberg is an internal audit, risk management and governance executive with more than 20 years of experience. He has launched and led the internal audit function at several publicly-traded companies in industries including software, media and entertainment, insurance, transportation and logistics. He can be reached at jaygoldberg@optonline.net.

About Cura Software

Hundreds of organizations worldwide rely on Cura Software to make Governance, Risk and Compliance Management more effective and efficient. Cura Software combines powerful technology with unparalleled domain expertise to help its customers comply with industry regulations, optimize risk management and gain better visibility into business operations.For more information, or to schedule a live demonstration, visit www.curasoftware.com.