



How to Get Started with Enterprise Risk Management

Enterprise Risk Management is a practice that has been around for decades, tracing its roots all the way back to the early 1970s. It garnered much attention in the early 2000s when the New York Stock Exchange required all of its listed companies to mandate their Audit Committees to “discuss policies with respect to risk assessment and management” and stated that “it is the job of the CEO and senior management to assess and manage the company’s exposure to risk.”¹ Since then, many risk management frameworks and standards have been published, including COSO’s Enterprise Risk Management – Integrated Framework in 2004 and ISO 3100 Principles and Guidelines on the Implementation of Risk Management in 2009. In light of these recent developments and the global economic environment, more companies are focused on implementing and further developing their risk management programs than ever. In the PricewaterhouseCoopers 13th Annual Global CEO Survey, published in January 2010, 82% of CEOs stated that they were making some changes or major changes to their approach for managing risk.²

* 1 NYSE Rulemaking: Securities and Exchange Commission. 11 April 2003. Release No. 34-47672; File No. SR-NYSE-2002-33. <http://www.sec.gov/rules/sro/34-47672.htm>.

* 2 PricewaterhouseCoopers. 13th Annual Global CEO Survey. January 2010. <http://www.pwc.com/gx/en/ceo-survey/data-smarter-growth.jhtml>.



The Security Division of EMC

Getting Started

A lot of companies want to make changes and enhance the maturity of their risk management initiatives but don't know what steps to take. In my conversations with senior managers for organizations across multiple industries, I frequently hear that they are being looked upon by executive management to deliver an efficient and effective risk management program and don't know where to start. Many understand the principles behind the leading methodologies and frameworks but don't have the resources or the knowledge to put together a program. From working in risk management over the past 15 years and witnessing both successes and struggles at many organizations, I submit the following tactical plan for establishing a risk management program that is quick to return significant value.

The basic premise of risk management boils down to three steps: identify, evaluate and respond. Let's consider each of these processes as I answer five top questions about how to start a risk management program.

How Do I Know What My Risks Are?

The first step in building any risk management program is to gather a list of your risks. The most important thing to remember when creating the list is that you can't be afraid to start small. I too often see cases in which companies won't publish a risk register because it is not all-inclusive. The list can and will grow, and you will never be able to get a risk management program off the ground unless you start somewhere.

There are two basic approaches for aggregating a risk inventory: top-down and bottom-up. The top-down approach involves understanding what the company's objectives are and thinking about what could threaten the achievement of those objectives. Company objectives can typically be picked out of board presentations, strategy documents, financial analyst calls, product roadmaps, etc. Once this information is collected, it is fairly easy (although rather depressing) to think of what could stand in the way of accomplishing those goals. Examples could be macro factors such as the economy, population migration patterns and the availability of new technologies, along with micro factors like competition, human resource availability and speed to market.

The bottom-up approach involves getting input from your colleagues. No one person in any mid- to large-sized company, including the CEO, can have a holistic view of the company's risk profile. There are too many things happening on a daily basis for anyone to have their finger on all the activities.

Thus, it is wise to survey employees to find out what risks they encounter on a daily basis. It is difficult for some people to think about risk, so ask questions like these:

- What keeps you up at night?
- What would prevent you from achieving your annual goals?
- What would prevent the company from succeeding?

Gathering the responses will enable you to populate the risk register, and the re-emerging themes will begin to help you answer the next question.

How Should I Prioritize My Risks?

Now that you have accumulated a list of risks to the company, you must figure out which ones to worry about. No one has the resources to tackle all their risks, nor is it possible to fully mitigate all risks, so you must prioritize them. This is done through risk evaluation and determination of inherent risk. Like anything, prioritization can be accomplished only via normalization and rationalization. You must ensure that everything is measured on a level playing field. Risk evaluation also enables you to support making tradeoffs when allocating resources for risk mitigation.

Typical inherent risk evaluation involves analyzing the impact the risk could potentially have on your company and the likelihood or probability it will occur. This may seem very daunting, and some companies get bogged down in the details of risk evaluation. However, always keep the end in mind—the purpose of the exercise is to rank the risks so you know where to spend your time and money when you have the ability to mitigate the risks.

Here are some important considerations to keep in mind when evaluating risk impact and likelihood:

- **Pick a Scale:** You can't prioritize risks if you don't evaluate them using a common scale. I like to recommend low, medium and high as this scale is easy to use and requires no explanation. As your risk management program matures and you increase the number of risks you evaluate, you can use a five- or seven-point scale to stratify the risks more.
- **Pick an Evaluation Method:** You can evaluate impact and likelihood using qualitative or quantitative methods. Qualitative evaluation is when an analyst rates the impact and likelihood manually based on subjective justification. Quantitative evaluation is automated based on calculations of supporting data. For example, let's assume you are trying to evaluate the likelihood of data breaches in a data center. Qualitative evaluation would include an analyst indicating the risk is medium since the data center has

had a breach before but it only happens once every few years. Quantitative evaluation could be performed by the analyst gathering the data of all transactions occurring in the data center over the past five years and calculating the rate at which a data breach occurs. If the rate is less than 1%, the likelihood would be low. If between 1% and 10%, the likelihood would be medium, and if over 10%, it would be high. Quantitative analysis is typically more precise but also requires more time and explanation. Thus, I recommend using qualitative methods first and switching to quantitative methods as you mature.

Once you have objectively rated the impact and likelihood of your risks, you multiply the two factors to determine the inherent risk. Most companies like to chart their risks on a heat map (Figure 1), which provides a nice visualization of their risk profile. I also recommend charting risks by function, business unit, category, etc. so you can start to understand what parts of the business require most of your attention. Once you have a prioritized list of risks, you are able to move on to the third question.

Impact	H	3	5	1
	M	1	2	0
	L	3	4	3
		L	M	H
		Likelihood		

Figure 1: Sample Risk Heat Map

What Should I Do About the High-Priority Risks?

It's now time to get more people involved and coordinate work streams to understand the potential for mitigating the highest priority risks. The number of risks you tackle depends on your resource availability. This is an ongoing effort and should be built into the normal course of business for all management.

Risk response typically comes in four flavors: reduce, transfer, share and avoid. The most important part of risk response is tracking and measuring progress. It is vital to define a risk response plan for each high priority risk and then track progress against achieving the plan. In addition, you need to measure the progress by determining the residual risk level. Residual risk starts with the inherent risk and reduces it by the impact of the response. Fully transferring or avoiding a risk may take a high inherent risk item to a low level. Sharing or reducing the risk may only limit that high risk item to a medium level. The measurement of residual risk will enable you to answer the fourth question.

How Can I Show Value from This Process?

All executives love squeezing value out of any process they can. Risk management is not exempt. As a risk manager, you will be asked to show value for the investment made in indentifying, evaluating and responding to your risk inventory. Fortunately, showing value is easy. During the course of this process, you have accumulated a wealth of data that you can mine and report on. Bringing visibility to the information is a key to demonstrating value. Dashboards and metrics are powerful concepts that are common in sales, marketing and other departments. Risk management should be no different.

Also, engaging others will increase value. You can get everyone to buy into risk management by enabling ownership of their own risks and promoting visibility and transparency of all the data. I have never seen one report produce more action than one that shows inherent vs. residual risk by business unit. No one wants to be the person with the least delta between inherent and residual risk. Pitting people against each other may seem cruel, but it is a great motivator.

As we've seen, the value of engaging others and building dynamic, real-time dashboards is clear. However, these activities can be daunting without the use of a tool. This brings me to the final question.

What Should I Do About the High-Priority Risks?

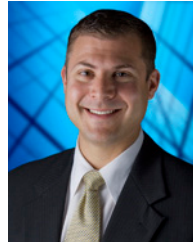
A tool is an absolute necessity when implementing a risk management program. There is no possible way to gather, analyze and report on all this data without some technology assistance. However, there are many tools, including Excel, GRC platforms like RSA Archer and point ERM solutions. Excel is a common choice as it is considered "free" to most users and requires no training. However, I would ask you to consider the following top requirements for selecting a risk management tool:

- **Ease of Implementation:** You need a system with best-practice processes built in so you can hit the ground running. Excel requires you to define the process and then configure the spreadsheet. RSA Archer and most point solutions offer a pre-configured process based on the COSO ERM Framework.
- **Ease of Use:** What good is a tool if no one is going to use it? User adoption is key to making the program successful. Excel has strengths in this category, but a flexible platform like RSA Archer provides a total user experience with user-specific dashboards, notifications and in-line help. Some point solutions do not focus on the user interface and end-user experience.

- **Ability to Correlate Data:** You will be handling lots of data in the risk management process, and you will need to leverage a tool that is proficient at gathering and correlating data. Unfortunately, you can't send out surveys to all company employees in Excel and automatically roll up the results. RSA Archer and some point solutions have built-in questionnaire capabilities.
- **Transparency:** You want to encourage participation in the process by making all the data available on a real-time basis. Excel does not have the ability to share data real-time with users, while that is the core competency of RSA Archer and most point solutions.
- **Reporting:** You will need to slice and dice the data in your risk program quickly and easily. Excel will enable you to do this with a bit of work if you know pivot tables, macros and charts. Most point solutions have many canned reports but do not provide the ability to easily create ad hoc reports. RSA Archer has user-friendly search capabilities that put the power of reporting in the hands of users, not just the process owner. Giving end users the ability to build reports will increase their engagement in the process.
- **Flexibility to Grow:** Your needs will change as your process matures. You will need to change your evaluation scale and methods as well as track new attributes and hierarchies. You will need a tool that offers the flexibility to modify the configuration quickly and without any coding. Of course, you will be able to do that in Excel. The RSA Archer Risk Management solution is built on the RSA Archer eGRC Platform, which enables drag-and-drop configuration of the risk management process. Most point solutions cannot be customized, or they require custom code to make modifications.

I hope these thoughts have helped you define the tactical steps to building a risk management program in your own company. One final consideration that cannot be ignored is the maintenance of the program. I often see companies going through the identification and evaluation process once and not updating the information thereafter. The information in your risk register will quickly become stale as your company changes and the world around it evolves. Thus, you need to re-identify and re-evaluate your risk profile on a quarterly or semi-annual basis. This will enable you to continuously provide value back to your company and assist in the achievement of its objectives.

About the Author



As Director of eGRC Solutions for RSA, The Security Division of EMC, David Walter leads the vision for the RSA Archer eGRC Suite. He is a CPA with core competence in finance and compliance, and he formerly served a diverse set of public and private companies, with roles including director of internal audit, CFO and vice president of finance.

Mr. Walter is an RSA Archer Certified Consultant and an expert in creating risk and compliance solutions built on the RSA Archer eGRC Platform.



The Security Division of EMC

www.rsa.com

©2010 EMC Corporation. All rights reserved.
EMC, RSA and (see list) are registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.

RSKPG IB 1010