

# **SO WHATEVER HAPPENED TO ENTERPRISE RISK MANAGEMENT ANYWAY?**

## **Regaining momentum in Enterprise Risk Management Programs**

**Sponsored by CFO.COM**

[www.cfo.com/whitepapers](http://www.cfo.com/whitepapers)

*The Top Down Group*



One of the biggest expected benefits as a by-product of companies' compliance with Section 404 of the Sarbanes Oxley Act of 2002 was the development of a formal Enterprise Risk Management program. ERM programs were going to measure the risks and inefficiencies across a company's entire operation, identify weaknesses and redundancies entity wide, and ultimately develop real solutions, including performance of regular operational efficiency audits designed to present findings and recommendations designed to reduce risk and eliminate inefficiencies.

But something funny happened along the way to building a top notch enterprise risk assessment process at many mid-sized companies: Nothing.

In reality, many mid-sized companies started the risk assessment process, drafted a narrative of the risks identified at a company, but other than obtaining a cursory review of the narrative by members of senior management and the audit committee, and perhaps having performing a few low risk operational audits, little if any enterprise risk management programs were ever fully developed at many mid-sized companies.

Achieving a fully integrated risk management program requires a deliberate strategy, willful execution, continuous monitoring, and a culture of responsiveness. In many cases the process started, and then simply stalled out. Executives know risk management is critical to a successful operation, but in many cases are having a difficult time restarting the program.

Why did this happen? Is there still time to fix it? And what's the best way to re-energize the program at the best value?

This whitepaper will explore some reasons why enterprise risk management may have stalled out at some companies, what can be done about it, how to go about developing a risk assessment program, and why it benefits a company to ultimately implement and utilize an enterprise risk management program for their operations.

## **We got our SOX to fit. You mean there's more?**

After initially implementing SOX 404 compliance initiatives then refining the program in subsequent years with the idea that they would begin development of a full Enterprise Risk Management program, mid-sized companies instead began to view the SOX compliance process as their own risk assessment program in and of itself.

And why not? SOX compliance was supposed to highlight the key risks and the related controls at a company and assess the effectiveness of these controls. Plus, SOX compliance was costly to implement and time consuming to perform. How much more time and resources was a company supposed to devote to evaluating its risk? Wasn't becoming compliant with Sarbanes Oxley enough?

Well, if one considers that SOX 404 was designed only to identify and assess the risks and controls surrounding internal controls over *financial reporting*, it becomes apparent that risks and inefficiencies surrounding corporate governance, information dissemination



and basic day to day operations are barely considered and rarely evaluated as part of a SOX compliance program.

Enterprise Risk Management typically involves identifying processes, events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, implementing measures to mitigate these risks and achieve these objectives, and monitoring their progress.

Thus, while SOX may be relatively deep (getting into the real details of controls surrounding the preparation and reporting of financial results) it is not very wide, meaning its scope, as noted is relatively limited and a company, if wants to truly assess and monitor *all* the key risks in its operations, needs to do more. But what?

## **I paid \$20,000 and all I got was a report?**

Once companies realized that there was more that they could be doing to monitor risk in their operations, they often utilized an external (and often expensive) consultant to prepare a formal risk assessment report and develop a corresponding ERM program.

The resulting report described, (often in considerable detail) the key functions and operations of a company, based on interviews conducted with key personnel, and usually recommended that further operational audits be performed (at an additional expense) to enable a more in-depth assessment of the key risks and inefficiencies identified. Risk assessment reports sometimes provided basic overview recommendations on how to monitor risks or eliminate inefficiencies, but more often than not these recommendations stopped at the summary level, without a detailed plan for implementation.

In other cases, the risk assessment program was initiated, a report was drafted and reviewed by senior management and the audit committee, and then ultimately was filed away and never seen again. So no follow up work or implementation of an enterprise risk management program was ever really completed. And more often than not this is the state of many mid-sized companies' ERM programs today.

## **What else could have been done?**

One of the biggest flaws in many risk assessment processes is relying on mostly qualitative (written) assessments, usually without the benefit of any corresponding quantitative (numerical) analysis. Essentially, the consultant notes observations and opinions about a process, based on interviews conducted with employees and they're own intuition, but may not compare it to other processes in the company with regard to its relative importance in operations and rarely, if ever, ranks it alongside those other processes as far as overall risk to operations.

Some additional quantitative risks that could be included as parts of a risk assessment are: What is the materiality of the process on the balance sheet? What are the expectations placed on employees involved in the process? How much pressure is there to perform? What is the level of inputs and outputs of the process?



And the reports were often only as good as the writing ability of the consultant itself. There was no easy-to-implement, easy-to-replicate methodology of measuring risk along predetermined criteria. So what could have been done differently?

A scoring system, with a listing of all the key functions and locations assessed could be seamlessly integrated along with the narrative report. The scoring system may look like this:

**Weight (importance of the process) x Risk level = Overall Risk Rating**

Standard methodology is as follows: Weights are assigned to each risk factor with 1 the lowest and 10 the highest based on the relative likelihood that the risk factor will affect the process or site being assessed. The assignment of weights is based on professional judgment, experience, and management's observations. Finally, a risk level is assigned to each risk factor with 1 the lowest and 3 the highest based on the likelihood that the determined risk factor will affect the specific process or site.

The risk level is multiplied with the weight factor for each determined risk factor and the amounts are added together to arrive at a final risk assessment for each area. A process with an overall risk level of 130 or below is considered to be acceptable or low risk. Processes scoring from between 131 and 210 are considered to be medium risk and should be examined more thoroughly, and processes scoring over 210 are considered to be high risk and should be addressed as soon as possible.

Finally, the risk assessment is then drafted, in narrative form, and released for review and comment by each of the interviewees, along with senior management. The narrative gives the reader a summary of the process being reviewed, the risk rating it received and recommended focus areas to be reviewed as part of an operational audit.

Documentation for SOX 404 should be leveraged to provide a significant portion of the narrative; however, the focus and conclusion would be more aligned to the evaluation of risk on an overall basis, and not just around risks surrounding financial reporting. And the scoring matrix can be easily updated as people, processes and circumstances change, making the risk assessment a live, working document.

An example of such a scoring system for a few select processes is provided below (please note that this is not inclusive of all processes normally measured as part of a risk assessment):



**Corporate  
Risk Analysis Summary**

	<b>Weight</b>	<b>Corporate Governance</b>			<b>Finance and Accounting</b>			<b>Legal and Contract Administration</b>		
		<b>Risk</b>			<b>Risk</b>			<b>Risk</b>		
		<b>Level</b>	<b>Points</b>	<b>Total</b>	<b>Level</b>	<b>Points</b>	<b>Total</b>	<b>Level</b>	<b>Points</b>	<b>Total</b>
<b>Business Environment:</b>										
1. Management team	8	2	16	2	16	1	8			
2. Strategic planning impact	6	3	18	3	18	3	18			
3. Risk evaluation	5	2	10	2	10	1	5			
4. Pressure to perform	3	2	6	3	9	1	3			
5. Employees experience/knowledge/training	3	2	6	3	9	1	3			
6. Reputation Risk	3	3	9	3	9	3	9			
	<b>28</b>									
			<b>65</b>			<b>71</b>				<b>46</b>
<b>Financial &amp; Operating Environment:</b>										
7. Materiality to Balance Sheet	5	1	5	3	15	2	10			
8. Materiality to Income Sheet	5	1	5	3	15	2	10			
9. Susceptibility to misappropriation, fraud or loss	5	1	5	3	15	1	5			
10. Completeness/adequacy of management reporting	5	1	5	1	5	1	5			
11. Effectiveness of controls (internal/external reports)	6	1	6	1	6	1	6			
12. Strategic volatility, Rate of tactical change	6	2	12	3	18	1	6			
13. Stability of transaction flow/Average transaction volume	4	1	4	2	8	2	8			
14. Complexity of operation/product	5	3	15	2	10	3	15			
15. Information Technology effectiveness/control	7	1	7	2	14	1	7			
	<b>48</b>									
			<b>64</b>			<b>106</b>				<b>72</b>
<b>Governance, Internal Control and Compliance</b>										
16. Corporate Governance/SOX Compliance	6	1	6	1	6	1	6			
17. Internal control environment	6	1	6	2	12	2	12			
18. Documentation of internal controls	6	1	6	2	12	1	6			
19. Compliance with laws and regulations	6	2	12	3	18	3	18			
	<b>24</b>									
			<b>30</b>			<b>48</b>				<b>42</b>
<b>Total Risk Score</b>	<b>100</b>		<b>159</b>			<b>225</b>				<b>160</b>

## Where do we go from here?

If a risk assessment has not yet been performed at your company, you should start the process immediately. It should be some combination of written narrative, along with some quantification of risk as noted above. A proper risk assessment, used to identify, monitor and mitigate potential risk and exposure at a company, assess and improve efficiency in operations, and assist with the prioritization of capital and personnel resources, is a valuable tool for executives to gauge the operations of their company.



A way to make the process even more efficient is to start the process during the walkthroughs usually performed as part of the SOX 404 compliance process, as least for the processes covered by SOX. To gaining an understanding of the governance and operations, interviews should be conducted by the person or persons performing the risk assessment, and quantitative risks should be measured as part of the process and updated accordingly.

Finding and recommendations should be included as part of the report, and an internal “champion” of the process should be identified early on, an individual or group responsible for overseeing preparation of the report and following up on implementation of its recommendations in a timely fashion.

If a risk assessment has already been performed, it is critical that some of its recommendations be incorporated into operations immediately. Institute a more quantitative grading system, which can be updated much more easily than a qualitative report, and begin to act of monitoring the key risks identified in the report. Too much is at stake for corporations to ignore the critical risks to their operations any longer.

## Summary

Risk Assessment, often referred to as Enterprise Risk Management, is used to identify, monitor and mitigate potential risk and exposure at a company, assess and improve efficiency in operations, and assist with the prioritization of capital and personnel resources.

Significant sites are identified, along with key processes and key personnel. Interviews are conducted with the key employees at the sites to evaluate, determine and assess the level of risk, the operational efficiency and the critical procedures of their site/ process. Management observations of existing operations and most pressing concerns are strongly considered when preparing the Risk Assessment.

Enterprise Risk Management gained significant momentum a few years ago with the implementation of SOX 404 compliance programs, but an effective risk assessment program was rarely developed beyond a rudimentary stage at many mid-sized companies who often lacked the resources. While a draft version of a risk assessment may have been prepared in many cases, it was often qualitative in nature and often subject to the opinions of select personnel. Many risk assessments were drafted, reviewed and revised, but never really followed up upon again and the program simply stalled out.

By incorporating a quantitative risk grading system, which can complement a written report and enable easy development of a formal ERM program, companies are able to easily assess and evaluate the critical operations of their business and proactively implement measures to mitigate risk or eliminate inefficiencies in operations.

An effective risk management program must be driven by senior management and the board, and must be embraced by the entire organization, but the ultimate benefits will be well worth the initial investment for your company.



## The Top Down Group

The Top Down group offers a full suite of internal audit and SOX 404 solutions for your company. We want our clients to view us as a business partner, not just a service provider. Our clients should see real value in Sarbanes Oxley compliance and internal audit services, focused on identifying and monitoring the key risks to their operations.

The Top Down Group is a leader in providing value added lower cost internal audit and SOX 404 compliance services to small and mid-sized public companies. We provide a proven, right sized SOX compliance program for our clients which allows for customization and scalability. We deliver maximum efficiency SOX solutions at a fair price, allowing them focus more on running the business and less on compliance issues.

We specialize in right-sizing SOX for each client, making sure the benefits of sound internal controls outweigh the costs and effort. SOX compliance doesn't have to be complicated, or expensive.

At the Top Down Group, we will:

- Develop a SOX and internal audit plan just right for your company.
- Look for ways to reduce costs, eliminate redundancies and create efficiencies in your operations.
- Understand your business, processes and controls to create a SOX or audit program to fit your needs and budget.
- Guide you step by step on documenting, testing and assessing your control environment to ensure a repeatable, efficient process, year after year.
- Deliver partner level service at staff level rates.

This document is provided by the Top Down Group for educational and information purposes only and is not intended and should not be construed as legal advice.

*The Top Down Group*



*Experts at getting your SOX to fit*