Syntex
www.syntexsolutions.com

Implementing Enterprise-wide Risk Reduction Across Operational and Financial Processes

Trent Derr
Syntex Management Systems Inc.
Global Leaders in Operational & Enterprise Risk Management

Today's World of Risk

As we look into the economic abyss that was created in the aftermath of the stock market dive in late 2008 and early 2009, it's pretty easy to realize that risk management is a vital core competency in any ongoing business. However, what isn't as easy to identify is that scope of business processes impacted by Risk Management is changing rather dramatically. Risk management is becoming much more than compliance, internal controls, audits, incident management and insurance. In today's sense, risk management is any organized activity designed to reduce the uncertainty of a company achieving its operational objectives. Thus a potential risk is created by any exception or deviation in a process that could impact a company's ability to meet its goals. Given that broader view of risk, it's more apparent why strictly staying in compliance, having good internal controls and buying enough insurance coverage are no longer sufficient.

The signs of the resurgence in risk management activity are everywhere. In a recent study by Towers Perrin, "Senior Finance Executives on the Current Financial Turmoil", 72% of the CFO's stated that they were concerned about their Risk Management practices. Even more recently, the U.S. Congress is considering further refining corporate governance beyond the current requirements of Sarbanes-Oxley. Under consideration is a requirement for the Board of Directors of publicly held companies to appoint special committees to oversee risk management. It seems likely that these new Risk Management Committees could have similar fines and penalties apply to them for being "out of compliance" as executives currently have under Sarbanes Oxley. In the Seventh Annual PriceWaterhouseCoopers study "What Directors Think", only 50% of the Directors felt the Board they were on was effective in managing risk. Given the potential requirement for a new Board level Risk Management Committee and a current confidence factor of only 50%, you can almost hear the simultaneous puckering up of Corporate Board Members. And we thought it was difficult to locate qualified Board Members before all of this.

On another front the two major credit rating agencies, S&P and Moody's, are putting more weight on a company's Enterprise Risk Management (ERM) practices when determining an organization's overall rating. In taking a more holistic view of a company's future performance and the resulting impact on earnings and capital, it makes sense to include along side the traditional financial measures those business practices that impact the strategic, operational, and other non-financial domains of risk. Practices around the management of strategic and operational risks represent a way to reduce the degree of variability in a company's future earnings and capital needs. Thus the variation in operational performance between similar companies can partially be explained by the differences in their Enterprise Risk Management practices.

That is one reason why it seems very likely that a Risk Scoring system will be developed by the analysts who evaluate companies from an investment and debt perspective. This Risk Score will very likely be similar to the FICO score you and I have as a measure of our credit worthiness. However the Risk Score for a corporation will include the key factors that are correlated with operational excellence (like process integrity, leadership commitment, risk culture, etc.). With that approach, those companies with better Risk Scores are highly likely to have lower variability and volatility in their operations – and thus more predictable earnings and capital projections. In the end, strong Enterprise Risk

Management helps create fewer operational and earnings “surprises”. Before Sarbanes Oxley, some companies would financially manage their earnings and performance results to be more in line with expectations. With more structure in place as a result of Sarbanes Oxley, the best way to ensure performance meets projections is to have reliable operational results driven by predictable operational processes. This is the core benefit of the continuous process improvement created by strong enterprise-wide Risk Management practices. Through this Risk Score, analysts and the public at large will be better able to benchmark the risk exposure that exists between peers and across industries. Independent of whether a Risk Score becomes mainstream or not, the Enterprise Risk Management assessment being performed by S&P and Moody’s will ultimately impact a company’s cost of capital.

It’s no wonder that risk management is under the microscope. The practice of risk management in many companies is quite challenged. Many companies approach risk management as a compliance function rather than an opportunity to improve operations. Thus they focus on avoiding penalties and fines rather than those steps that will actually improve processes. Also risk management is typically managed with disparate systems, spreadsheets, and piles of paper that exist in their own process silos (i.e. SOX, Environmental, Credit, Trading, Safety, etc). Even the risk management processes being used aren’t standardized across the various domains of a company. So there is no single source of the truth where anyone can determine the organization’s actual risk profile and identify its current highest exposures. In addition, too many companies still focus on lagging indicators like losses, claims and incidents. It’s too late once those consequences have already occurred. These actual loss events are only the tip of the iceberg with the vast majority of the unrealized exposures still lying below the surface of the water. Finally, typically only a few people are “responsible” for risk management, and thus, risk management really doesn’t become imbedded in the culture as a part of everyone’s job.

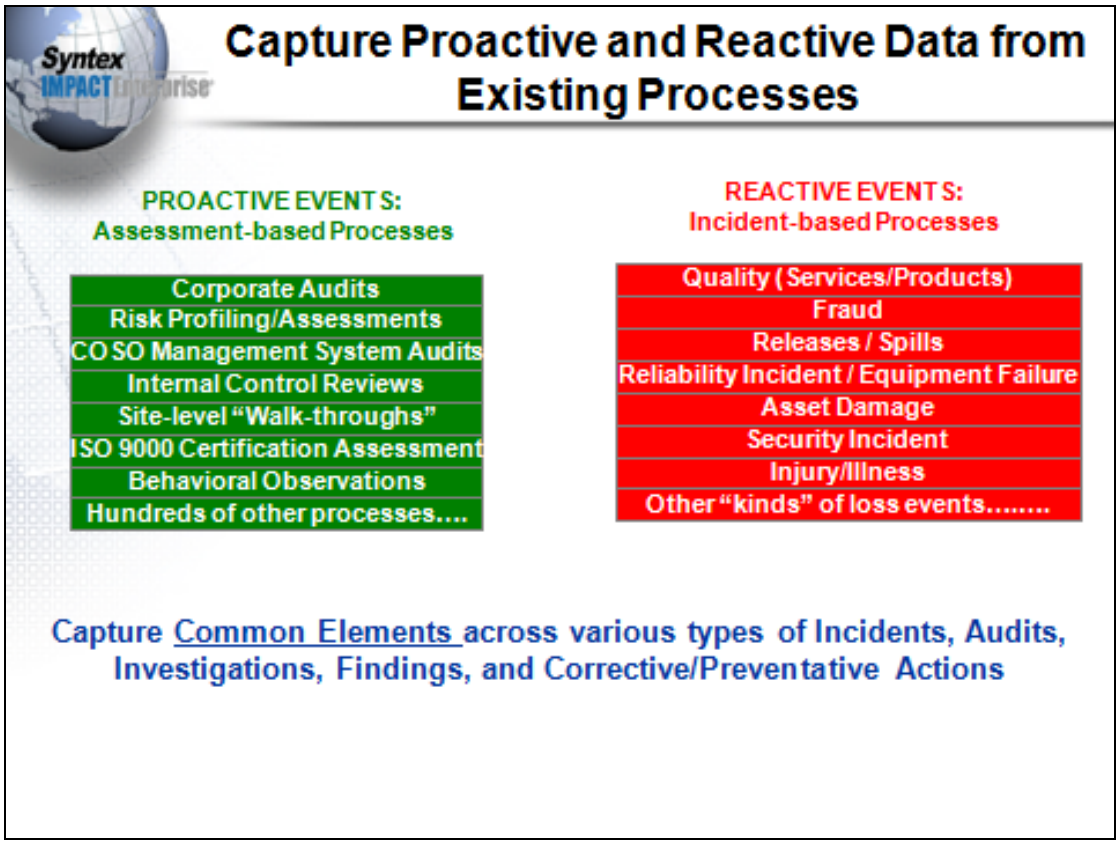
Shifting the Mindset Regarding Risk Management

So how do we overcome these challenges? The key is for management to believe that Risk Management should address any deviation in a process that threatens the company’s ability to achieve its objectives. This represents a shift to view Risk Management as a continuous improvement process focused on risk reduction. There are several advantages of addressing risk through continuous process improvement. Once a company has a continuous improvement culture in place, it will be better positioned to address whatever regulatory compliance or new risk management needs develop. Also the scope of the processes to be managed can span any risk domain including strategic, operational integrity, financial, asset integrity, environmental, health, safety, quality, security, and reputation. The desired outcome of a fully integrated Risk Management process is to reduce the variability in process execution which ultimately produces more predictable financial and operational results for the entire organization.

One piece of good news is you can start this journey by leveraging your existing systems and processes. The first step is to aggregate a single repository of risk data by consolidating the risk process information from your existing financial, operational and risk systems. Within each risk process domain, you’ll be able to identify similar data that is captured when an event is reported (a loss or audit finding), when the potential risk is assessed, when root cause is analyzed, when a process correction is implemented, and when best practices are shared. For a complete risk picture, it is important to capture data from both reactive events (incident based processes) and proactive events

(audit/assessment based processes). This consolidated process data will be needed to assess a company's actual risk profile. As a subsequent step, the company needs to establish a single integrated Action Item System across all the risk process domains to address both preventative and corrective actions. Having a closed loop Action Item System will aid in the visibility and accountability by ensuring that the proper mitigating actions are actually implemented in a timely manner.

As a starting point to leverage the common Risk Data Repository and the integrated Action Item System, it is ideal to start the implementation with a functional area of the company with the most management support and an identified risk reduction objective. With some early adopters on board, you'll have more internal supporters and lessons learned under your belt before you tackle the more challenging areas of the organization. Over time, you'll add more risk based processes to the repository and action item system. As a general rule, companies tend to average 50 risk based processes implemented over a 2 year period. It's not uncommon to have over 130 processes implemented over a 3 to 5 year timeframe. Below is an example of some of the process events that can be addressed.



\

Culture Matters

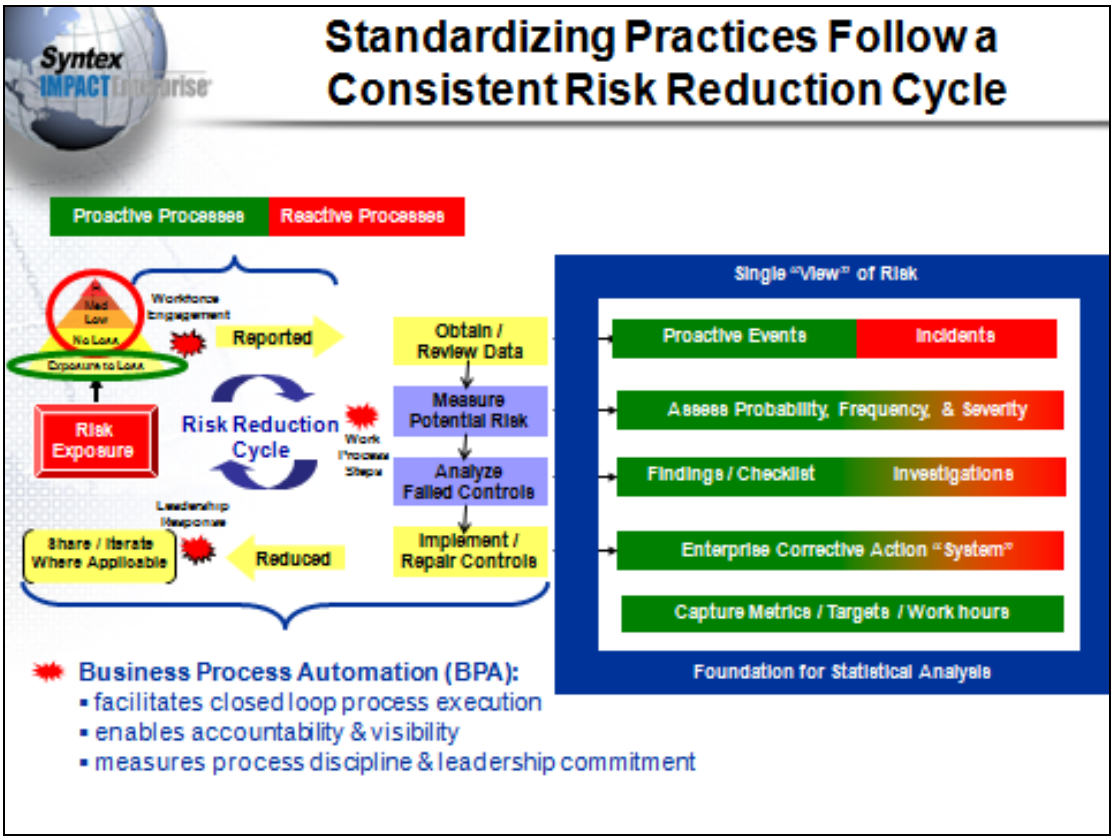
An additional vital step in implementing the continuous process improvement approach is proactively evolving the company's risk management culture. One common factor between companies with strong Enterprise Risk Management practices is that they have a management system that is imbedded as part of their core processes and culture. At ExxonMobil, that management system is called the Operational Management Integrity System (OMIS). For GE, they primarily use Six Sigma as their overriding management system and driver of their operational culture. In companies with strong risk management cultures enabled through a management system, they embed this process orientation in all operational aspects of the business which is included from the very beginning of employment starting with the way they train employees to do their jobs. This "Plan, Do, Check, Act" (PDCA) orientation reduces variation and creates more predictability in the operations of the company. The risk reduction orientation permeates the way they investigate incidents when something goes wrong, the way they audit their processes to help ensure that the defined procedures are being executed consistently, and the way they use an integrated action item management to keep front line workers and managers accountable for their risk mitigation duties. They continually train and communicate to their teams to focus on risk management and management systems as a way to improve their operations each and every day.

As a contrast, one can read in the news about another fatality at a refinery, additional fraud discovered at a firm already in trouble, or a rogue trader continually taking risky positions beyond his level of authority. Of course, every company claims to be managing operational risk. And they all are to some extent. However a company's risk culture has a lot to do with how the average employee views risk events and risk exposure. As mentioned above, companies with less mature risk cultures tend to focus on "compliance". Another common cultural problem is to focus solely on the problems that are believed to be the "big" exposures – those items with a high potential severity even if the potential frequency of an incident is low. A key problem is that the organization doesn't understand that the "big" exposure is related to lots of low consequence behaviors. By focusing on intuitively what they believe are their "big" potential exposures without focusing on the other actual and potential events of lower severity, the company often is blind to the cumulative effect of multiple failures creating the PERFECT STORM. Thus without analyzing their respective risk management practices, a company with weak operational risk practices can look as good from a financial risk perspective as a company with strong operational risk management practices, until a catastrophic event happens. Then in the aftermath of a serious incident or major audit finding, it becomes all too clear the culture that overlooked "small" process problems, the cumulative track record of incidents that pointed to something "big" yet to occur, and all the corrective actions that were known but not implemented. All the things that a strong Risk Management culture helps prevent. The surprises that a continuous process improvement approach helps prevent.

Enabling a Common Risk Framework

The next step in the successful execution of a continuous improvement initiative lies in the organization's ability to establish a common framework. The framework needs to span mitigating risk exposures discovered from reactive (incident based), proactive (audit based), and analytical (statistical analysis based) processes. Integration of these typically

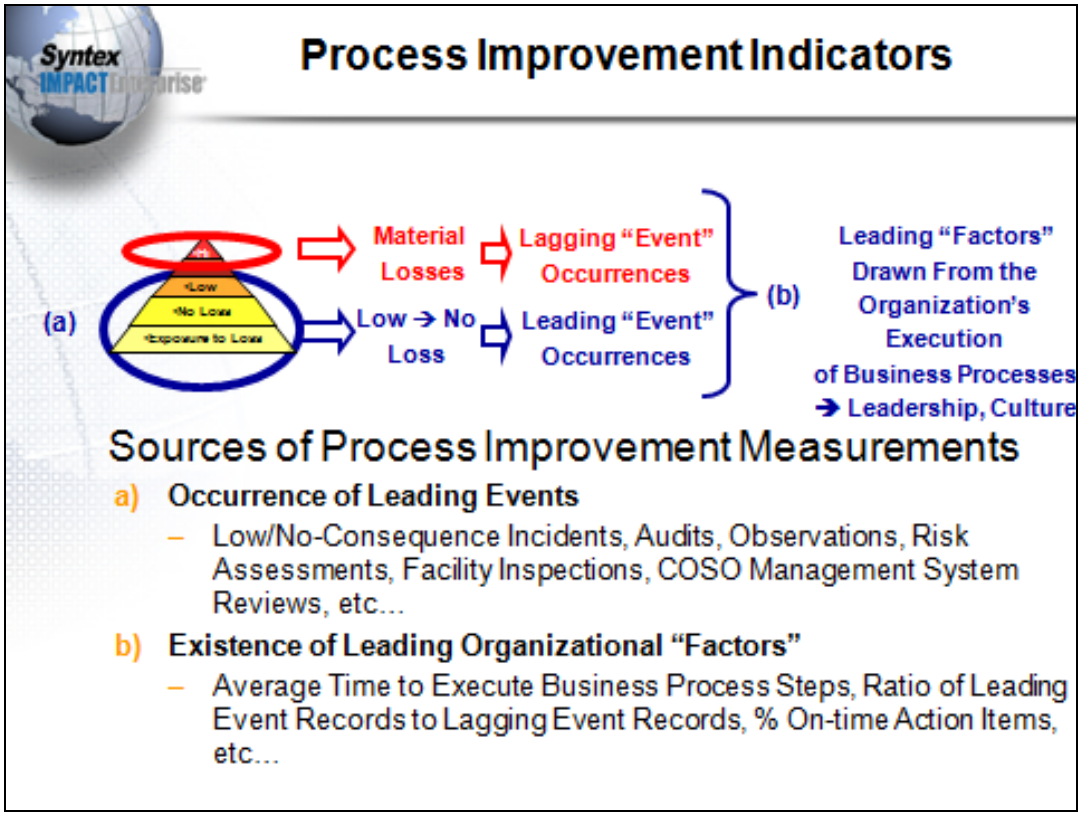
disparate processes and systems provide leaders with information that raises the awareness of and improves responsiveness to resolving management system weaknesses. To effectively execute continuous process improvement, organizations need an enterprise-wide risk management framework to integrate their various management systems and provide a conduit for predictable, consistent execution. Below is an example of a standardize approach for continuous improvement using a business process model called the Risk Reduction Cycle.



By implementing a consistent Risk Reduction Cycle process, a company can more effectively develop a consistent repository of risk data, use a repeatable process for proactive and reactive events, and execute more effective analytics to determine the enterprise-wide risk exposure. The first step of the risk reduction cycle is to capture information regarding the event (whether the event is an incident or audit/assessment). Next the event data is reviewed and additional information is added. At that point, the event is assessed related to probability, potential severity and frequency of the various types of consequences. This provides the risk weighting for the event by determining what potential consequences could have occurred (vs. what actually did occur). Next the root cause analysis is performed for incidents or findings are developed for an audit. Once the corrective or preventative actions are developed, the integrated action item system is used for closed loop execution of those mitigating steps. Finally a lesson learned step executed to share best practices and relevant learnings across the organization. Throughout the process, there are two key enablers: 1) a repository with a

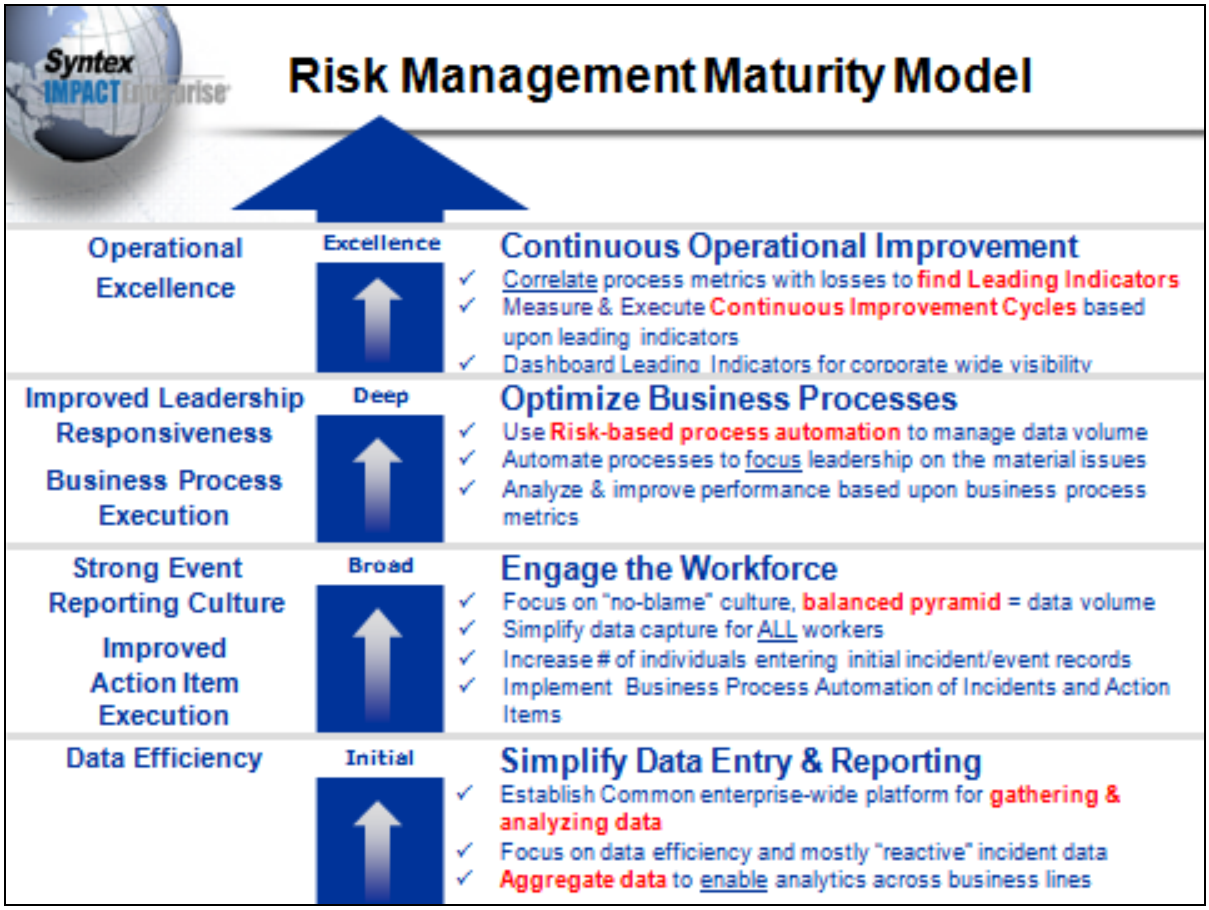
single view of the company's risk exposure and 2) a business process automation framework to use workflow to manage and monitor the progress of the Risk Reduction activities.

Due to the combination of the single, enterprise-wide view of the risk data along with the business process automation, the company now has a framework for tracking process improvement indicators. As Dr. Edwards Demining stated, "You can't manage, what you can't measure." Rather than using lagging indicators (like the number of major loss events), you are able to manage from leading factors drawn from the organization's actual execution of the risk reduction processes. To provide good leading indicator data, the organizational cultural improvements will be targeting a balanced pyramid of many more proactive findings discovered through audits compared to the number of no or low loss incidents reported. Also, many more low consequence events should be reported than the number of material loss events. The types of metrics that can be measured to provide leading indicators of process improvement include average time to execute a particular business process step, ratio of leading event records to lagging event records, percent action items completed on-site and etc. Ultimately these metrics become components of higher level factors such as leadership commitment and risk culture. The diagram below outlines the sources for process improvement metrics.



A Roadmap for Implementing these Changes

Now that we've outlined the goals of a continuous process improvement initiative to reduce risk, let's walk through a structured roadmap describing how to guide your organization through the journey. As the company is implementing and maturing its continuous process improvement initiative, the organization will undergo some clear evolutionary stages in its cultural maturation. Below is a Risk Management Maturity Model outlining the major mileposts of risk process maturity.



The initial foundation for continuous process improvement is establishing integrated data via a common, enterprise-wide platform for managing operational risks. At a minimum, the company will need a common risk data repository at this stage. This is achieved through simplifying event data entry, and the benefit is efficiency in reporting and analysis.

After achieving data efficiency, the next step is to engage more of the workforce in identifying and reporting risks. This is achieved through a focus on improving the culture so that employees do not feel that either they individually or their department will be "punished" for reporting any type of risk. There are several keys to achieving this level of risk process maturation. The company needs to provide easy-to-use systems to enter information about events, provide incentives that do not punish individuals or departments for incident-related events, and establish an easy-to-use action item system that provides feedback to the workforce and shows leadership involvement in the resolution of issues. The benefits of this stage of maturity are a strong event reporting culture, a balanced pyramid of risk events, and improved execution of action items.

After a strong event reporting culture is in place, the next stage is to optimize the execution of business processes that are critical to risk reduction. This is achieved by increasing the automation of these processes and by making process enhancements based on the ongoing performance. For example, if investigation methods are being applied inconsistently, the company can use business process automation to implement a business rule that will automate these investigation steps. The typical benefits of this stage of maturity are improved leadership responsiveness and improved execution of risk reduction processes.

Once a strong event reporting culture is in place and risk-related processes have been automated and optimized, a company can achieve operational excellence by identifying and monitoring the key process improvement indicators from these business risk reduction processes. By using statistical analysis to correlate these process indicators to loss rates, the company can identify the Leading Indicators that will produce the biggest impact. This also supplies management with the metrics to monitor and manage continuous process improvement. These Leading Indicators may include metrics about reporting culture, action item execution, business process execution, leadership responsiveness, and others. For example, if a site is performing poorly (has a high incident rate, repeated negative audit findings, etc.), the Leading Indicators should be analyzed and used to make improvements. Examples of these indicators could include metrics such as rate of employee event reporting, mean time for leaders to respond, rate of applying a root cause analysis process, and a risk-weighted action item completion rate. Often a dashboard of metrics and graphs is used for effective and consistent communication of these key factors across the organization to drive further process improvement.

The enterprise-wide Risk Framework enabled through the Maturity Model helps your organization achieve its objectives across four categories:

- Strategic – high-level goals, aligned with a company's mission
- Operational – efficient and effective use of the organization's resources
- Reporting – reliability of the company's reporting
- Compliance – compliance with the applicable regulations.

The resulting benefits of this Risk Framework span both Risk Reduction and Operational Effectiveness. For risk reduction, the organization improves compliance (fines/penalties), reduces the likelihood of a loss, and reduces the total cost of the losses that occur. For operational effectiveness, the framework improves reliability and process integrity, shortens process cycle times, and increases both accountability and visibility across the company.

Summarizing the Business Impact

The ultimate goal of Risk Management is targeted at reducing any factor that represents a threat to a company attaining its strategic objectives. The desired outcome is to reduce the variability in the organization's process execution and thus produce more predictable financial and operational results.

The scope of the financial impact is on both revenue and net income because Risk Management is as concerned with revenue growth as it is with loss prevention. This expanded opportunity is based on the premise that a continuous improvement initiative enabled by enterprise-wide common Risk Framework will increase risk mitigation effectiveness, reduce process variability, and help ensure that a company's strategic objectives can be accomplished. Companies that implement more and more of their processes under the framework will yield greater returns by integrating those activities with a common set of risk mitigation processes and tools.

Companies at different levels of Risk Management Maturity will have different degrees of variability and volatility in their business operations. With each step up in maturation, a company creates more predictable operational processes and thus has more predictable earnings and a more stable capital structure. At the most basic level of Risk Management, a company has implemented integrated, repeatable processes across the organization with a common data repository. At the next level, through a company's culture, training, and practices, it has created an environment where employees are continually looking for, identifying, and reporting risk exposures in the company. This increased level of awareness and information creates the opportunity for the next level of maturity in which the company has different processes based upon the potential risk in the exposures that have been identified. As a result the company can prioritize and allocate resources to address those exposures with the highest risk ranking (assessment of risk through the probability, frequency and potential severity of the exposure). Finally at the highest level of Risk Management Maturity, the organization has a continual process improvement process in place that includes the repeated identification of the leading indicators of specific risk exposures in the business. Through these leading indicators, the business can have even more confidence that the allocation of resources to risk mitigation is truly going to those factors that are effectively reducing the current risk exposure. Through this evolutionary maturation process a company continues to reduce its variability and volatility in operations to help produce a more predictable earnings and capital outlook.

About the Author

Trent Derr is the President and CEO of Syntex Management Systems, Inc., an operational risk management software company. Syntex's customers span multiple industries and include 5 of the Fortune Global Top 10 companies. Trent was previously Chief Operating Officer for P2 Energy Solutions and Chief Operating Officer and co-Founder for Novoforum. In addition, Trent has held senior positions with SAP, Oracle, Software 2000, and PriceWaterhouse. The Syntex website is www.syntexsolutions.com.