A CONVERGENCE-BASED APPROACH FOR MANAGING OPERATIONAL RISK AND SECURITY IN TODAY'S CHALLENGING ENVIRONMENT

By Marc S Sokol, CISM, CHS-III

(With special thanks to Vicki Yamasaki, Richard Moore, Debra Zoppy, Cliff Lange, and Jack Campbell for their contributions, review, and support)

February 18, 2015

"We call it business. We pretend the plan and the forecast are the real tools of business, but of course they're minor accessories. Conversation and trust are the real tools of business."
- Liz Ryan, Forbes magazine

Companies today are faced with a very challenging operating environment including a diverse set of environmental variables and threat landscape including:

- Low interest rate yields,
- Turmoil in Europe,
- Stagnant U.S. economy,
- Growing tax burden,
- Volatility in certain investment markets,
- Growing threat of terrorism by ideological extremists,
- Stronger regulatory intervention combined with more prescriptive regulations,
- Increased scrutiny by rating agencies,
- The velocity, breadth, and capability, of cyber-attacks in which a single micro-agent from anywhere in the world can inflict financial, legal, regulatory, trust, and brand damage,
- Third party upstream and downstream risk/liability rising with the broader reliance on third party support so companies can focus more on core competencies,
- Human capital risks (succession, engagement, retention, performance, development, compliance),
- Natural disasters that concurrently affect multiple geographical regions, managing brand and reputation in a social media "viral" world,
- Sustained pressure remains to contain expenses on non-revenue generating areas of a company, and
- Maintaining and satisfying the demands of more empowered, better-informed, and less loyal customers.

However, while the environment in which companies operate today has changed and the risks are significantly more dynamic, companies continue to resist this change and manage their operational risks and security programs in a legacy and antiquated manner that is not well positioned to adapt and respond to a very changing landscape of threats. Specifically, a typical organization may have dozens of risk managers spread across Legal, Human Resources, Lines of Business, Finance, Corporate Security, IT Security, Business Continuity, Compliance, Information Technology, and Facilities/Real Estate. Each of these domains has its own individual silos and risk landscape and the various risk professionals inside each silo have there own focus on the risk triggers that are in their respective domains, not all the others inside the same company. It is the latter that is a key requirement for adapting to and managing the myriad of operational risks faced by companies today. For example, do the HR recruiter and the Chief Security Officer think the same about what are red flags in the background check of a new potential candidate or established guidelines for safe terminations? Does the IT administrator think about the same red flags that the CFO thinks about in terms of data integrity and financial reporting accuracy (e.g., its important to ensure that formulas in a spreadsheet or program are not changed without authorization, but are the formulas in that spreadsheet correct and is their integrity in the results?) Does the business owner see the same concerns that security, compliance and law see in a third party services relationship or an online business application? Do IT and Facilities understand the impact that systems and workspace availability have on certain key business operations? Can a company effectively ensure that it doesn't have hidden concentration risks in the aggregate across the enterprise that if realized, could substantially damage or impair the company? Is the company's risk appetite set by executive management being monitored and aligned with risk taking collectively across the spectrum of operational risk consequences (as opposed to on a project by project basis) by a business or support center?

Thus, the convergence of thinking by risk professionals in an organization is paramount to effective enterprise stewardship amidst these demands and challenges of today's corporate environment. However, what have perplexed many companies are exactly how to converge these resources to pursue a common mission while maintaining their specific roles and responsibilities. In addition, what is also challenging is the ambiguity in the definition of operational risk, the span in which affects every business and support center, and exactly how it can be assessed and managed effectively. For example, a commonly used definition of Operational Risk can be found in BASEL II (http://www.bis.org/list/bcbs/tid_28/index.htm) that states that Operational Risk is "the risk of loss arising from inadequate or failed internal processes, people or systems, or from external events." Additionally, this framework and approach focuses solely on the risk to a company's capital based on prior loss events. However, operational risk is a broad discipline and, contrary to other risks (e.g., credit and market risk), are not willingly incurred and are not revenue driven. They cannot be diversified, hedged, and as long as people, process, technology, and the environment in which we operate remain imperfect, they cannot be fully eliminated. Further, there are substantial differences in the way operational risks can be assessed and managed as compared to the other risk categories. Specifically, in the areas of credit, market, or investment risk, the function of performing this analysis has the following characteristics:

- Risk domains such as Credit, Market, and Investment risk management are generally performed in an isolated area of expertise within the company (generally the finance or investments area of a company)
- The necessary historical and research data that illustrates the factors and drivers that affect the economic markets is readily available both at the market level (e.g., interest rates, unemployment, changes in regulation, consumer confidence, GDP, etc.) and at the company level (i.e., financial statements, reporting disclosures, etc.)
- Extensive frameworks, models, and analytical tools are readily available
- Revenue driven and willingly incurred (risk/reward)

However, Operational Risk has the following characteristics:

- Requires extensive and ongoing cooperation and partnerships across the company from all business and support operations areas, and thus a substantial challenge in many siloed organizations
- Operational risk management and governance likely will identify opportunities for process and control improvements and/or the potential for operational failures. This scope can lead to a perceived contention between risk leaders and the business/operations leaders
- The factors and drivers that supply important information regarding operational risk are not readily available. Specifically, companies generally will avoid publicly disclosing operational failures unless required by law, and even in those cases will generally avoid any detailed information regarding an incident as it may be perceived as possibly ineffective operational or senior management, and thus could increase legal liability and reputational harm. Moreover, prior loss events generally are not a valid reference for predicting future loss events in Operational Risk because the dynamic environment in which we operate continues to change and the actors involved do not follow industry standard practices (e.g., investment folks, tec.) like investment managers, but rather are criminals, activities, nation state supported, ideological extremists, activists.

Operational risk management is, nonetheless, critical in minimizing unforeseen events and keeping potential losses within defined levels of risk appetite (i.e. the amount of risk one is prepared to accept in pursuit of business objectives), and determined by balancing the costs of sustaining a certain level of residual risk against the expected business benefits.

Fortunately, many companies today are recognizing the importance of their corporate stewardship in actively managing the operational risks they face today and in the future. They are seeking innovative, yet pragmatic business aligned solutions to address this important opportunity; especially given the impact of realizing the consequences continues to escalate over time. As a result, an effective operational risk framework and associated program must go well beyond the ambiguous BASEL type definition of operational risk, that states *"Risks of direct or indirect loss and/or not achieving business objectives due to failed process, people, information systems, and/or from the external environment"*. Rather, Operational Risk should be defined as "*The risk of consequences to the organization for failing to maintain adequate people, process, technology, and environmental controls/safeguards resulting in increased Fraud (internal and external), loss of business performance and/or increased business interruption, regulatory intervention and penalties, legal liability, financial losses/restitution, reputational harm and/or brand erosion (loss of consumer trust), increased errors/omissions in data processing and financial reporting, data loss and/or unauthorized access, use, and/or disclosure of Privacy data, security breaches (logical or physical), loss or damages to assets, and reduction in workplace safety.*" As a result, the risk analysis can be aligned with key business goals via the direct business consequences in terms of the total inherent risk (aka distressed value), the effectiveness of existing safeguards and controls intended to reduce the inherent risk, and the resulting residual risk level. The residual risk level can then be compared with the established risk appetite and whether those consequences, if realized, aligns with business objectives including whether they are adequately balanced with the expected benefits of pursuing or maintaining the business opportunity or function respectively. The legacy approach commonly sought as a result of the BASEL guidelines, while they may be effective solely from a financial perspective in establishing some level of capital reserve allocations, from a business operations perspective they appear to a business leader as a myriad of statistical modeling data that includes abstract valuations of probability and likelihood solely based on a sterile view of prior loss event data. They afford neither any real evaluation of operations, nor will not adequately deliver the intelligence data at the right level to proactively enable the business leader to make thoughtful, measured decisions regarding the present and future risk they are facing as many aspects of operational risk are not limited to economics and capital reserves (e.g., reputational harm, lost trust and consumer confidence, regulatory intervention, etc.).

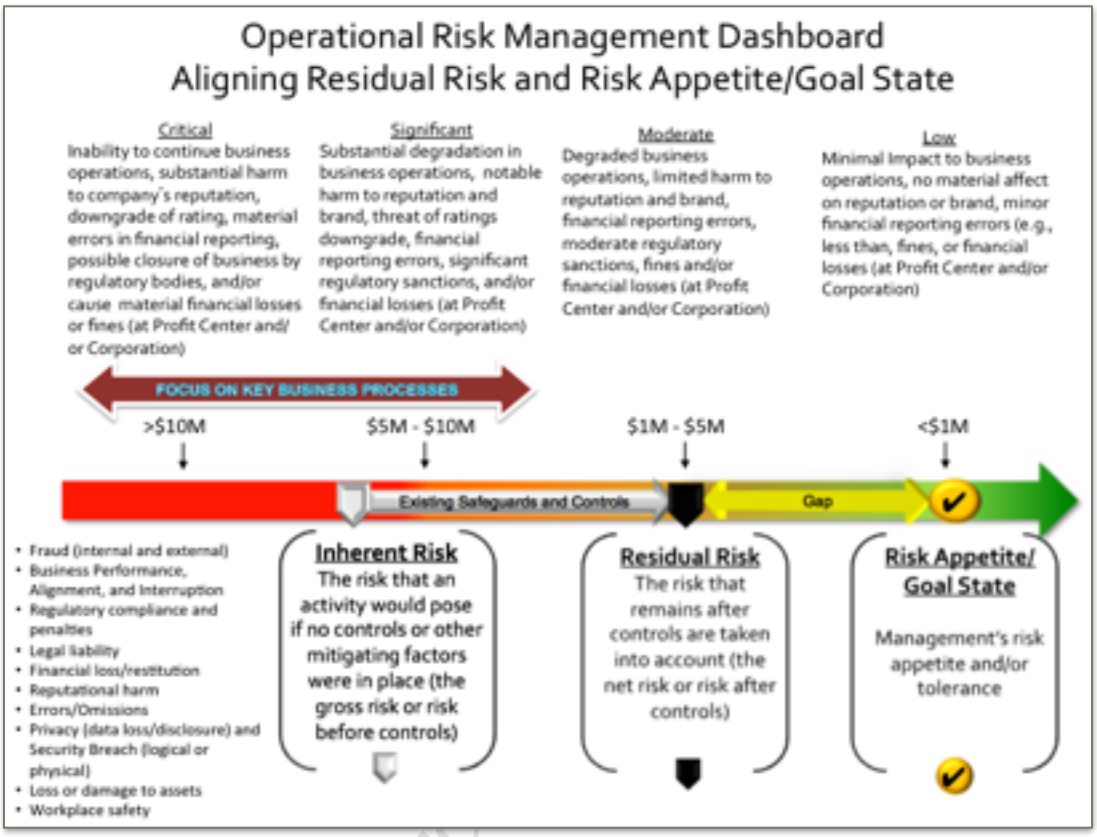
Therefore, there are two key criteria for ensuring a successful operational risk management program that truly can be integrated into the culture of a company and fully integrated into day to day business operations and decisions. First, it is essential to establish and ensure the full support of the CEO and executive leadership team of a company in making operational risk (including third party risk) a priority in the organization and business leaders will be held accountable and responsible for understanding their operational risks and ensuring their alignment with the company's established risk appetite.

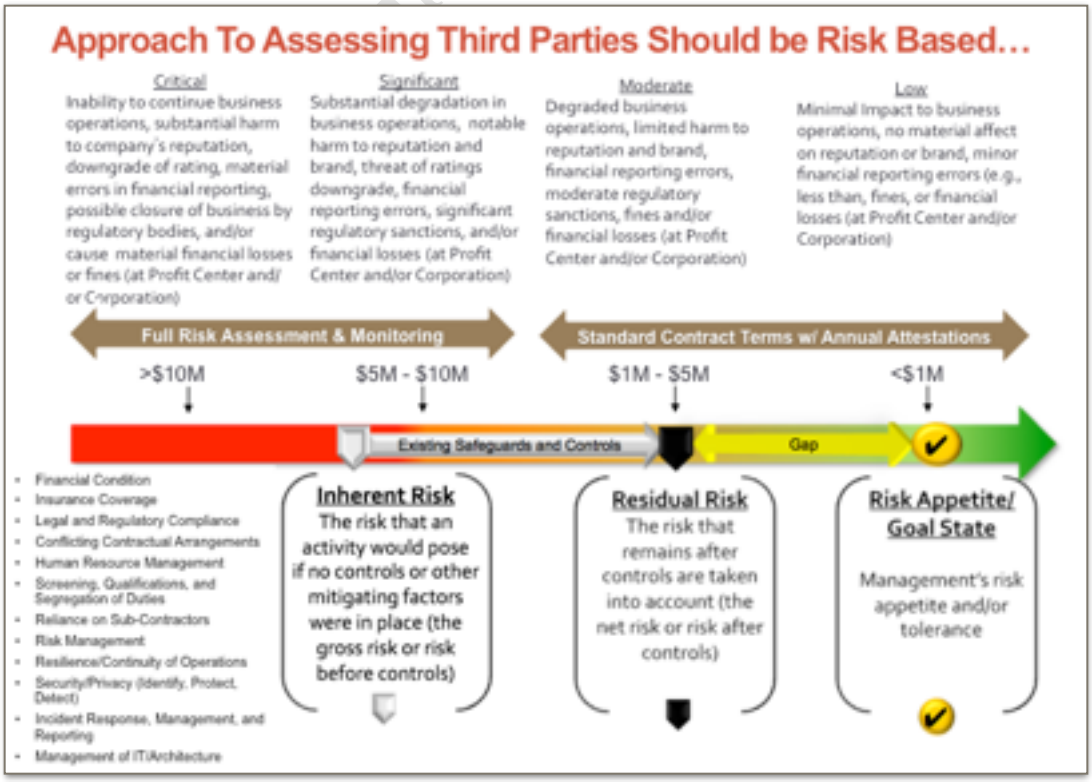
Second, the company should establish a set of key consequences is relevant to the business model and priorities of the organization. The following is an example of a set of operational risk consequences derived from a number of various industry studies and frameworks on operational risk:

1. **Fraud** - risk from deception that occurs with intent to result in financial or personal gain
2. **Business performance, alignment, and interruption** risk may arise when product, service, fail to meet performance required and/or become jeopardized by natural or man-made events
3. **Regulatory intervention and penalties** may arise when the services, products, or activities fail to comply with applicable laws and industry regulations
4. **Legal liability** may arise when a service provider exposes the customer/institution to legal expenses and possible lawsuits and/or judgments due to intentional or unintentional product or process failures
5. **Financial loss/restitution** risk of fines, penalties, and/or other sanctions to be incurred
6. **Reputational harm** may arise when actions or poor performance of a service provider causes the public to form a negative opinion or loss of trust about the company
7. **Error/Omissions** risk arises when work is inadequate, incomplete, incorrect, or when negligent actions occur
8. **Privacy (data loss/disclosure) and security (breach either logical or physical)** risk of unauthorized access to, collection of, use of, and/or disclosure of personal information
9. **Loss or damage to assets** risk occurs when property owned by the company regarded as "having value", become unavailable, lost, stolen, corrupted, or inoperable
10. **Workplace safety** risk occurs when there is a potential for personal injury, abuse, and/or illness in the workplace and/or can materially impact morale and the ability of staff to perform their duties

Upon establishing a reasonable set of consequences (i.e., limit to 10), the company's executives (with input from the Board) can establish a risk appetite (the amount and type of risk that the firm is willing to seek or accept in the pursuit of its long term objectives as generally defined in industry standards including the Institute of Risk Management, ISO31000, and BS311001) for each potential consequence. Next, an inventory of key business processes should be developed and each evaluated for its inherent risk (distressed value). In many cases, this inventory already exists in a business area's Continuity Plans. Only those processes with an inherent risk rating that exceeds the highest risk appetite identified for a consequence need be included in the next step. Existing safeguards/controls for that process (which includes people, process, technology and environment) should then be evaluated spanning people, process, technology, and environment (it's important to include third party service providers if they are an integral part of the business process). The effectiveness of these safeguards/controls can be evaluated in a variety of ways including maximizing existing data, if available, including internal or external audits performed, regulatory reviews, and/or assessing their alignment with known effective industry standards. The end result will illustrate the residual risk for that business process across the spectrum of key consequences concerning the business and/or company (essentially Inherent Risk less the effectiveness score of existing safeguards and controls produces the residual risk score) and will identify any gap between the residual risk and established risk appetite. This will afford management the transparency and prioritize any mitigation efforts if warranted. It may also result in a recalibration of risk appetite.

The following are sample qualitative Operational Risk Management and Third Party Risk Management dashboards intended to aid in illustrating a means for qualitatively reporting key operational risks





It is important to keep in mind that, due to the breadth of these consequences, the convergence of thinking by risk professionals across the organization in order to effectively assess these key consequences is going to require breaking down the many silos and single domain thought process through strong leadership, top-down support, inclusion, teamwork, and most importantly effective communication and trust. Thus, while each "domain" may have its own objectives, they all can align with a common mission, work together, and thus benefit from the force-multiplier effect that collaboration and teamwork brings to overcoming dynamic obstacles and challenges

In conclusion, companies today are faced with a very challenging environment in which operational risk must be managed effectively. Using a multidimensional approach that inspires convergence of thinking by risk professionals across the organization is paramount to developing and implementing an effective operational risk framework and program that can be integrated into every day business decisions and the culture of a company. Only through this integration can an organization ensure sustained and optimal enterprise stewardship.

About the Author:
Marc S Sokol, CISM, CHS-III

Marc is an accomplished, energetic, pioneering industry leader in risk and security management with over 20 years of proven success developing, implementing, and leading business aligned and pragmatic governance, risk management, security, privacy and compliance solutions and programs for companies including Citibank, Merrill Lynch and Guardian Life Insurance Company. His impactful and successful solutions and programs are founded upon a philosophy of minimizing risk while maximizing operational capability through collaboration, teamwork, balance, efficiency, and increasing the agility and performance of the organization. Marc also gives back to the industry by mentoring peers and actively engaging in a number of public/private information sharing partnerships including the and the Financial Services Information Sharing and Analysis Center (FS-ISAC) where he was a founding member and Director on the Board for almost a decade, led and/or participated in a number of industry organizations and groups including ACLI, LOMA/LIMRA, ASIS, FINRA, BITS, Institute of Operational Risk, Governance Risk and Compliance Professionals, USSS Electronic Crimes Task Force, among numerous others, has received numerous industry awards for his programs and contributions to the profession, and is a featured speaker and panelist at numerous industry conferences sharing solutions and strategies with peers.