

Enterprise Risk Management (ERM)

A GRC Based Approach to Risk and Reward Management



Preface

At MetricStream we challenge ourselves and our customers to adopt an approach to risk management that enables us to utilize ERM in the broader context of Governance, Risk & Compliance (GRC) Management: to mitigate risks and also revisit their business processes to capture value generating business opportunities. Concepts and viewpoints herein build upon our experiences with our customers across industry in helping them reengineer their business processes to bring about a change in how they view, mitigate and profit from business risks.

This point is important enough to reiterate, however briefly, in this paper. But readers will note that the topic at hand - recognizing ERM in the broader unified GRC environment - lends itself more to a focus on business process reengineering for avoidance, rather than on risk-taking for reward. The narrower focus of this paper shouldn't obscure the bigger picture, of the effect of ERM as a central covenant to a unified and effective GRC program.

Companies will make money by taking smart risks and lose money by failing to re-tool their legacy business processes to assess and mitigate risk effectively.

Table of Contents

It's a perilous time out there; the emergence of Enterprise Risk Management (ERM)	4
New Guidance – Standard & Poor's risks affecting shareholder value	5
Building the business case for ERM	7
MetricStream: GRC's preeminence powers ERM across industry silos	9

The emergence of GRC based - Enterprise Risk Management (ERM)

Near Real Time Visibility to Threats and Opportunity

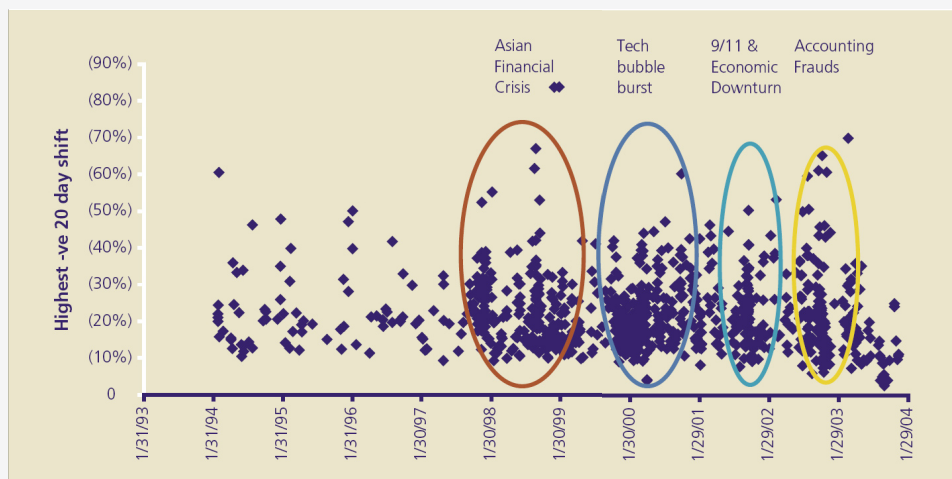
We live in a perilous world, as we speak the US Federal Reserve prepares to embrace for the current economic environment without using the “R” word, and that R word isn’t “risks” or proactive “risk management”. It is reactive “Recession”. From meltdowns in the mortgage industry, terrible weather and natural disasters in your global operations, lead paint in toys to corporate executives detailing your company’s financial performance on social blogosphere – threats are everywhere. And so are opportunities, diverse, interconnected and complex such as disruptive innovation, new regulatory mandates and competitor missteps. As put by a Chief Risk Officer of a global financial institution, “Risks create opportunity; opportunity in turn creates value; and that value ultimately creates shareholder wealth”

Almost half of the 1000 largest global companies suffered declines in share prices of more than 20 percent in a one-month period, relative to the Morgan Stanley Capital International (MSCI) World Index. By the end of 2003, roughly one-quarter of these companies had still not recovered their lost market value. Another one-quarter took more than a year for their share prices to recover. With the emergence of unified Governance, Risk and Compliance (GRC) based ERM solution – firms are no longer surrounded by reactive measures that cause shareholder value to decline and cause a decline in corporate goodwill and responsibility in the marketplace. An effective GRC program covers all tenants of effective strategic management – ethical corporate governance, where the CEO sets the tone for the business strategy and the Board is empowered by real-time visibility into operational details i.e. the realities - of this vision’s material weakness. GRC covers risks that emanate from multi-regulatory and compliance management initiatives, that include dealing with SOX, SEC, PCAOB, ISO, FCPA, FDA, cGxP, FERC, NERC, COBIT, PRIVACY, IP, BASEII, AML, GREEN TECH, EH&S, 21 CFR, FAA and so on. In the past, large or small firms each mandate had its own program, its own team and its own tool, and hence businesses were playing catch-up. GRC intermediates the prevalence of this silo approach by combining these silos into a single program that simply enables the firm to be proactive in its approach to dealing with these myriad of complexities. However, GRC can be effective only if the right priorities are visible at the right time to the right stakeholder.

ERM is hence the central convent of a unified approach to GRC. ERM is the means to prioritize and manage risks and opportunities across a firm in a way that it generates greater business value. ERM pays for itself by reducing financial losses, improving business performance and enhancing risk identification and assessment efforts.

Rare Events Can Devastate Value

Impact of Recent Low-Probability Events on Value Losses
(Source: Deloitte ERM Value Killers© 2005)



New guidance from S&P to identify risks affecting shareholder value

“The ERM Evaluation ultimately will be our opinion of the quality of management practices” – S&P

Our interest in codifying management analysis under the ERM heading coincides with increased interest by many companies to initiate their own ERM programs — or other risk-management practices -- to increase risk-adjusted returns, improve strategic judgment, and/or avoid extraordinary losses due to lawsuits, fines, operational failures, or negligence. The intersection of these interests is in the expectation that a firm’s future ability to meet financial obligations in full and on time is more likely to be enhanced by strong ERM or diminished by weak or nonexistent ERM. Our principal interest in evaluating ERM is to implement steps that will limit the frequency and severity of losses that could potentially affect ratings.

Source: S&P Initial Risk Enterprise Risk Management Analysis For Credit Ratings Of Nonfinancial Companies

S&P’s guidance is primarily aimed at helping financial and non-financial services customers to have a management that values ERM to and has a clear strategy to mitigate losses in shareholder value. They’ve introduced Enterprise Risk Management (ERM) analysis into the corporate credit ratings processes to provide guidance via means of a structured framework to evaluate the company’s management as a principal component in determining the overall business profile – they intend to take Enterprise Risk Management (ERM) into their analysis of business and its impact on corporate credit ratings. This undertaking and will impact a wide range of verticals namely: Manufacturing, Commodities, Utilities, Consumer, Healthcare, Technology, Media, Telecommunications and so on. S&P’s wide reaching impact will see other rating agencies use basic ERM frameworks in their analysis of businesses. S&P expects firms with superior ERM ratings to have less volatility in earnings and cash flow, and will optimize the risk/return relationship. Furthermore they intend to use these ratings to serve as industry wide risk management benchmarking.

S&P deems financial services firms, due to the nature of their business, intrinsically riskier than non-financial services organizations; and hence in contrast the ratings process for the non-financial services organizations would be a verdict of the efficacy of the management to execute the vision of the company and build shareholder value. The scoring methodology will have companies scored in four primary categories: weak, adequate, strong and excellent – the scoring weight would factor in the relative significance of ERM in the vertical industry. Where companies rated ‘weak’ display low levels of ERM maturity – complete absence of controls, in contrast with those rated ‘excellent’ are mature companies with a comprehensive program of leadership, process, people and technology to manage risks.

In 2005, Hurricane Katrina cost insurers more than \$41 billion, the largest loss event ever for the industry. The magnitude of losses eventually reported shocked many. In the wake of the disaster, ERM was a differentiating element when we reviewed insurer credit ratings. Some insurers with weaker ERM had losses that were as much as twice what they previously reported as their “probable maximum loss”. These insurers were unable to even estimate their losses several days after the event. On the other hand, insurers with stronger ERM could quickly estimate losses that were within 25% of actual claims. (Source: S&P)

Sample Risk Types			
Environment Risks	Financial Risks	Supply Risks	Management Risks
Business Continuity	Capital availability	Commodity Prices	Corporate Governance
Business Market Environment	Credit/counterparty	Supply Chain	Data Security
Environmental	Financial Market Risk		Employee health and Safety
Liability lawsuits	Inflation		Intellectual Property
Natural Disasters/Weather	Interest Rates		Labor Disputes
Pandemic	Liquidity		Labor Skills shortage
Physical damage			M&A/restructuring
Political risk			Managing complexity
Regulatory/legislative			Outsourcing problems

Four major analytic components or “pillars” will support S&P’s ERM analysis; these factors are broad, sector agnostic views into the risks faced by the firm. These include:

- Analysis of making routine corporate decisions
- Analysis of risk controls
- Analysis of emerging risk preparation
- Analysis of strategic risk management

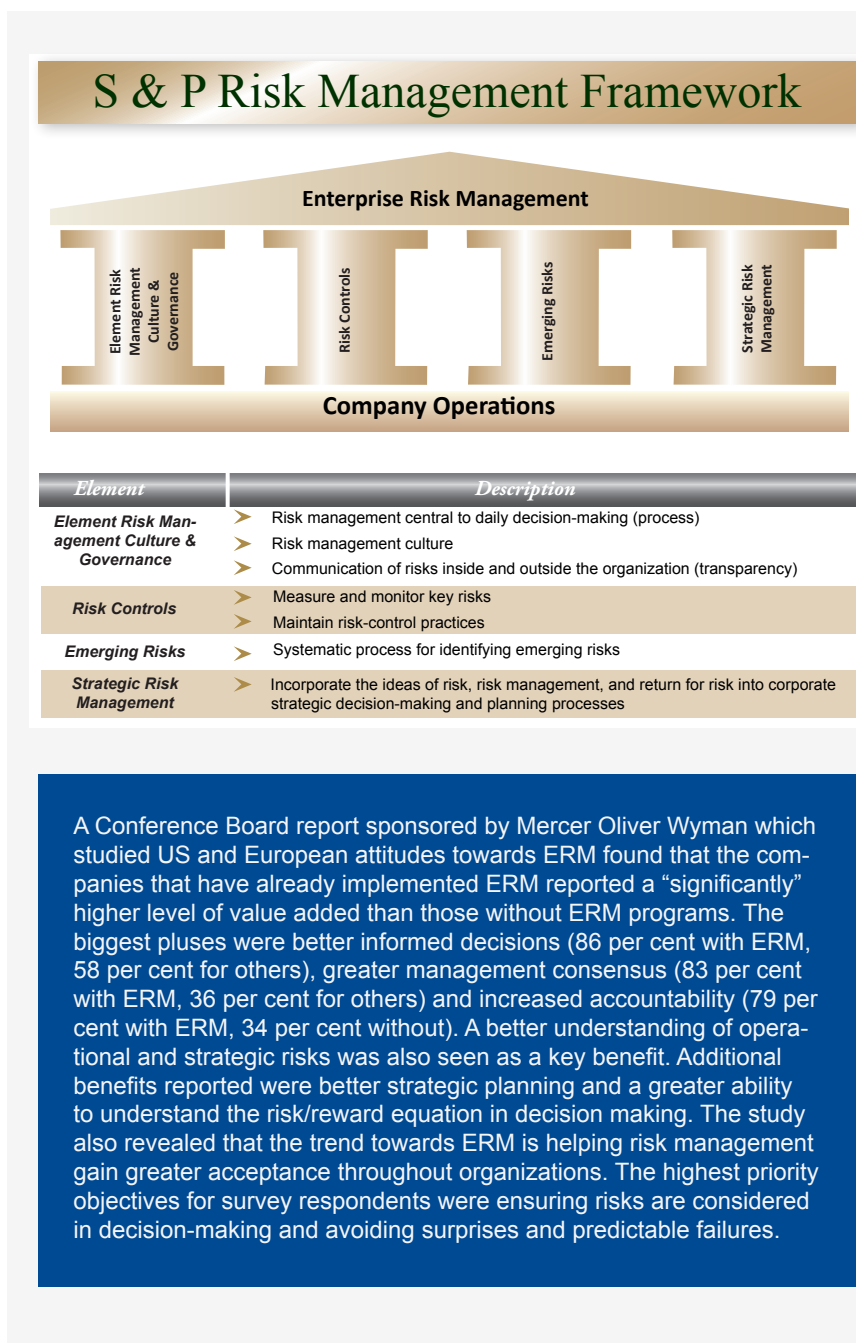
Risk management culture and governance provides visibility of importance of “risk taking” or lack of in routine decision making – within the company’s corporate culture. S&P will evaluate a firm’s maturity by assessing its firm structure, roles and responsibilities to execute ERM. The visibility that the top-management has to daily execution issues with line management and the rendezvous that occurs to communicate and collaborate on routine decision making are firm indicators of a winning ERM strategy.

Risk controls help organizations implement the culture and governance, through identifying, measuring, and on-going monitoring, reconciling risk, setting risk limits and arrive at the firm’s daily profile for managing risks in a distributed world. S&P intends to develop an exhaustive list of controls across sector and firm – and depending upon the relative weight of each control will help painting a picture of the firm’s overall ERM efforts.

Emerging risk preparation – the black swan effect author Nassim Nicholas Taleb in a recent book ventures out to talk about the black swan affect that can have on a firm’s long term survival. These are the types of risks that are extremely rare adverse events and are impossible to manage in a control environment. However some ERM best practices– can help a firm remain prepared for addressing such scenarios coming to life. Preparedness includes environmental scanning, trend analysis, stress testing, contingency planning, problem post-mortem, and risk transfer. A firm’s ability to prepare itself for the best or the worst of – will factor in to its S&P Risk profile.

Strategic Risk Management will help S&P to arrive at a single classification of your firms ERM standing or profile – this could be expressed in terms of earnings loss, Risk profile can be expressed in terms of earnings loss, enterprise value, or other important financial metrics for various risks or for each firm business.

The essence of planning for the future as a progressive firm is changing. Infinite – risk/reward possibilities, disparate and complex threats are in the face of today’s vibrant and interconnected global firm. Old adages on risk – and reward are still worth their value in gold, however they now require several additional people, process, organization



A Conference Board report sponsored by Mercer Oliver Wyman which studied US and European attitudes towards ERM found that the companies that have already implemented ERM reported a “significantly” higher level of value added than those without ERM programs. The biggest pluses were better informed decisions (86 per cent with ERM, 58 per cent for others), greater management consensus (83 per cent with ERM, 36 per cent for others) and increased accountability (79 per cent with ERM, 34 per cent without). A better understanding of operational and strategic risks was also seen as a key benefit. Additional benefits reported were better strategic planning and a greater ability to understand the risk/reward equation in decision making. The study also revealed that the trend towards ERM is helping risk management gain greater acceptance throughout organizations. The highest priority objectives for survey respondents were ensuring risks are considered in decision-making and avoiding surprises and predictable failures.

and technology “upgrades” for firms to survive and thrive. ERM hence will provide the leaders of the organization – a means to increase earnings – and shareholder value – whilst staying within the well-defined and organizationally absorbed risk tolerance.

Building the Business Case for ERM

Improved Risk Awareness

Application of the Enterprise Risk Management Framework, in conjunction with related risk management activities, augments a cultural shift to a risk-smart workforce and environment in the organization, which ensures that the organization has the capacity and tools to be innovative while recognizing and respecting the need to be prudent in protecting its interest. According to a KPMG survey on ERM conducted in 2006, 76% of the enterprises quoted **“improved awareness of risk and collaboration”** as one of the major benefits. This is further upheld by former Federal Reserve Banker Susan Schmidt Bies, *“Increased risk awareness by staff throughout the enterprise is integral to managing risk successfully.”*

Improved Organizational Efficiency

The implementation of an ERM framework brings with it improved efficiency across the entire value chain - providing top-down coordination necessary to make various functions of an organization work efficiently. An integrated team not only better addresses the individual risks facing the company but also the interdependencies between these risks.

Enhanced Shareholder Value

A strategic ERM framework brings with direct impacts to the overall profitability of a firm. The February, 2008’s Treasury & Risk Magazine cover story, Audit Busters, reports the business case for the CRO partnering with the CFO at large corporation resulting in the transformation of their compliance programs to serve their business strategy while

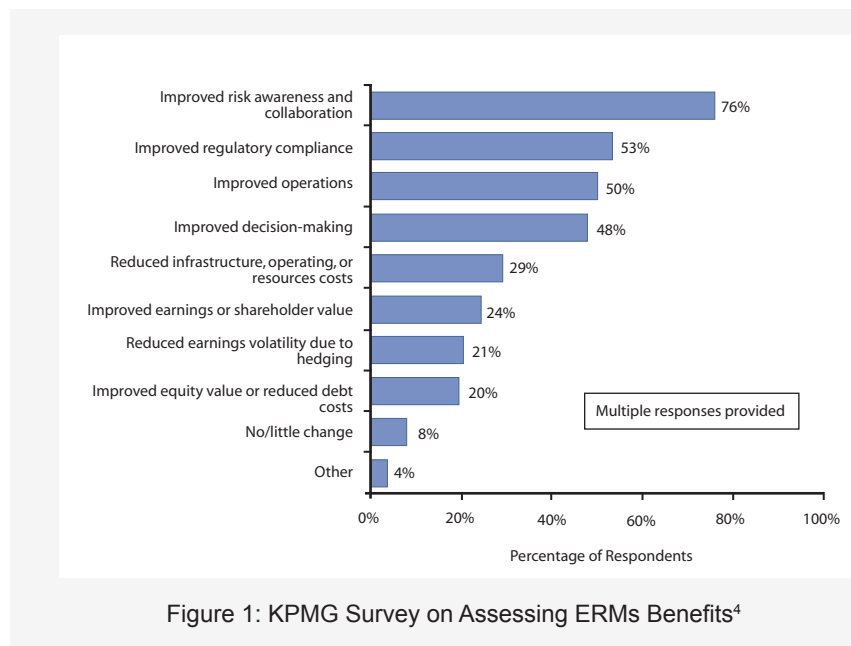
reducing their external audit hours by 60% at the same time. *“Costs can vary”, the CRO says. “Despite the fact that Risk management software could cost you anywhere from \$25,000 to \$250,000, depending on the size of the company and the complexity of the operation, it’s not expensive. The payoff is enormous, because you’re not just saving on auditors’ fees. You’re also saving on internal costs, enhancing your credibility, and streamlining risk management across the entire organization. It ultimately pays for itself.”*

Risk Exposures Clearly Mapped

ERM enables an organization to identify measure, monitor, and control its inherent risk exposures of the business at all levels. Elements like Risk Assessment, Event Management, and Key Risk Indicator play an important role; enabling the organization to evaluate the risk controls, based on the identified inherent risk, and to measure the residual risk which remains after the implementation of controls.

Roles and responsibilities re-defined

Clearly defined roles and responsibilities within the firms risk profile not only streamlines the risk management process, but also allows risk managers to incorporate accountability into the work culture of the organization.



Enhance Corporate Social Responsibility (CSR) Factor

According to the economist intelligence unit survey 2007, the most important outcomes of effective risk management is that it helps in **“protecting and enhancing the reputation of the organization”** (50 percent). In addition, 41 percent say ERM helps in ensuring regulatory compliance and effective capital and resources allocation. Respondents also highlighted “loss avoidance” 38%, increasing shareholder value” 32% and “reduced earnings volatility” 26% as some of the other benefits.

ERM – creating sustainable value

A majority of the respondents in the AON survey on ERM 2007 had companies relaying that their ERM functions produces clearly identifiable outcomes and benefits. They bring about organizational sustainability and competitive advantages; an enhanced sense of corporate goals and objectives, talent management, significant reductions of exposure and losses. Identifying principal benefits of ERM, 92% of the respondents say that ERM helps in demonstrating compliance, 69% say it enhances behavior and improves organizational performance and efficiency 54% say it helps in reducing cost of risk and secures growth opportunity under optimized condition.

Executives of most companies and other entities have developed processes to identify and manage risk across the enterprise, and many others have begun development or are considering doing so. Recognizing the need for definitive guidance on enterprise risk management, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and RIMS have developed conceptually sound frameworks providing integrated principles, and practical implementation guidance supporting the firms programs to develop or benchmark their enterprise risk management processes. Each describes an approach for identifying, analyzing, responding to, and monitoring risks or opportunities, within the internal and external environment facing the enterprise.

A Business Case for Enterprise Risk Management (ERM)	
Qualitative	Quantitative
Lower incidence of loss events	Increase management consensus on risks
Risk threshold helps identify opportunities	React faster and earlier to loss events
Tightly manage customer credit	Increase company credit rating (S&P)
Larger number of risk factors & active monitoring	Become a risk-management first mover
Reduced cost of risk management activities	Build overall shareholder value
Quantify market risks	Build predictability of company performance

A unified GRC's approach brings a high ROI for your ERM program

What does your organization consider to be the most important objectives and benefits of risk management?

Select up to three responses
(% respondents)



The Economist Intelligence Unit 2007

Figure 2: KPMG's Survey⁶

MetricStream: GRC's preeminence powers ERM across industry silos

MetricStream recently released a version 2.0 of the "Enterprise Compliance Map[®]" – through this map (which is only available as a folded road-map style hardcopy) we intend to portray ERM as the central covenant in a company's GRC program.

Our ERM solution is based on thought leadership & best-practices experiences work, where we've worked hand-in-hand with our customers to bring to bear some of the best practices that companies exhibit when it comes to managing ERM. This knowledge is represented in our vertical specific ERM solutions that power the GRC programs for several fortune 500 companies.

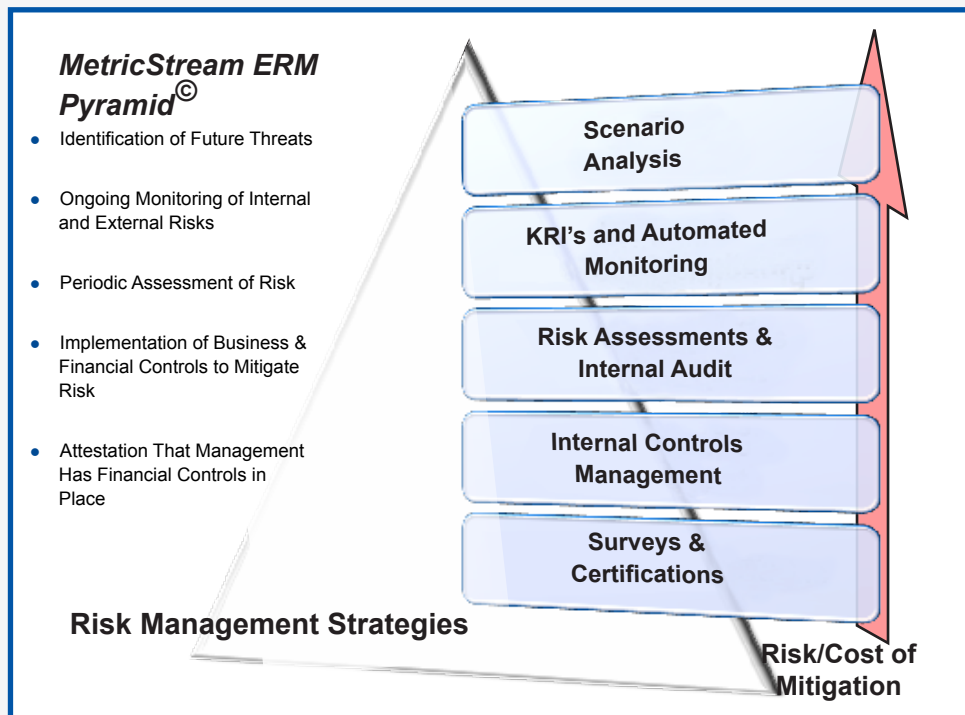
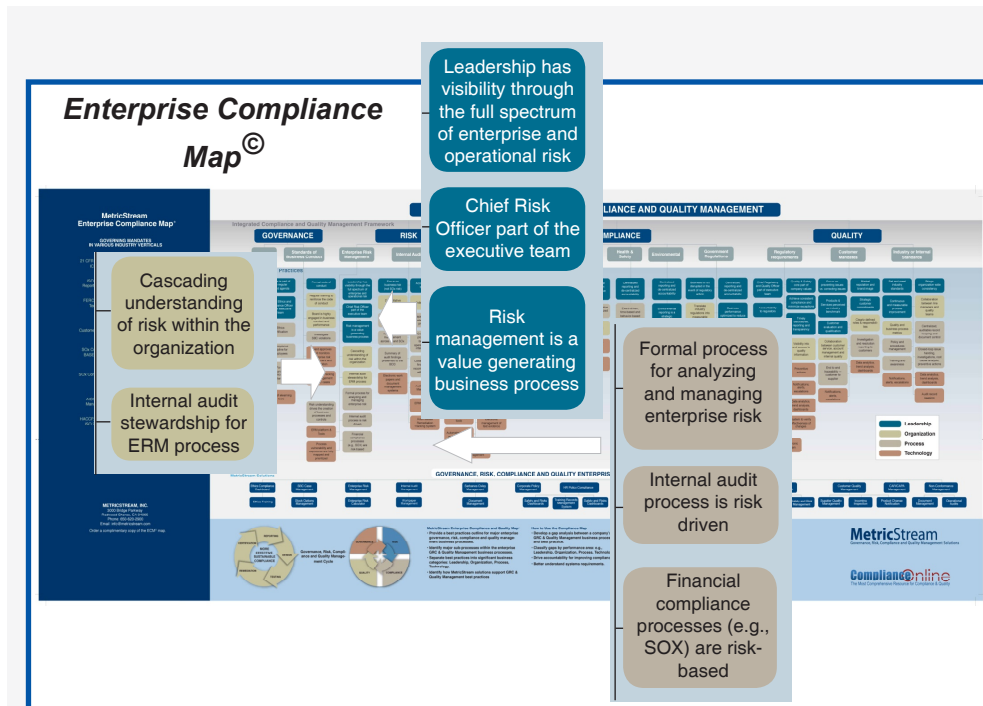
Enterprise Risk Management (ERM) methodology and tools empower the organization through careful structuring of risk assessment and by automating compliance efforts.

Regulatory Compliance Management

The MetricStream solution provides a common framework and an integrated approach to manage cross-industry mandates and regulations such as SOX, OSHA, EH&S and FCPA as well as the industry focused regulatory guidelines from AML, BASELII, FERC, NERC and Data Management laws.

Streamlined Risk Methodology

The MetricStream solution ensures that a formal procedure for analyzing and managing enterprise risk is implemented and followed. It identifies and documents potential threats and vulnerabilities, quantifies total cost of risk and compliance and drives the creation of business processes and controls. Its flexible scheduling tool allows the enterprise to assess, test and document controls. Prioritizing response strategies for optimal risk/reward outcomes is also easier to perform. The solution quantifies market risk for portfolios and ensures that the right risk methodology is followed.



Increased Protection

Organizations must adopt a strategic approach to risk management in order to ensure maximum protection from attacks. Process vulnerability and risk exposures are fully mapped by MetricStream and threats to the most critical assets are prioritized to set the right protection strategy for the organization. The underlying workflow and collaboration engine of MetricStream's solution determines the potential impact of threat occurrence and the existing level of risk to develop and implement a suitable corporate risk management and mitigation plan.

Efficient Controls

The MetricStream solution enables process owners to take direct responsibility for managing controls while auditors can focus on key compliance risks and project oversight. To eliminate risks from deviations in procedures, errors and redundant activities, compliance and controls can be made consistent across the enterprise using the centralized framework. It also helps avoid the danger of stringent and varied sanctions by encouraging employees across the enterprise to contribute information that pertains to reducing exposure to risk and improving safety, productivity and quality.

Cost Reduction

Automated information flows, assessments and testing, remediation assignments and time stamped audit trails reduce overall compliance and risk management costs. The solution helps avoid increased write-offs, losses and rising cost overlays while creating investment opportunities and improving performance.

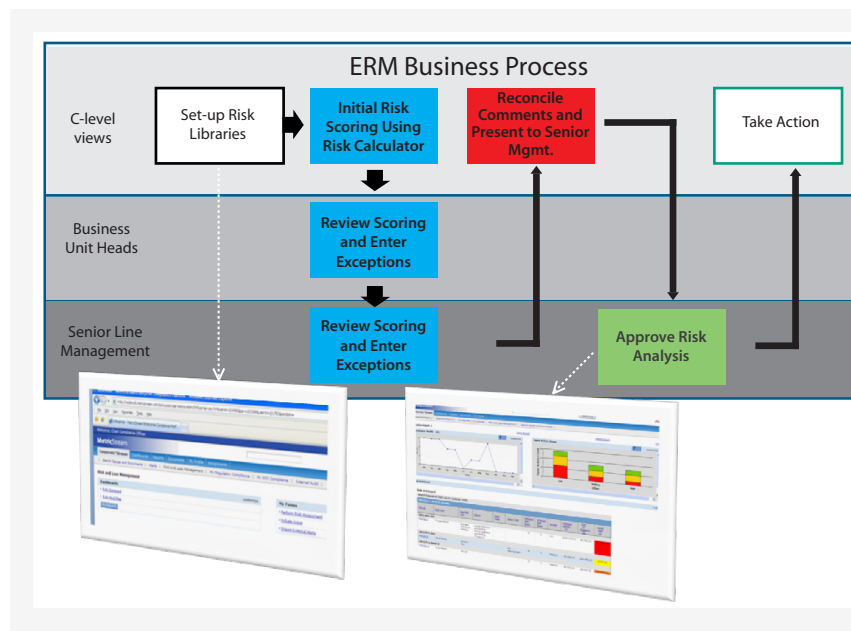
Web-based Reporting and Role-based Dashboards – Risk heat maps, graphical charts and compliance dashboards provide increased enterprise-wide transparency into the compliance process and highlight issues that need to be addressed. Continuous reporting and benchmarking of implemented procedures using control diagrams and scorecards ensures that risks are identified and resolved in real-time. Detailed and relevant risk data is automatically compiled by the MetricStream solution and drives internal audit, regulatory and financial compliance processes (e.g., FERC, NERC, SOX). Quarterly and monthly trending analysis, detailed reports and elaborative dashboards provide a bird's eye view of the risk scenario. Automated alerts help the risk managers foresee future challenges and manage risks better.

Integrated Document Management System –

MetricStream's integrated document management system with change control capabilities synchronizes compliance documentation and business processes, ensuring availability of data across the enterprise. When fully integrated with a company's daily compliance management activities, accurate tracking of risks and compliance efforts helps the company easily and effectively grow its business and strengthen its operations.

Structured Process for Sharing Confidential Information

– MetricStream's centralized document control system coupled with its rigorous data mapping process enables real time sharing of sensitive data among key stakeholders and support NERC CIP data loss prevention.



Closed-loop Issues Management – The MetricStream solution provides a robust issue and remediation management platform that enables companies to establish and follow mandates for managing nonconformance, adverse events, exceptions, failures, and process deviations. It is a comprehensive solution that enables companies to streamline the development and implementation of remediation and corrective action plans processes across the enterprise.

It provides end-to-end exception and change management capabilities to help companies capture problem data from anywhere in their operation, conduct investigation to determine the root cause, manage the entire preventive and corrective process, implement changes, and ensure that the issue is resolved effectively. Powerful analytics and reporting capability with graphical dashboards to track each case from initiation to closure, gives managers complete real-time visibility into the remediation process.

Conclusion

Many of the world's largest companies struggle with an ever changing risk profile in today's dynamic and disparate world. There have been hence tremendous losses in shareholder value over the recent year and the last decade. Many of these losses occurred due to failures in recognizing and managing diverse risks. Today, GRC based Enterprise Risk Management is a critical CEO and board agenda as regulatory authorities, government & quasi-government regulatory agencies and credit rating agencies view a company's ERM practices as a leading indicator of management ability to execute on the vision. To preserve value, companies need to go beyond managing risk management in silos to create an integrated, organization-wide GRC management function. Firms adopting such a comprehensive approach to GRC and ERM will have access to systems that would help them define an overall risk appetite and weigh critical interdependencies among different types of risks. Finally, ERM is as much about people and organizations as it's about business processes and information systems that are needed that are needed for real-time reports to apprise senior management and the board of directors of primary risks and opportunities. Leveraging ERM to implement a more comprehensive GRC based approach to their control environment will render the organization to be better placed to maximize shareholder value.

References:

- ERM still out of reach for many: By Stuart Fagg
<http://www.riskmanagementmagazine.com.au/articles/17/0c035617.asp>
- Excellence in Risk Management IV - An Annual Survey of Risk - The 360° View of Risk
http://searchdatamanagement.techtarget.com/news/article/0,289142,sid91_gci1308910,00.html
- Enterprise Risk Management in the United States A 2006 Report Card
<http://www.taxgovernanceinstitute.com/documents/TGI/3132007203018kpmg082560.pdf>
- ENTERPRISE RISK MANAGEMENT SURVEY, 2006
<http://www.rmahq.org/NR/rdonlyres/B9281EB1-8961-4C5A-B211-C0927C870451/0/ERMDistribute2Public.pdf>
- Best practice in risk management A function comes of age
http://www.kpmg.com.au/Portals/0/eiu_Risk_Management.pdf
- Enterprise Risk Management - The full picture by AON

About MetricStream

MetricStream is the leading provider of solutions for Governance, Risk, Compliance (GRC) and Quality Management. Organizations today need a systematic approach to defining and managing GRC initiatives and quality management programs through a sustainable and integrated process that is aligned with the corporate strategy instead of a series of unrelated tactical projects. MetricStream has enabled leading corporations in diverse industries to make the shift from isolated compliance initiatives and departmental silos of risk-related information to integrated enterprise-wide strategy for GRC and quality management.

MetricStream, Inc.

2600 E. Bayshore Road

Palo Alto, CA 94303

Phone: 650-620-2900

Fax: 650-632-1953

info@metricstream.com

Copyright © 2010 MetricStream. All rights reserved.

For More Information
about MetricStream GRC and Quality
Management Solutions
please visit www.metricstream.com