

Unified Governance, Risk and Compliance Framework

Blueprint for Delivering Business Performance



Preface

The evolution of capital markets, globalization and macroeconomic changes are not just increasing the challenges but also creating unprecedented opportunities for companies. Most enterprises today understand the importance of linking and managing risk alongside compliance initiatives and corporate governance issues. Better preparedness around Governance, Risk and Compliance (GRC) allows them to respond to and leverage domestic and global events and trends much faster. By putting a unified structure in place to manage GRC, enterprises can make decisions faster and feel more certain and informed, creating significant competitive leverage and unexpected benefits.

Table of Contents

Introduction	1
GRC Processes: State of the Corporation	2
Corporate Governance	2
Risk Management	3
Regulatory Compliance	5
GRC Roles and Responsibilities	6
Approches, Tool and Strategies: Delivering Business Performance	7
MetricStream's Industry-Leading GRC Framework	10
Summary	13

Introduction

Growing regulatory environment, higher business complexity, and increased focus on accountability are placing great responsibility on the management and demanding seamless operations. In this business environment, consistent and trustworthy information forms the cornerstone of strategic decision-making. Top management needs to get a comprehensive, up-to-date view of the corporate risk and compliance position. Executives and board members demand deeper insights into the governance, risk, and compliance related management practices. The “no mistakes” business climate has led enterprises to pursue a broad range of governance, risk and compliance initiatives across the organization. Although, risks are interdependent and controls are shared, they are planned and managed in silos, potentially increasing the overall business risk of the organization. In addition, parallel compliance and risk initiatives lead to duplication of efforts and cause costs to spiral out of control. Governance, risk, and compliance process through control, definition, enforcement, and monitoring has the ability to coordinate and integrate these initiatives.

This paper takes a detailed look at Governance, Risk and Compliance (GRC) – a value added principle becoming increasingly important to enterprises around the globe. It proceeds to discuss emerging perception of GRC as an integrated set of concepts that, when applied holistically within an organization can add significant value and provide competitive advantage.



The Governance, Risk and Compliance: State of the Corporation

A growing array of complex federal regulations, escalating pressure from financial markets, and increasing demands from stakeholders are fueling the convergence of the distinct, but interdependent disciplines of Governance, Risk, and Compliance (GRC). The span of most Governance, Risk, and Compliance initiatives is broad and is inclusive of:

Corporate Governance

The governance process within an organization defines and communicates corporate control, key policies, enterprise risk management, regulatory and compliance management, and oversight (e.g. compliance with ethics and options compliance as well as overall oversight of regulatory issues), and evaluates business performance through balanced scorecards, risk scorecards and operational dashboards.

Risk Philosophy and Appetite

Corporate Governance lays down risk philosophy for the company- defining risk appetite, rationalizing and monitoring risks, and identifying core business areas where the company is willing to retain risks to generate targeted returns. It streamlines the decision making process, thereby ensuring integrity of financial reports, and finally providing a degree of confidence necessary for proper functioning of an organization.

Business Ethics and Compliance

With words such as 'quality' and 'business excellence' becoming an integral part of the management vocabulary, the implementation of corporate ethical culture and policies has become indispensable for corporate governance.

Corporate Policy Compliance

Corporate Governance manages the strategic directives, board compliance capabilities such as options policy compliance, ethics and policy compliance. It optimizes business operations and ensures compliance by centrally monitoring key controls for business processes and cross-enterprise functionalities.

According to a recent note from Gartner, "For Sarbanes-Oxley, we put the burden on a global Bank at about 0.2 percent to 0.4 percent on EBITDA. So if the Securities and Exchange Commission is one of 370 regulators for a global bank - to approach each regulatory program individually would eat up all the profits. Lots of companies have separate compliance programs for every regulatory regime. As regulatory regimes proliferate, a comprehensive compliance program keeps regulations from depressing earnings."

An integrated Governance, Risk and Compliance approach enables an organization to integrate and streamline these individual compliance initiatives, so it can significantly reduce the cost of compliance.

In a survey of Senior Executives of US based industrial manufacturing units, 65% of those surveyed agree that their current ERM programs help their organization be more successful. Additionally, two-thirds (67 percent) feel that a more efficiently run ERM program would help their organization remain competitive.

Source: <http://www.pwc.com>

Business Performance Reporting

Business Performance Reporting such as balanced scorecards, risk scorecards, and operational controls dashboards keep boards informed about matters related to performance, compliance and risk. This caters to the quest of the top management –insight into the company's situation with respect to operations across entire value chain, employees, customers, vendors, strategic partners, government and regulatory agencies, analysts, investors and the general public.

Policy and Procedure Management

Policy and Procedure Management offers the ability to enforce enterprise-wide access to policies and involves documentation of corporate policies and guidelines and their respective enforcement and compliance. This requires a robust mechanism that manages life cycles communication, training, and awareness tied to compliance, risks and controls.

Corporate Social Responsibility

As the requirements for Corporate Social Responsibility and sustainable growth become progressively more demanding in terms of their degree of transparency, reliability and ability to be audited, enterprises are taking up CRS initiatives as a part of corporate governance to establish the infrastructure – resources, budgets, planning, IT support - to support them as ongoing enterprise wide programs.

Risk Management

Recent jump in regulatory mandates and increasingly activist shareholders have sensitized many organizations to identify and manage areas of risk in their business: be it financial, operational, IT, brand or reputation related risk. These risks are no longer considered the sole responsibility of specialists and executives. Boards demand visibility into exposure and status so they can effectively manage the organization's long-term strategies. As a result, companies are looking to identify, measure, prioritize, and mitigate all types of risk in the business through proactive risk management process. A comprehensive risk management program includes:

Risk Identification

The scope of risk management has been broadened; the goal of a corporate risk manager today is not just managing a predetermined set of exposures of the enterprise, but also performing necessary walkthroughs, asking the right questions at the right time, observing key risk management components, assigning appropriate personnel at all levels, and promoting strengthened governance.

Planning: Building the foundation for a successful risk assessment.

Data gathering: Collecting risk information through facilitated risk discussions

Risk Analysis

Risk analysis assesses risk's probability, severity, and impact. Teams determine how to address the key risks in the most effective and cost efficient manner; by identifying controls, estimating costs, assessing the degree of risk reduction, and then determining which controls to implement. The output of this process is a clear and actionable plan to control or accept each of the top risks identified in the Risk Identification phase.

Risk Matrix: Risk Matrix enables risk managers to categorize risks- into the ones that require action as well as those which are acceptable. Based on their ranking, they can plot each risk on the risk matrix in the appropriate area (i.e., high, medium or low impact and high, medium or low likelihood). The graph indicates which risks are acceptable, which may require action, and which require immediate action.

Implementation

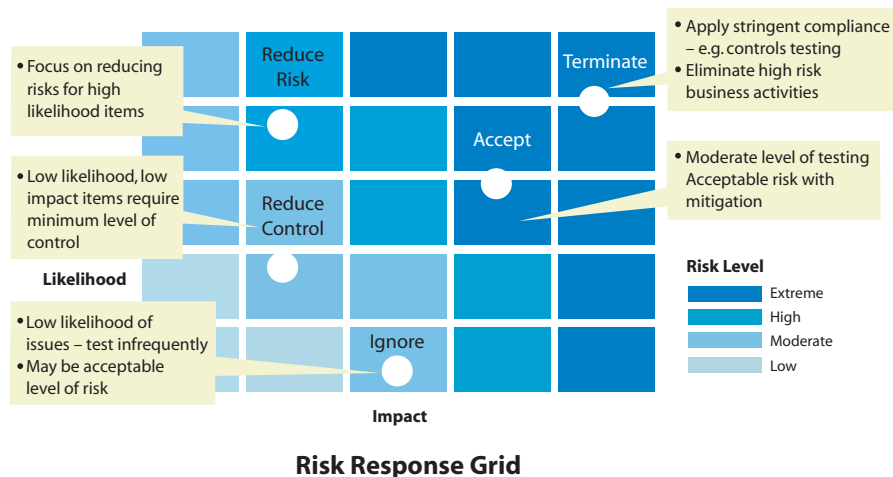
During the implementation process, the correct treatment for each risk is chosen and implemented. The risk managers create and execute plans based on the list of control solutions that emerge during the decision support process, and deploy the requisite tools, processes and the framework. The process is implemented all through the project cycle - from the inception of the idea to project formulation to project closure.

Verification

When the first three processes of the risk analysis are complete, organizations should estimate their progress with regard to risk management as a whole. Verification introduces the concept of a "Risk Scorecard". Implementation efficiency is measured using key performance indicators (KPIs) like percentage of revenues saved due to early mitigation of risks, revenue increase due to innovation in risk management and risk exposure amount as against the total project value.

Monitoring

Monitoring involves repeating above mentioned processes regularly and keeping the risk information up-to-date. It is critical to optimize a risk management strategy as it verifies existing processes, implements corrective action plans and streamlines the remediation workflow.



Types of Risks

Financial Risk: Unpredictable exchange rates, interest rates and commodity prices not only affect a firm’s profits earnings but also its survival. Market risks like Interest-rate risk, equity price risk and foreign exchange risk often hit the bottom line of an organization. Further risks of lowered credit rating exert added pressures on the CROs and the CFOs.

Operational Risk: Operational risk like project delivery risks, capex pitfalls, and fraud can be perpetrated by any factor –lack of prudent methodology to monitor projects and processes, an internal employee manipulating internal control environment of an organization or an external counterparty.

Technology Risks:With organizations becoming far more reliant on computers, networks and electronic data to run mission-critical elements of their operations, risks surrounding IT, such as network failure, lack of resources and skills, hacking and viruses, and poor system integration, have the potential to have a greater negative impact on an organization than in the past.

Business Continuity Risks: Increasing threats, both man-made and natural, incredibly rapid technological evolution, new business concepts and processes, a global economy, and an increasing stakeholder awareness have made business continuity truly a professional discipline and not just an unavoidable task to satisfy auditors and regulators. With growing maturity of the business continuity and risk management cultures, audit and compliance issues are firmly embedded in the overall approach toward risk and, most importantly, corporate governance.

Industry Specific Risks

Pharmacovigilance Risks and Drug Safety: Driven by a growing interest amongst regulators, consumers and the medical community, drug safety and pharmacovigilance risk management has risen dramatically in both importance and visibility over recent years.

Supply Chain Risk: Low-cost country sourcing, multi-tiered supplier networks and business process outsourcing are among the supply chain initiatives that companies, large and small, have employed. As a result of trends and developments within supply chain, organizations continually face new or changing uncertainties.

Food Safety Risk: Leading food companies are realizing the repercussions of a food safety problem - in dollars and customer and consumer confidence. To help prevent the problem, advanced risk management solutions to address increasing food safety issues and new bio-security challenges are being implemented.

Utilities Risks: Utilities continue to be affected by higher energy prices, continued focus on deregulation, and the economic impact of unsuccessful business alliances and mergers. To conform to regulatory actions and adapt to changing consumer demographics, most enterprises in utilities sector are following strategic risk management policies.

Finance & Banking: Financial and Banking institutes are subjected to a wide array of risks in course of their operations. Risks like liquidity, credit and solvency risks can result in loss to the financial institutes. Risks emanating from macroeconomic and policy reforms, and legal and regulatory factors can jeopardize any financial institution’s operations.

Regulatory Compliance

As companies race to meet regulatory deadlines, the initiatives to comply with regulations typically begin as a project. These projects consume significant resources as meeting the deadline becomes the most important objective. However, compliance is not a one-time event – organizations realize that they need to make it into a repeatable process, so that they can continue to sustain compliance with that regulation at a lower cost than for the first deadline. When an organization is dealing with multiple regulations at the same time, a streamlined process of managing compliance with each of these initiatives is critical, or else, costs can spiral out of control and the risk of non-compliance also increases. The compliance process enables organizations to make compliance repeatable and hence enables them to sustain it on an ongoing basis at a lower cost.

Document and Process Management

Most enterprises require their Chief Compliance Officers to follow the process of Risk Documentation which gathers, records, reports, and maintains pertinent information needed to ensure successful risk management. The examples of information include risk management plans, lists of identified risks, risk assessment reports, handling methods and techniques, and metrics for monitoring risks.

Define and Document Controls

Chief Compliance Officers (CCOs) define and document control activities occur throughout the organization, at all levels and in all functions- approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Monitoring Controls

Control systems need to be monitored--a process that assesses the quality of the enterprise's performance over time. This is accomplished through ongoing monitoring activities, and evaluations.

Disclosure and Certification

In GRC's parlance disclosure and certification are the benchmark settings that endorse adherence to requisite compliance and quality mandates. CCOs often rely on certificates and endorsement by the managers and CIOs, as it increases accountability across the processes.

Today's Regulatory Compliance Scenario

Complex and changing regulations form a growing pressure for compliance officers who are grappling with regulatory information overload. Non-compliance involves stiff financial penalties as well as potential criminal charges.

Finance & Banking

Regulatory constraints on business activities and higher capital requirements, credit risks and money-laundering activities have resulted in ad hoc development of risk management processes. Adhering to the SOX, Basel II, Bank Secrecy Act, and Anti-Money-Laundering (BSA/AML) compliance requires precautionary measures and identification of BSA/AML risk and deficiencies in various areas of business.

IT Compliance

International regulations such as SOX, COSO/COBIT, ITIL and ISO 17799 have added to the pressure on organizations engaged in the competitive globalized IT landscape. Organizations unwary of state-wide laws such as California's Database Security Breach Disclosure Law risk exposure of in-house controversies, as well as penalties in the form of prohibition and injunctions.

Healthcare and Life Sciences

Any company involved in life sciences and health care faces inherent risks, based on the products' functions and markets. Stringent regulations and guidelines from FDA, HIPAA, etc., strive to reduce the risks for both the patients and the companies.

Energy & Utilities

Accidents and injuries, fatalities, losses to plant and equipment, spillages and other loss of product and materials plague the energy industry. Optimizing generation plant usage, delivery schedules, natural gas and electricity selling prices, deliveries, oil pipeline usage and cash flows all in a real time, is a formidable task. Moreover, stringent compliance and regulatory requirements, like SOX, FERC and NERC regulations, from state and regional public service commissions add to the woes of energy risk managers.

General Manufacturing

Manufacturers across a wide range of industries face many common challenges in their efforts to meet

rising quality standards. Many organizations are deploying quality management methodologies such as Six Sigma and ISO 9000. Further Sarbanes-Oxley Act (SOX) mandates a stricter governance model and tighter internal controls.

Food and Beverage Industry

Mandates by the FDA and the USDA such as HACCP procedures and ISO 22000-based food safety management systems are the basis for many quality and compliance programs in the food and beverage industry. Improperly trained employees, substandard products, or poor service can cost millions of dollars a year in lost sales and leave the door open to more severe consequences.

enterprise compliance are quite similar, it follows that the CFO could provide leadership in the area of company wide financial compliance and SOX certification.

Chief Compliance Officer

Compliance Managers are entrusted with ensuring that the organization has the processes and controls to meet the requirements imposed by governmental bodies, regulators, industry mandates like Anti-Money Laundering, Foreign Corrupt Practices Act, cGMP, GLBA or internal policies. However, as the multiple compliance initiatives become more intertwined from regulatory and organizational perspectives, Chief Compliance Officers are also focusing on effective rationalization of controls to provide a clear, unambiguous process for compliance management and to



GRC Roles and Responsibilities

A successful GRC program integrates into the company culture, ethics, and principles. Compliance isn't just about rules; it is about behavior. Professionals at various levels of the enterprise, like chief risk and compliance officer, have become an important nexus of GRC insight across the organization. Let us give a look at few executive roles that are usually considered by organization to take up the challenge to maintain world-class GRC program across the organization:

Chief Financial Officer

Financial reporting, performance management, budgeting, and other financial processes provide the CFO detailed insight into the workings of virtually every business, division and department within the company. Further, as the advantages and potential pitfalls of managing the financial processes and

deliver a single point of reference for the organization.

Chief Risk Officer

Risk Managers' role has evolved from that of managing a predetermined set of risk exposures to identifying core business areas where the company should be willing to retain risks to seize growth opportunities and generate returns for investors. This ties risk management to business performance and changes the risk management from an exclusive centralized function to a federated, top-down approach aligned centrally with business objectives and reporting and assessments are distributed to lines of business for ownership, execution and accountability. By managing risk appetite and response to risks, Chief Risk Officers drive organizational behavior today.

Chief Audit Officer

Audit Managers are accountable for monitoring risks and ensure compliance across organizational silos and the role is evolving into an independent and horizontal function. This requires a common framework for all types of audits – financial, risk, operations, internal, suppliers, and compliance – such that auditing priorities are determined by an enterprise-level risk-based approach and not departmental and tactical imperatives.

Chief Quality Officer

Combination of product proliferation, outsourced manufacturing operations, a stringent regulatory environment and rigorous customer requirements is driving Quality Managers to proactively manage their quality processes. Quality Managers are leveraging best practices that call for integrated processes for compliance with internal quality standards and policies and industry mandates like TS 16949, ISO 13485, and ISO 22000, Six Sigma, and TQM.

Chief Information Officer

With IT governance and compliance process becoming inclusive of multiple internal and external stakeholders, organizations are increasingly adopting an integrated IT governance framework, which ensures information and systems integrity, data security and privacy, and compliance to quality mandates like COBIT, ISO 17799/27002, ITIL, SAS 70, etc..

Chief Legal Officer

Cultivating a culture of compliance and maintaining a high level of integrity among employees are growing challenges today due to greater regulatory oversight and investor activism. Legal Counsels help employee employees to adopt policies and procedures, follow the code of ethics, and adhere to principles of corporate governance.

Chief HR Officer

Providing guidelines, monitoring processes and providing constant access to information, rigorous training and awareness programs on compliance and ethics is proving essential to ensure effective implementation of governance programs. Most HR managers provide an integrated training platform to ensure compliance with HR policies and procedures, compliance with governmental health and safety regulations, and compliance training and certification.

Approches, Tool and Strategies: Delivering Business Performance

New definitions, requirements and standards are emerging – from both internal and external sources – forcing boards and managers to adopt an integrated approach to GRC as a business enabler and value driver, and follow GRC principles. Amidst this dynamic environment, profitable companies are employing a variety of tools and strategies to succeed in the marketplace. Regardless of the solution they employ, most companies share a common mantra- its corporate policies must support its business strategy.

This is a key element of corporate governance – using corporate policies to underpin strategy execution. Below we are providing a broad overview of the approaches, strategies and tools that can be used to leverage GRC initiatives within an enterprise:

Audit Management

Auditing is evolving into an independent and horizontal function to monitor risks and non compliance across the entire value chain. By virtue of its understanding of the organization and its culture, operations, and risk profile, an internal audit (IA) function enables the board and audit committee to evaluate the performance of GRC practices. Effective corporate governance, risk and compliance management drives the need for a common framework for all types of audits in organizations - financial, risk, operations, internal, suppliers, compliance, etc. The objectivity, skills, and knowledge of competent internal auditors can contribute to the effectiveness of an organization's internal control, risk management, and related governance processes.

Reporting and Visualization

Information flows within an organization play a key role in establishing and maintaining an effective operational risk framework. The development of good reporting format will greatly enhance the risk manager's ability to gain the necessary insight into the potential risks. The Governance, Risk and Compliance function should monitor and report its measures of risks to appropriate levels of senior management and to the board of directors. Accordingly, an accurate, informative and timely management information system is an important factor in the overall effectiveness of the risk management process.

Corporate Risk Database

The pivotal component of a holistic Governance, Risk and Compliance process is the corporate risk database- aggregate recording and reporting system that captures key risks and ensures existing controls are complemented by management action to provide a reasonable chance of success. The database has inputs from all levels of employees – from senior managers to work teams, as they attempt to assess and deal with risk in their area of working. It is the risk register that underpins the board's view on internal controls.

Risk Analytics

An ideal risk management process ensures that organizational behavior is driven by its risk appetite. With a formal risk analysis, risk managers add versatility to the way the enterprise addresses varied risks – currency, supply chain, safety; and map them successfully to compliance (regulatory or internal).

Quantitative Risk Analysis where risks are prioritized according to their potential impact on project objectives, analyzing their effect, and assigning a numerical rating to those risks. For example, Monte Carlo simulation uses a mathematical method to approximate the distribution of potential results based on probabilistic inputs.

Qualitative Risk Analysis where managers assess the impact and likelihood of identified risks in qualitative terms like severe, very high, high, moderate low etc. and measured against a risk impact scale constructed using ordinal (very high, high, low... etc) or cardinal scales (0.1, 0.2, 0.3 ... etc).

Enterprise Risk Calculator

An Enterprise Risk Calculator indicates areas where risks and potential losses exist, such as the rate of expansion and the level of internal competition. Using the risk calculator, managers can determine if their company has a safe or dangerous amount of risk. The risk calculator measures three kinds of internal pressures: risk stemming from growth, corporate culture, and information management; helping gain consensus for risk factors across the organization and develop effective strategies for lowering risk.

Risk Heat Maps

One way of gaining a transparent and integrated view is to use a heat map - a simple diagram showing the risks (broken down by risk category and amount) each business unit bears and an overall view of the corporate earnings at risk. The heat map tags exposures in different colors to highlight the greatest risk concen-

trations; e.g. red might indicate that a business unit's risk accounted for more than 10 percent of a company's overall capital, green for more than 5 percent. To make risks transparent--and to draw up an accurate heat map--companies need an effective system for reporting risk.

Top Down Structure

In a top-down approach, the risk manager identifies the potential risks in a sequential manner, starting with company-level operations, and then drilling down to significant sub system level and relevant individual controls at the process, transaction, or application levels. The top-down approach enables the risk manager to focus early in the process on matters that may have a subsequent effect.

Remediation Management

After a comprehensive risk analysis, managers will be able to pin down the potential risks, and the ways to correct them. Effective remediation management of quality, compliance and risk related issues is essential for a closed loop, continuous improvement process - providing end-to-end exception and change management capabilities to help companies capture problem data from anywhere in their operation, conducting investigation to determine the root cause, managing the entire preventive and corrective process, implementing changes, and ensuring 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. An efficient remediation management system ensures faster resolution of the issues, and streamlines the development and implementation of remediation and corrective action plans processes across the enterprise.

Central GRC Repository

By consolidating their risk repositories, top management can obtain an enterprise-wide view of Governance, Risk and Compliance. It correlates and aligns governance initiative information, risk intelligence, and compliance management information from every department. It streamlines Governance, Risk and Compliance processes, by letting risk managers monitor all controls, technology frameworks, business processes, and applications across the organization. It is reusable, and maps risks and controls to multiple enterprise initiatives. The benefits of a centralized repository are significant – when in place it helps

avoid fragmentation of Governance, Risk, and Compliance information ensures consistency in risk approach, enables greater understanding of Governance, Risk, and Compliance processes in every department, and reduces wasted time and money associated with redundant efforts and technical resources.

Threshold-based Notifications and Alerts

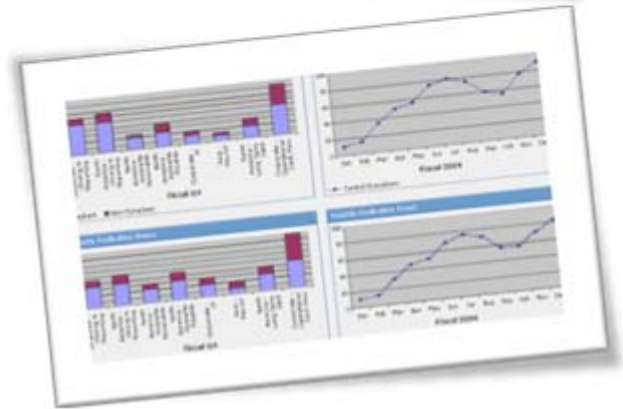
Email notifications are automatically generated according to pre-determined assessment schedules, and sent to risk owners as reviews fall due. Risk owners simply follow a link in the email through to leaders where they complete their review.

Program Dashboards

A risk dashboard can highlight the highest risk areas concisely and help develop an integrated approach to reducing risk exposure. It provides executives with a personalized real-time view of risk position and controls via intuitive graphs and charts.

Ethics and Compliance Training Program

A robust accountability structure combats corporate malfeasance. Companies looking to develop responsible, cost-efficient and effective compliance processes are establishing an accountability structure that ensures exhaustive oversight and process ownership, and also that an appropriate ethical attitude pervades the organization. To clearly define lines of accountability, many companies have redesigned their organizational structures to include compliance as part of the wider risk function for example, “regulatory risk management.” Responsibilities of other executives, such as the ethics officer (EO) have also been clarified to strengthen accountability in response to SOX and other governance regulations. Further, most enterprises requires employees in high-risk job functions — such as business development, marketing and finance — to participate in more frequent and comprehensive training.



Perform Risk Assessment
Fields marked with a red asterisk are required.

Risk Classification
RAM (Checklist) ID: RAM-ID-5
Risk Type: Issue Based Risk
Regulatory/Compliance Requirement: Investment Management

Organization Unit
Research and Development - C
Risk Factor: Internal Audit High Risk Issues
Risk Component: Proprietary capital - market ma

Issue ID
MS-CI-2007-00065
Issue Type: NASD Process
Inherent Score: 3

Comments
Risk assessment for
Risk : General ledger may not balance
Risk : All transactions, reclasses, adjustments and Elimination entries

Overall Calculated Risk Score: 28
Overall Adjusted Risk Factor: 12

Financial Risk	Operational Risk	Political Risk	Environmental Risk	Competitive Risk	
Financial Risk	Likelihood	Impact	Calculated Risk Score (based on Likelihood/Impact Scoring)	Weighting Factor (%)	Adjusted Risk Factor (Calculated)
Write-offs	High	Low	6	25	1.5
Margin Decline	Low	Low	2	50	1
Operating cost increase	High	High	10	75	7.5
Fraud	High	Medium	8	25	2
Changes in historical procurement patterns	Low	Low	2	10	0.2
Sub Total (Calculated Risk Score) - Financial Risk			28		
Sub Total (Adjusted Risk Factor) - Financial Risk					12.2

Buttons: Save, Save & Close, Submit, Cancel

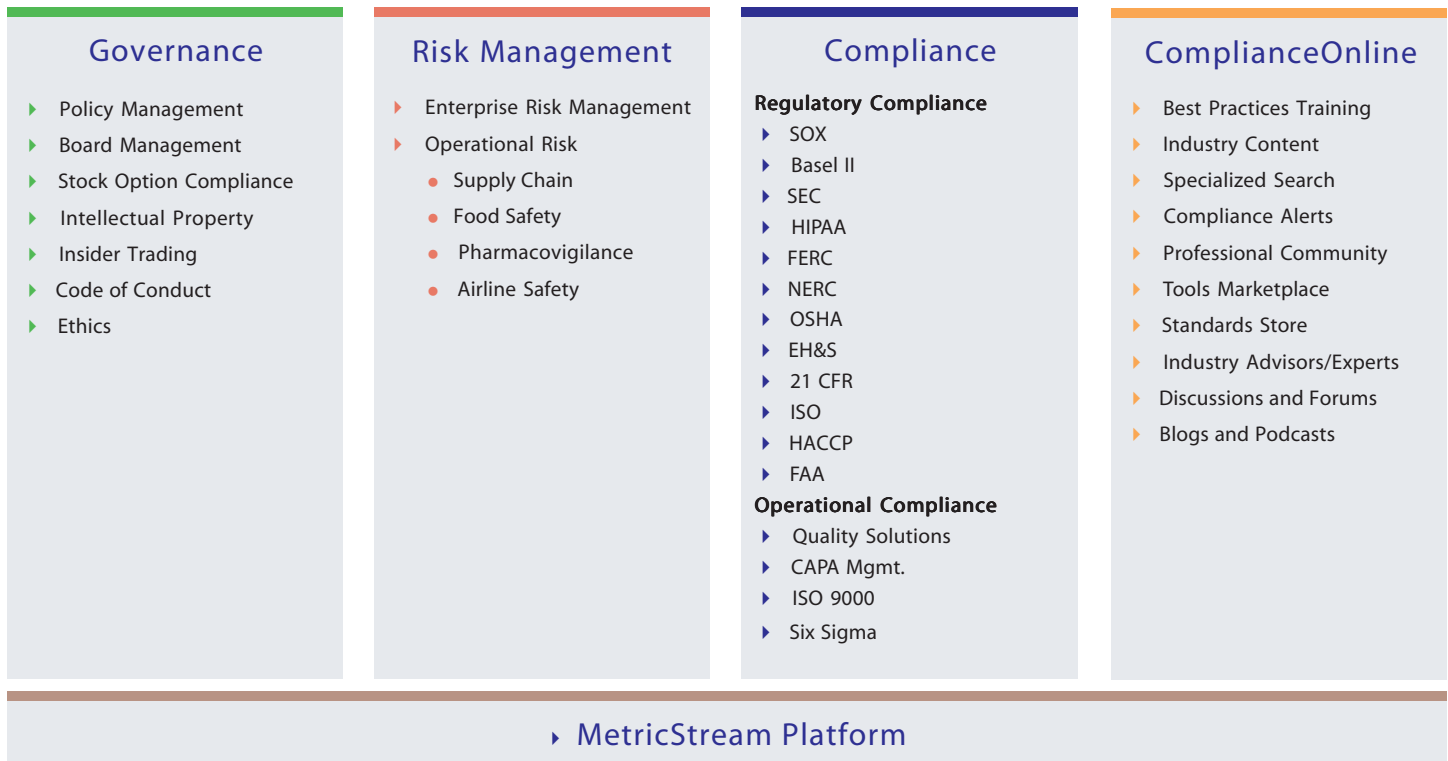
MetricStream's Industry-Leading GRC Framework

MetricStream solutions are uniquely designed to support the integrated Governance, Risk, and Compliance framework. The MetricStream Compliance Platform becomes the nucleus of a corporate governance ecosystem, coordinating all governance, risk and compliance activities throughout the enterprise via a single management system.

provides corporate ethics compliance solutions to organizations to continually audit their internal controls and validate compliance with corporate ethics policies and ensure that they have a mechanism to identify gaps and deficiencies as well as remedy them in a timely manner.

As a part of Corporate Governance solution, MetricStream enables organizations to continually audit their stock option grant processes and assess

MetricStream GRC Dashboard and Scorecard



MetricStream delivers the most comprehensive mapping of the Governance, Risk, and Compliance framework within the industry with the following unique capabilities:

Corporate Governance Solution

MetricStream uniquely combines software and content to deliver corporate governance solutions with embedded best practices templates, access to training content from an expert community, and integration of business processes with regulatory notifications and industry alerts.

MetricStream provides a flexible framework to streamline business ethics programs, and ensure business ethics compliance across an enterprise. It

internal controls to identify risks and validate compliance with SEC requirements as well as the board compensation committee policies.

MetricStream provides a flexible framework to streamline creation and management of corporate policies and procedures and supports implementation of programs for accountability and communication. The corporate policy compliance software solution supports policy documentation, change management, communication and awareness programs and training management. It also provides powerful tools for monitoring and documenting compliance through periodic audits, surveys and self-assessments.

Regulatory Compliance Management

MetricStream Compliance Management solution provides a common framework and an integrated approach to manage all compliance requirements faced by an organization. With automated information flows, assessments and testing, and remediation assignments, MetricStream solutions ensure consistent compliance and controls process across the enterprise eliminating any deviations and errors as well as redundant activities, and reduced over-all compliance costs. The solution also features compliance dashboards and risk heat maps; that provide enterprise-wide visibility into the compliance management process to keep the compliance and business processes in sync. It also caters to the requirements of industry standard quality management methodologies such as ISO 9000, cGMPs, and Six Sigma.

MetricStream enables companies to manage cross-industry mandates and regulations such as SOX, OSHA, EH&S, and FCPA as well as the industry focused regulatory guidelines from FDA, FERC, NERC, FAA, HACCP, COSO/COBIT, ITIL, ISO 17799, AML, Basel II and Data Retention laws.

Enterprise Risk Management Framework

Enterprise Risk Management (ERM) solution from MetricStream enables organizations to identify, assess, quantify, monitor, and manage their enterprise risk in an integrated manner. It brings together all risk management related data - automated alerts, data feeds, risk libraries, risk analytics, key risk indicators, risk heat maps, graphical and trend 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. MetricStream uniquely combines software and content to deliver Enterprise Risk Management software solution to customers. Embedded best practices content helps define the scope of processes and sub-processes for which risk management needs to be performed and guides development of control and test libraries. It also provides other intelligent and content driven features such access to training content from an expert community from within the solutions and integration of business processes with regulatory notifications and industry alerts.

Integrated Document Management System

MetricStream's seamless and integrated document management 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 management activities, accurate tracking of risks helps the company to easily and effectively grow its business and strengthen its operations.

Internal Audit Management

MetricStream's solution provides an integrated audit management that supports all auditing based activities in an organization - managing audit schedules, auditing work papers, conducting ad-hoc audits, documenting audit findings, drafting audit reports and recommendations, summarizing audit findings and presenting the same to the top management. MetricStream solution maintains a repository of audits compliant with regulations and industry standards. The value generated is in form of accountability and compliance drive across organizational silos.

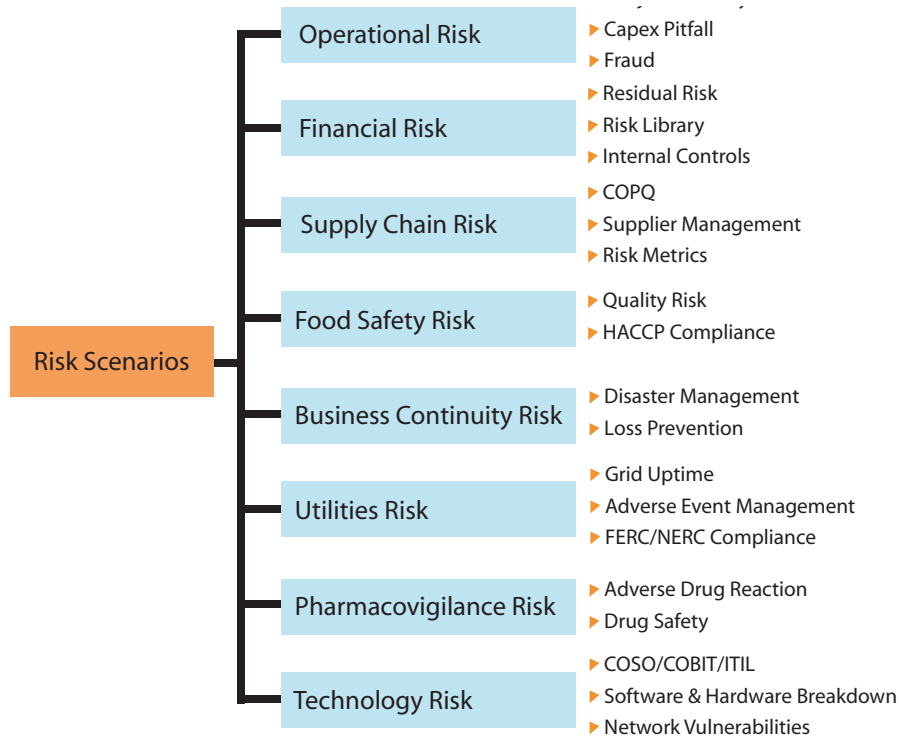
Structured Process for Sharing Confidential Information

MetricStream's centralized document management system coupled with its rigorous data mapping process enables real time sharing of sensitive data among key stakeholders, and prevents data loss.

Closed-loop Issues Management

MetricStream's solution provides a robust issue management platform that enables companies to establish and follow mandates for managing nonconformance, adverse events, exceptions, failures, and process deviations. This comprehensive solution enables companies to streamline the development and implementation of remediation and corrective action plans across the enterprise.

It provides end to end exception and change management capabilities to help the risk manager capture problem data anywhere in the operations, conduct investigations to determine the root causes, 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 the manager complete real time visibility into the remediation process.



MetricStream’s Best-in-class GRC Solution

Rich corporate governance capabilities

- Enterprise risk management framework
- Risk, compliance and governance scorecards and dashboards
- End-to-end compliance process for stock option policies, internal policies, etc.

Central repository of all corporate policies, change management and mechanism for communication

- Comprehensive risk management features including
- Documentation of all risks in a central repository through integrated document management
- Risk identification from surveys and events and categorization
- Risk assessment and calculation
- Risk prioritization using heat maps
- Remediation workflow

Extensive multi-regulatory compliance capabilities

- Support for multiple compliance frameworks such as COSO and COBIT
- Ability to create a comprehensive risk based controls framework
- Comprehensive controls testing capabilities such as inspections, audits, manual and automated assessments
- Flexible scheduling of testing of controls
- Rich workflow for remediation, certification and disclosure

Summary

Many organizations find themselves managing their Governance, Risk and Compliance (GRC) initiatives in silos. However as the multiple risk and compliance initiatives become more intertwined from regulatory and organizational perspectives, manifold systems cause confusion due to duplicative and contradictory processes and documentation, resulting in increased business risk. In addition the redundancy of work, as well as sheer expense of maintaining multiple point software solutions causes the cost of compliance and risk management to increase significantly.

To address above requirements, forward-thinking organizations are taking a broader, more integrated approach. Essentially, this approach is an evolution toward an integrated program of governance, risk, and compliance (GRC) management- a value-adding principle that is being embraced by an ever-growing number of leading organizations throughout the global business community. By taking an integrated GRC process approach and deploying a single system that supports a federated organizational approach to managing the multiple GRC initiatives, compliance effectiveness can be increased while cost of compliance is reduced. With an integrated GRC framework, GRC initiatives are aligned centrally with corporate governance and reporting but are distributed to lines of business to assign ownership, execution and accountability. Such an approach results in a dramatic and positive impact on organizational effectiveness by providing a clear, unambiguous process and a single point of reference for the organization.



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.

3000 Bridge Parkway
Redwood Shores CA 94065

Phone: 650-620-2900

Fax: 650-632-1953

info@metricstream.com

Copyrights © 2008. MetricStream. All rights reserved

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