

## Visibility and Value: The Evolution of Operational Compliance and Quality into Enterprise Risk Management

In an increasingly regulated market, organizations are searching for ways to streamline compliance activities and functions. However, as the sophistication of GRC solutions grow, organizations are seeking to integrate external compliance practices with internal policies and quality controls to integrate regulatory compliance with operational guidelines to improve the timeliness and quality of deliverables and effectively manage risk. Analyzing data collected from over 800 global organizations compiled for Aberdeen Group's February 2008 study, *GRC Strategic Agenda: The Value Proposition of Governance, Risk, and Compliance*, this Analyst Insight details the evolution of operational compliance and quality assurance to streamline processes and optimize a holistic Enterprise Risk Management (ERM) program.

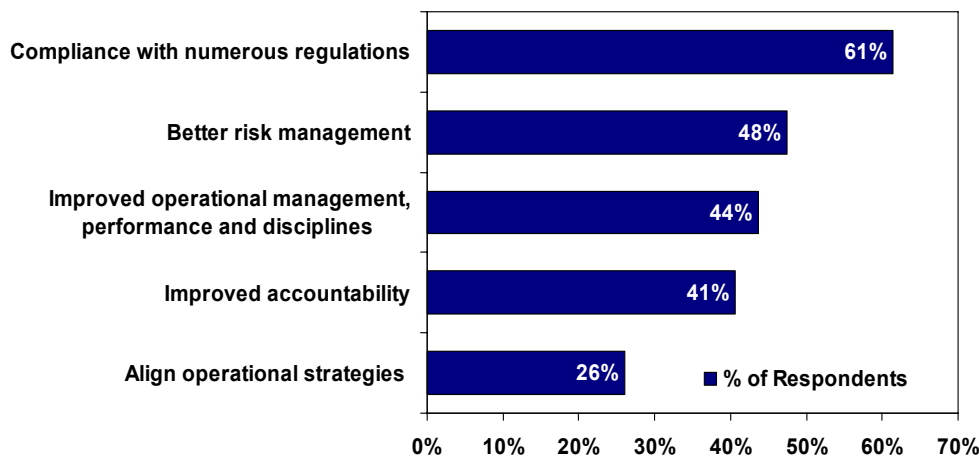
### Analyst Insight

Aberdeen's Insights provide the analyst perspective of the research as drawn from an aggregated view of the research surveys, interviews, and data analysis

### The Importance of Compliance

The large and continually growing number of cross-industry mandates, governmental regulations, and industry-specific regulatory guidelines is forcing organizations (particularly those competing in multi-regulatory environments) to re-think how compliance issues are managed. Aberdeen's recent GRC report reveals the need to achieve compliance with numerous regulations is the primary factor driving organizations to invest in GRC solutions (Figure 1).

**Figure 1: Top Two Reasons Organizations Are Investing in GRC**



Source: Aberdeen Group, May 2008

Especially relevant in multi-regulatory industries, the ability to streamline and automate manual processes, provide scalability sufficient to ensure compliance with existing and new regulations, and effectively share and enforce internal best-practices to consistently deliver high-quality services and / or products is essential to garner the greatest benefits from an Enterprise Risk Management (ERM) program. The unveiling of the new release of MetricStream's Compliance Management solution, designed to manage compliance with multiple regulations, is one example of a common framework that can be leveraged to not only meet outside regulations, but also incorporate internal policies and quality controls to provide a clearer picture of an organization's overall risk level.

The end user community's continually increasing demand for, and interest in, GRC solutions is based on the premise that such solutions offer organizations the ability to not only achieve regulatory compliance, but also mitigate and manage operational and business risks. Further highlighting the interconnection between compliance and risk management, Aberdeen's February report found that the top two factors driving organizations to focus resources on security and risk management initiatives are the need to comply with government regulations (61%) and the desire to protect the organization and its brand (42%). The vast and detrimental potential impact on corporate reputation, brand value, and, ultimately, shareholder value reinforces the importance of investing in solutions that ensure that an organization's assets, information, and data are both secure and compliant.

## Reducing Risk through Quality Assurance

Increasing global competition and regulatory pressures are forcing organizations to view risk management and compliance on a federated, enterprise-wide scale. Traditionally concerned with departmental, geographical, or product-specific quality management, executive management in charge of quality, compliance, and operations are increasingly focusing on how quality defects can result in non-compliance with regulations formerly outside of their purview, and, more importantly, the substantial impact on enterprise-wide risk to the business as a whole. Risk and quality management solutions that are customizable allow organizations to employ the appropriate internal controls and standards that can significantly mitigate the developing geopolitical, supply-chain, and operational risks that can translate to significant enterprise level risk. In addition, scalability is critical to ensuring enterprise wide adoption.

In fact, Aberdeen Group's March 2008 benchmark report, [Risk Mitigation in Manufacturing Operations](#), found that Best-in-Class companies are 275% more likely than Laggards to adopt an ERM solution and more likely than all others to assess and mitigate non-compliance and operational risks by providing transparency of risks across the enterprise.

### Multi-regulatory industries / environments defined:

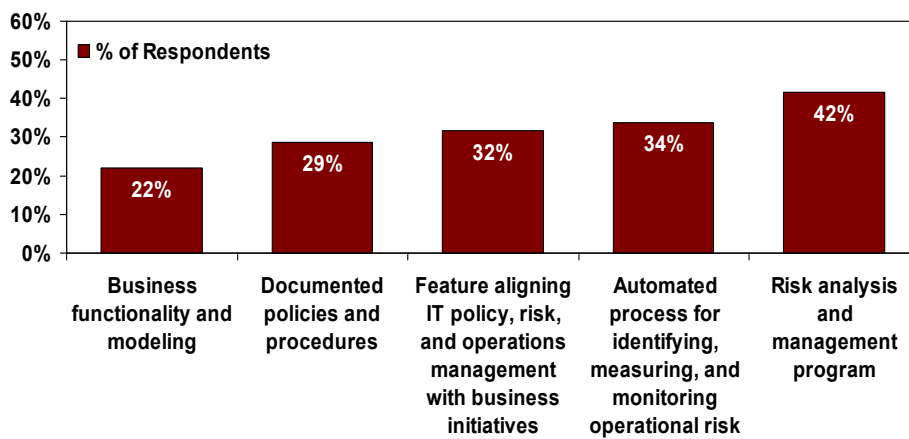
Industries that are required to achieve and prove compliance with a variety of governmental (including federal, state, and municipal) and industry-specific regulatory mandates. Such regulations are frequently amended or changed and differ, sometimes greatly, in terms of scope and applicability within an individual organization. Common examples of multi-regulatory industries include:

- Banking / Financial Services / Insurance
- Pharmaceutical manufacturing
- Energy and Utilities

## Satisfying the Demand - Impact on the Market

To achieve differentiation and success in the crowded GRC space, solutions should both directly address the end user community's current problems, as well as proactively alleviate their future pain points. In addition to regulatory compliance, organizations deciding whether or not to invest in a particular GRC solution identified automated risk analysis and management processes and features facilitating the alignment of IT to business units as most important (Figure 2).

**Figure 2: Features Organizations Need in a GRC Solution**



Source: Aberdeen Group, May 2008

Viewed as an individual application, the new release of MetricStream's Compliance Management solution offers a variety of benefits. Implementation of such a solution, in conjunction with applications for risk, audit, and/or policy management as a part of a holistically derived enterprise-wide GRC initiative, results in a enterprise-spanning framework that standardizes quality initiatives, advances operational compliance goals, and reduces the likelihood these issues will funnel into increased overall enterprise risk.

### Case Study — Streamlining through Automation

One of the largest electric utilities in the United States, with utility operations and nuclear power plants in a variety of states, over 2.6 million retail customers, and revenues in excess of \$10 billion dollars, sought a more efficient and cost effective way to meet the rising number of governmental (federal, state, and regional) and industry-specific regulations. Their internally developed compliance and ERM application, designed for a narrow set of compliance regulations, had several critical limitations.

Lacking scalability, visibility and proper controls, new processes and reporting requirements were manually set up, manually distributed across the various departments, lines of business and disparate geographic locations, and did not enforce the appropriate authorizations to limit non-privileged employees from viewing sensitive information and records. Seeking to integrate, automate, and streamline these cumbersome and costly manual processes, the utility selected MetricStream to design and implement an integrated enterprise-wide framework to manage all compliance requirements and ERM programs.

Providing comprehensive functionality for governmental and industry regulations, ERM, and corporate standards of conduct based on the utility's specific compliance requirements and associated risk levels, the solution integrates into existing enterprise applications, implements change control to ensure all processes and records stay in sync, and supports risk assessments and computations to provide the visibility necessary to clearly view the organization's risk posture. This enables the ability to accurately prioritize their strategies and mitigation plans, formulate best-practice frameworks, and scale those practices across the enterprise.

Additionally, executive dashboards provide visibility into the various compliance and risk management processes, ensures appropriate accountability and confidentiality through automated certifications powered by electronic certifications, and incorporates granular access controls to ensure the protection of sensitive information and records.

### Key Takeaways

To realize the optimal benefits of a GRC or ERM initiative, organizations must take into account how siloed activities impact the overall risk structure of the enterprise. As the evolution of quality management and operational compliance continues, there are a variety of features that a GRC initiative can incorporate to offer the greatest opportunity to achieve

compliance, manage risks at multiple levels of the enterprise, and drive sustainable business advancements.

- **Flexibility** - Depending on a multitude of factors such as industry, size, and geographic location, individual organization's enterprise compliance and risk management strategies can differ dramatically; solutions that offer a variety of compliance, quality control, and assessment capabilities allows companies to implement a framework that most efficiently advances their business goals based on their unique risk appetite.
- **Balancing Centralization** - The use of centralized monitoring and reporting activities allows internal audit processes to focus on key risks associated with compliance, product or service quality, and project oversight while enabling process owners to leverage their expertise and take responsibility for managing the controls and risk management strategies directly impacting their department. As highlighted in Aberdeen's February 2008 GRC study, such tactics enables organizations to realize a 16% year-over-year increase in optimizing existing business processes. Decentralized control management with centralized monitoring and reporting significantly reduces the possibility that quality or operational compliance issues will "bleed" into larger enterprise level risk.

For more information on this or other research topics, please visit [www.aberdeen.com](http://www.aberdeen.com).

Related Research	
<a href="#"><u>GRC Strategic Agenda: The Value Proposition of Governance, Risk, and Compliance</u></a> ; February 2008 <a href="#"><u>Risk Mitigation in Manufacturing Operations</u></a> ; March 2008	<a href="#"><u>Driving Sustainable Business Advancements through GRC: The Convergence of Governance, Risk, and Compliance</u></a> ; April, 2008
Author: Stephen Walker, Senior Associate, Technology Markets Group, <a href="mailto:stephen.walker@aberdeen.com">stephen.walker@aberdeen.com</a>	

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. 010908a