Aberdeen Group
A Harte-Hanks Company

Effective GRC Management

Positioning Your Company for Growth

December 2010

William Jan

~ Underwritten, in Part, by ~

lightwave SECURITY

mega

neupart
The ERP of Security

Aberdeen Group
A Harte-Hanks Company

Executive Summary

The purpose of this report is to provide guidance on implementing effective Governance, Risk, and Compliance (GRC) management, and the corresponding capabilities and enabling technologies that help improve financial and operational control. Over 100 companies were surveyed between November and December 2010 to identify best practices and current initiatives in enterprise GRC management. The top-performing companies demonstrated that to achieve a high-level of success in managing GRC, a strategic combination of business process evaluation and software-supported analysis should be implemented. In the end, such strategies enabled competitive differentiation, cost reduction, and growth.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth and comprehensive look into process, procedure, methodologies, and technologies with best practice identification and actionable recommendations

Best-in-Class Performance

Aberdeen used the following five key performance criteria to distinguish the Best-in-Class companies achieving the following results:

- 23% reduction in risk value in the past two years
- 23% reduction in compliance-related costs in the past two years
- 22% growth in new market revenue in the past twelve months
- 90% positive compliance audit success rate (yielding favorable results) in the past twelve months
- 84% success rate in execution of management directives in the past twelve months

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance shared several common characteristics including being:

- 78% more likely than their competitors to define a workflow for conducting organizational audits
- 54% more likely than their competitors to systematically evaluate business processes for compliance
- 27% more likely than their competitors to conduct quantified risk assessments

Required Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance, companies must:

- Define a workflow from risk identification to mitigation
- Align staff accountability to corporate objectives
- Establish platforms to promote visibility and collaboration on strategic, financial, and operational plans

How Does Your Performance Compare to the Best-in-Class?

- Compare your processes
- Receive a free, personal PDF scorecard
- Benefit from custom recommendations to improve your performance, based on the research

Take the Assessment

Receive Your Free Scorecard

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.

Aberdeen Group
A Harte-Hanks Company

Table of Contents

Figures

Tables

© 2010 Aberdeen Group.

Telephone: 617 854 5200
Fax: 617 723 7897

Aberdeen Group
A Harte-Hanks Company

Chapter One: Benchmarking the Best-in-Class

In a recovering economy, companies must remain versatile in their strategies and operations to stay competitive. Part of these change initiatives include organizational restructuring, objective realignment, strategic partnerships, and compliance to a host of regulatory requirements. What is critical to industry executives, however, is the impact of these changes on organizational Governance, Risk, and Compliance (GRC). With each change in organizational hierarchy, in target sales region, or in supply chain partners, industry leaders are faced with a growing need to actively manage GRC. The objective of this report is to identify the pressures and challenges that prompt companies to implement effective GRC management, and the processes and technologies that enable them to reduce risk-related costs and increase revenue opportunities.

Fast Facts

√ 50% of the Best-in-Class companies integrate compliance measures into their business practices

√ 71% of the Best-in-Class companies have defined workflow in place, from risk identification to risk mitigation

Business Context

In this study, governance describes the method in which executives "conduct" their organizations. Providing clear visibility to management directives for the staff, and ensuring that these initiatives are properly executed in a timely manner, remain top priorities on the executive's agenda. A responsible executive also identifies the liability associated with any business decision, and therefore must perform an accurate risk assessment to formulate mitigation strategies. Finally, organizations must be able to work effectively with government and regulatory bodies to ensure business compliance. Drivers for adopting effective GRC management are reviewed in two facets: Internally within the organization to understand the impact of proper governance and risk mitigation, and externally to understand the impact of tightened regulations. From an executive's perspective, the key benefits to GRC management are:

- Driving organizational alignment of executive and staff agendas through effective governance
- Understanding risks in terms of dollar-value impact and corporate brand equity
- Prioritizing organizational initiatives based on risk level
- Creating additional revenue opportunities by meeting compliance requirements for selling into new markets / regions

"We are beginning to introduce systems and adjust processes to obtain efficiency and accuracy - to engage in proactive planning and insights to the trends in business and individual accountability."

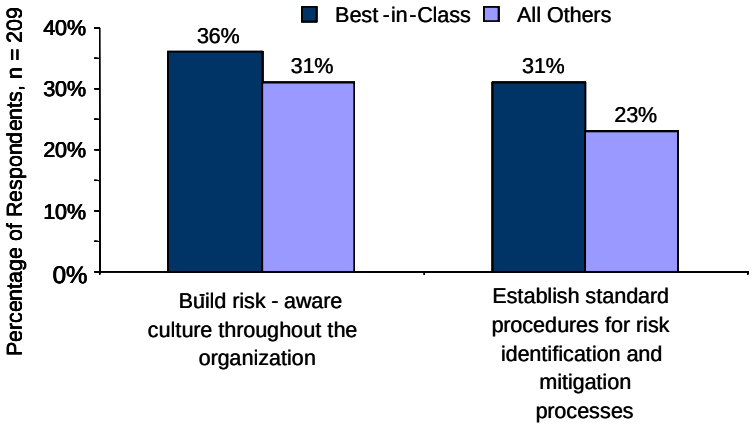
~ General Manager, Business Development, Right Management

The series of corporate consolidations and new regulatory requirements amidst a recovering economy has introduced a series of new liabilities for organizations. Executives at parent companies continue to be concerned about management standards across their constituent companies, operational risks, and the ability to comply in a dynamic regulatory environment. In Aberdeen's September 2010 study, *The Executive Enterprise Risk Management (ERM) Agenda: Mitigate Risks, Improve Performance*,

© 2010 Aberdeen Group.

organizations remain focused on promoting risk-awareness and mitigating risks (Figure 1).

Figure 1: Top Risk Management Strategies among Companies



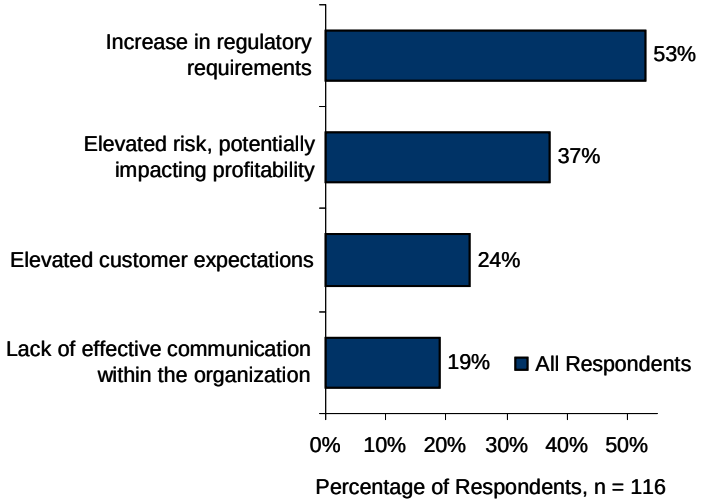
Source: Aberdeen Group, September 2010

Best-in-Class Criteria (ERM Study, September 2010)

- √ Ability to integrate and align risk with corporate goals
- √ Ability to drill down to successive levels of detail from summary positions
- √ Ability to perform "what-if" scenario-planning and change analysis

This study discusses enterprise GRC from both financial and operational standpoints. Together, these segments cover a host of areas, including finance (accounting / reporting), trade (buyer / supplier transaction), manufacturing (material / process), environmental / safety, and others. Feedback from industry executives was collected to determine which strategies and capabilities are used by the top-performing organizations to achieve success in GRC management. Figure 2 looks at the top concerns that prompt executives to implement / improve their GRC management strategies. Survey respondents were asked to select the top two.

Figure 2: Top Pressures Driving GRC Management Strategies



Source: Aberdeen Group, December 2010

© 2010 Aberdeen Group.

In an economy where revenue-generating investments continue to be a focus among C-level executives, the concept of risk and compliance often gets de-prioritized on the agenda. Why? Because the failure to quantify risk and assign a monetary value to an unforeseen liability becomes an impediment for any financial officer to justify a Return on Investment (ROI). Furthermore, even if the value of the liability is identified, GRC management is often viewed as a cost-saving measure (reduction of fines / penalties and corrective labor), as opposed to a new revenue generator. Organizations under such circumstances typically leverage GRC management to resolve problems that have already "erupted," as opposed to using such processes to proactively mitigate risks and prevent unseen costs. By having effective processes and tools in place to identify areas of risk, companies can actually derive new market revenue from two perspectives: 1 being able to sell into global markets by meeting compliance requirements, and 2 gain new customers through competitive differentiation (customers will always want to conduct business with an organization possessing lower liabilities especially in the case where organizations are under close scrutiny of media for non-compliance).

Using GRC to Position Your Company for Growth: Enabling Regulatory Agility in Selling into Global Markets

According to Aberdeen's November 2009 study, *Materials Compliance for Green Product Development: Balancing Social Responsibility with Profitability*, there continues to be a tremendous pressure for companies to leverage compliance efforts in search of revenue growth.

Compliance-awareness and consumer consciousness continue to prompt governments to introduce new regulatory bodies, regulations, and stricter penalties for non-compliance. Requirements often change by market and region, meaning multiple, differing sets of regulations that companies must be able to address. Being proactive in GRC practices can, for example, help manufacturers alleviate regulatory pressures by optimizing products for import / export. Materials compliance requirements for selling / transporting these products, for instance, can be difficult to assess, understand, or adhere to - since many of them are not only regional-specific, but are also industry and product-specific (Table 1). Due to this complexity, more companies are now tracking regulatory requirements as part of their core business processes. Table 2 presents the top standards, regulations, and directives that many companies are addressing today in conducting global business.

Table 1: Materials Compliance Regulations for Import / Export

Name / Description
Restriction of Hazardous Substances Directive (RoHS) - European Union
California RoHS / Prop 57
RoHS initiatives by other US states
Waste Electrical and Electronic Equipment directive (WEEE) - European Union

© 2010 Aberdeen Group.

Name / Description
Registration, Evaluation, Authorisation and restriction of Chemicals (REACH) - European Union
RoHS - China
RoHS - Japan / Japan Green
Energy-Using Products (EUPs), EU Battery, Energy Star
Toxic Substances Control Act (TSCA) - United States
FDA Code of Federal Regulations (CFRs)
Full Material Disclosure (FMD)
Electronic Waste Recycling Act (EWRA) - United States / California
End of Life Vehicle (ELV)
Joint Industry Guide (JIG)
Act for Resource Recycling of Electrical and Electronic Equipment and Vehicles - South Korea
Health Canada & Canada's Chemical Management Plan
Substitute It Now (SIN) lists, Non-Government Organization (NGO) lists
Allergen Labeling Requirements - FDA
Japanese industrial standard for Marking Of Specific chemical Substances (J-MOSS) - Japan
Nutritional Labeling Requirements - FDA
UN / Stockholm Convention Persistent Organic Pollutants (POPs)
Seventh Amendment - European Union

Source: Aberdeen Group, December 2010

Table 2: Regional Regulations, Directives, and Standards

Name / Description	Region
Sarbanes-Oxley Act (SOX)	United States
HL7 (Health Level Seven International)	United States
PATRIOT Act (USAPA)	United States
HIPAA (Health Insurance Portability and Accountability Act)	United States
SEC & NASDAQ regulations	United States
SB 1386 (Compliance Management Toolkit)	United States
Gramm-Leach-Bliley Act (GLB)	United States
Federal Information Security Management Act of 2002 (FISMA)	United States
Personal Information Protection and Electronic Documents Act (PIPEDA) 2000	Canada
Electronic Signature Directive	European Union
Human Rights Act 1998	European Union

© 2010 Aberdeen Group.

Name / Description	Region
EDI Directive	European Union
Basel II Capital Accord	European Union
e-Commerce Directive	European Union
The Privacy and Electronic Communications (EC Directive) Regulations 2003 (e-Privacy Directive)	European Union
MoReq - Model Requirements for the Management of Electronic Records	European Union
Markets in Financial Instruments Directive (MiFID)	European Union
ISO27001 (ISO 27001) - previously BS7799-2:2002 (BS 7799) Information Security Management System; also global standard ISO17799 (ISO 17799)	United Kingdom
Electronic Communications Act 2000	United Kingdom
BS10181 (BS 10181) Authentication and Access Control; also global standard ISO10181 (ISO 10181)	United Kingdom
Financial Services & Markets Act 2000	United Kingdom
Enterprise Act 2002	United Kingdom
Freedom of Information Act 2000 (FOI or FOIA)	United Kingdom
Regulation of Investigatory Powers Act (RIPA) 2000	United Kingdom
Data Protection Act 1998	United Kingdom
BS 25999 (BS25999) Standard for Business Continuity Management	United Kingdom
International Financial Reporting Standards (IFRS)	Worldwide
BIP0008 - Code of Practice for Legal Admissibility of Information Stored Electronically	Worldwide
ISO27001 (ISO 27001) - previously BS7799-2:2002 (BS 7799) Information Security Management System; also global standard ISO17799 (ISO 17799)	Worldwide
ISO Legal Codes of Practice for the Management of Fixed Content Data	Worldwide
ISO10181 (ISO 10181) Authentication and Access Control	Worldwide
ISO15489 (ISO 15489) Records Management	Worldwide

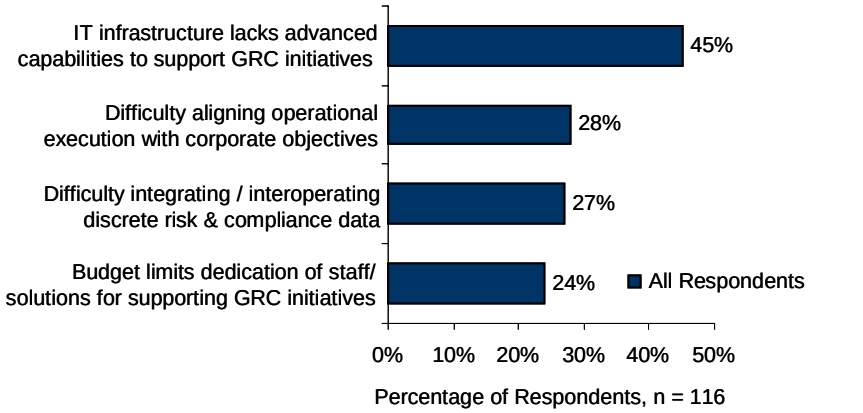
Source: Aberdeen Group, December 2010

In addition to tracking the numerous regulations that dictate a company's ability to sell into global markets, organizations are increasingly complying with more than one regulation at a time. Many of these regulations have local versions that are different from one another such as regulations specific to the European Union, the People's Republic of China, and even states such as California. In this context, the company must comply or be fined / banned from selling their products in the region. As a result, organizations must closely track and manage their processes against regulations that vary widely. To further complicate the initiative, companies

© 2010 Aberdeen Group.

are experiencing a multitude of challenges that impede the enterprise-side adoption of GRC management (Figure 3).

Figure 3: Challenges for Undertaking GRC Initiatives



Source: Aberdeen Group, December 2010

These challenges not only speak to IT integration and interoperability barriers, but also to the difficulty in communication between the departments on defining risk. Whether it is on the manufacturing shop floor, the finance department, or the operations department, the element of risk is different for each stakeholder. Defining each risk in qualitative terms is not enough for finance and / or C-level executives to make an informed decision. Once the risks have been identified by the various department stakeholders, they must be defined in terms of monetary impact (both near- and long-term), so that executives can prioritize the risks based on overall corporate liability. Additionally, by effectively quantifying risks in terms of dollar value, department stakeholders can present a strong ROI case to their executives on GRC management.

The Maturity Class Framework

GRC, in general, should not be viewed as something static. Companies often react to a host of dynamic competitive, regulatory, operational, and financial pressures by changing their strategies (and in some cases, their objectives) to adapt and grow in their respective industries. That said, companies can better position themselves for growth if they become proactive in their GRC management initiatives: making sure that objectives, risk, regulatory information, and accountability information are made visible to stakeholders ahead of time to enable informed decisions. Effective decisions made at the right time could yield performance improvements. To that end, Aberdeen uses four key performance criteria to distinguish the Best-in-Class companies from Industry Average and Laggard organizations (Table 3).

© 2010 Aberdeen Group.

Table 3: Top Performers Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance
Best-in-Class: Top 20% of aggregate performance scorers	▪ 23% reduction in risk value in the past two years ▪ 23% reduction in compliance-related costs in the past two years ▪ 22% growth in new-market revenue in the past twelve months ▪ 90% positive compliance audit success rate (yielding favorable results) in the past twelve months ▪ 84% success rate in execution of management directives in the past twelve months
Industry Average: Middle 50% of aggregate performance scorers	▪ 6% reduction in risk value in the past two years ▪ 2% reduction in compliance-related costs in the past two years ▪ 12% growth in new-market revenue in the past twelve months ▪ 59% positive compliance audit success rate (yielding favorable results) in the past twelve months ▪ 64% success rate in execution of management directives in the past twelve months
Laggard: Bottom 30% of aggregate performance scorers	▪ **No change** in risk value in the past two years ▪ 10% **increase** in compliance-related costs in the past two years ▪ 4% growth in new-market revenue in the past twelve months ▪ 50% positive compliance audit success rate (yielding favorable results) in the past twelve months ▪ 50% success rate in execution of management directives in the past twelve months

Source: Aberdeen Group, December 2010

While the Best-in-Class companies enjoyed a high-level of positive audit rate and successful execution of corporate directives, the performance among the Industry Average and the Laggard companies are staggering - nearly half of audits revealed non-compliant practices. Even more alarming is the low success rate in the execution management directives - this could imply inadequate organizational communication, as well as a shortage of resources.

The Best-in-Class PACE Model

Using effective solutions to achieve GRC management goals requires a combination of strategic actions, organizational capabilities, and enabling technologies that are summarized in Table 4.

© 2010 Aberdeen Group.

Table 4: The Best-in-Class PACE Framework

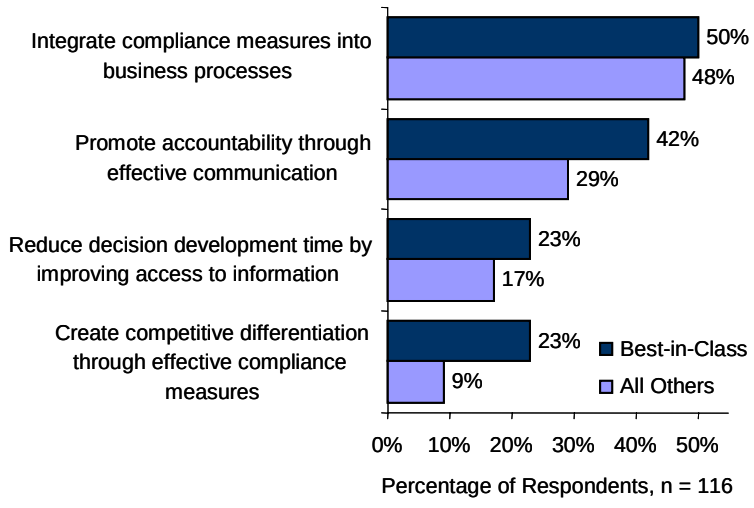
Pressures	Actions	Capabilities	Enablers
▪ Increase in regulatory requirements	▪ Integrate compliance measures into business processes ▪ Promote accountability through effective communication	▪ Defined workflow for conducting organizational audits ▪ Systematic monitoring of key risk indicators (KRIs) ▪ Accountability is assessed and delegated down the organizational hierarchy ▪ Business objectives are clearly defined	▪ Governance, Risk, and Compliance (GRC) solutions ▪ Risk management tools (point solutions) ▪ Workflow automation solutions ▪ Strategy management solutions ▪ Enterprise Resource Planning (ERP) solutions ▪ Safety compliance solutions ▪ Environmental compliance solutions ▪ Financial modeling solutions ▪ IT security solutions ▪ Enterprise Performance Management (EPM) solutions (e.g., Profitability and Cost Management solution) ▪ Regulatory portals ▪ Business Process Management (BPM) solutions ▪ Sustainability solutions

Source: Aberdeen Group, December 2010

Best-in-Class Strategies

Implementing GRC management can significantly improve operational and financial control, but many organizations lack the initiatives, capabilities, and technological enablers to realize such opportunities. Organizations earning Best-in-Class status possess elaborate GRC management capabilities as defined by: a strong alignment of staff accountability to corporate objectives, and robust solutions that provide stakeholders with access to risk data and compliance information for effective decision-making. The strategic actions of the Best-in-Class companies are identified in Figure 4.

Figure 4: Top Strategic Actions



Source: Aberdeen Group, December 2010

© 2010 Aberdeen Group.

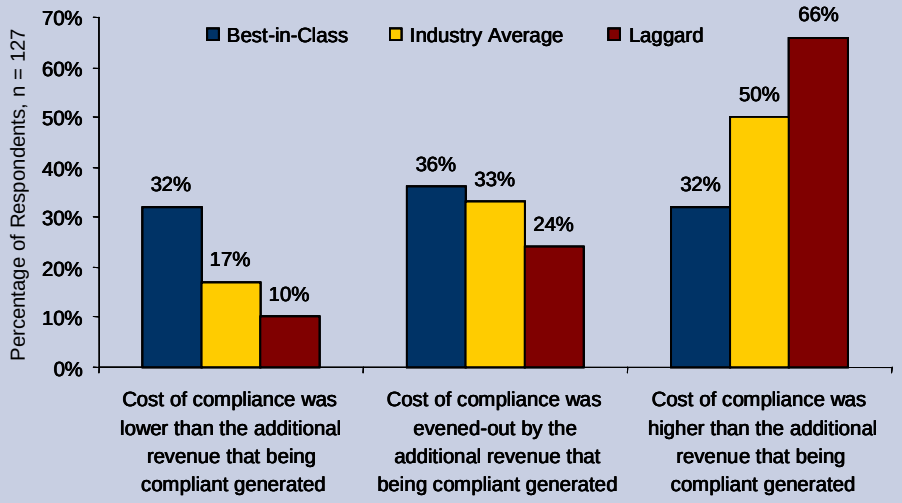
While the Best-in-Class companies share similar strategies with their competitors on integrating compliance measures into their business processes, the notable differentiation factor lies in the focus on organizational accountability through effective communication - a key element in ensuring that stakeholders within various departments can communicate their respective risk impact on overall corporate liability. Improved communication also facilitates staff understanding of management directives, and engagements with compliance auditors. Finally, a resounding difference can be seen on creating competitive differentiation through effective compliance measures - a strategy that the Best-in-Class companies are 1.5 times more likely to do than their competitors. By staying ahead in the compliance curve during times of complex regulatory changes, top companies are continuing attract new customers by improve their corporate image. Additionally, these Best-in-Class companies are demonstrating their proactive initiatives in managing liability, thus alleviating business concerns with their customers and business partners.

Aberdeen Insights — Strategy

One of the core questions that companies ask themselves before investing in compliance management solutions or services is: will this really pay off in the end? Companies that believe the answer is, "no," are among those that believe improving compliance will translate to a higher cost of doing business causing them to lose ground to competitors. On the other hand, companies that believe the answer is, "yes," are looking at compliance as a means to sell into new / global markets.

In a recent Aberdeen compliance study, Best-in-Class companies were seen to leverage compliance towards generating new-market revenue. As a result, these top companies generated more ROI from their compliance measures than their competitors (Figure 5).

Figure 5: Return on Investment for Compliance Management



Source: Aberdeen Group, November 2009

Aberdeen Insights — Strategy

As mentioned earlier, GRC management has traditionally been viewed as a means to reduce liability-related costs, and problems associated with financial and operational control. Given the dynamic regulatory environment, GRC management is now setting the stage for new revenue opportunities. By improving access to selling into global markets, and attracting new customers through liability-reduction, companies are increasingly viewing GRC solutions and services as key elements to their growth strategy.

In the next chapter, we will see what the top performers are doing to achieve these gains.

© 2010 Aberdeen Group.

Chapter Two: Benchmarking Requirements for Success

Chapter One covered how the Best-in-Class are able to increase their GRC performance through their strategies and initiatives. Chapter Two takes a closer look at GRC management solutions and processes that enable a higher level of information visibility and decision effectiveness. Such initiatives are prompting new market opportunities and liability reductions that result in enterprise growth.

Case Study — Expediting Processes and Mitigating Risks

Many companies are looking at process innovation and / or re-engineering as a means to adapt to a dynamic regulatory environment. Companies are therefore undertaking GRC initiatives to reduce risk-related costs, and to improve the effectiveness of their processes. "In September 2007, we decided to implement an ERP system, which went live in January 2009. Consequently, we now have all risk and control matrices for financial applications and supply chain in place," explains the CFO of a New Jersey-based biopharmaceutical company. "We conducted Selective Multi-versioning (SMV) [SMV is a type of algorithm that reduces the risk of using outdated data] analysis with the help of an outside team of consultants and an internal auditor team to identify a solution that would help us streamline our operation and save time. Both teams recommended having a GRC solution in place to address those issues."

The biopharmaceutical company had approximately 1,000 employees in 2006, and since then, it has expanded its workforce to about 3,500. The company is currently implementing the compliance component of its chosen multi-tier [the four tiers are the Access Control Governor (ACG), Transaction Control Governor (TCG), Configuration Control Governor (CCG), and the Preventive Control Governor (PCG)] GRC solution and is hoping to roll out the risk component in the following year. When asked about the underlying selection criteria for the solution, the CFO responded, "We are currently implementing level II (the Transactional Control Governor (TCG)) of the four levels (ACG, TCG, CCG, and PCG) of the selected GRC solution. We are particularly excited about level IV, which will allow us to modify our workflow without going through SMV conflict - this being our primary factor for deciding on this solution over another."

continued

Fast Facts

- √ Best-in-Class companies are 38% more likely than the Industry average to clearly define their business objectives
- √ Best-in-Class companies are twice as likely as laggards to have a centralized repository for maintaining compliance audit information

© 2010 Aberdeen Group.

Case Study — Expediting Processes and Mitigating Risks

By implementing this solution, the company is hoping to have better mitigation capabilities in place, especially as the company plans to expand its operations to Europe / Middle East / Africa (EMEA) and South America. The company does not have the critical mass to achieve segregation of duties in different countries, so level IV will address this issue by providing remote visibility via a real-time, automated notification and approval system.

When asked about the reason for undertaking GRC initiatives, the CFO stated, "We are trying to augment our manually-intensive processes with an automated one to expedite processes and to reduce the number of exceptions." In fact, since the implementation of tier I of their GRC solution, the company was able to easily process and resolve 300 to 400 technical issues in real time.

"Fortunately, management at our company was very supportive and openly embraced GRC initiatives. We are now implementing the entire module in increments," said the CFO. "GRC can be a very expensive proposition, and sometimes due to other competing priorities, it can take a back seat - as it did for us in years past. However, once implemented, it can address several pain points and definitely leads to greater confidence in terms of quantifying and managing risks."

Competitive Assessment

Aberdeen Group analyzed the aggregated metrics of surveyed companies to determine whether their performance ranked as Best-in-Class, Industry Average, or Laggard. In addition to having common performance levels, each class also shared characteristics in five key categories: (1) **process** (the approaches they take to execute daily operations); (2) **organization** (corporate focus and collaboration among stakeholders); (3) **knowledge management** (contextualizing data and exposing it to key stakeholders); (4) **technology** (the selection of the appropriate tools and the effective deployment of those tools); and (5) **performance management** (the ability of the organization to measure its results to improve its business). These characteristics (Table 5) serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the key metrics.

Table 5: The Competitive Framework

	Best-in-Class	Average	Laggards
Process	Information access is controlled to ensure security		
	76%	74%	67%
	Defined workflow for conducting organizational audits		
	64%	39%	33%

© 2010 Aberdeen Group.

	Best-in-Class	Average	Laggards
Organization	External feedback platforms are established to understand customer expectations in GRC landscape		
	38%	21%	12%
Knowledge	Centralized repository for business process information - documentation of process workflows		
	61%	39%	33%
	Centralized repository for maintaining compliance audit information accountability information (delegation audit trail)		
	60%	31%	22%
Technology	GRC technologies currently in use:		
	▪ 59% Risk management tools ▪ 61% Profitability and cost management solution ▪ 38% Strategy management solutions ▪ 58% Safety compliance solutions ▪ 70% IT security Solutions ▪ 42% Sustainability solutions	▪ 38% Risk management tools ▪ 44% Profitability and cost management solution ▪ 23% Strategy management solutions ▪ 38% Safety compliance solutions ▪ 63% IT security Solutions ▪ 15% Sustainability solutions	▪ 38% Risk management tools ▪ 37% Profitability and cost management solution ▪ 18% Strategy management solutions ▪ 38% Safety compliance solutions ▪ 60% IT security Solutions ▪ 14% Sustainability solutions
Performance	Systematic evaluation of business process compliance		
	54%	38%	31%
	Quantified risk assessments are conducted systematically (dollar-value impact per risk)		
	42%	38%	28%

Source: Aberdeen Group, December 2010

"Automation (of GRC initiatives) has increased data transfer from one system to another, but interpreting the data and taking the necessary action is still something that is open and cannot be solved through automation alone."

~ Manager, Marketing, IT Consulting Firm

Capabilities and Enablers

Based on the findings of the Competitive Framework and interviews with end-users, Aberdeen's analysis of the Best-in-Class reveals that, in order to manage GRC effectively, executives must have access to tools that enable visibility to financial and operational directives, risks, and compliance requirements, as well as their impact on business objectives. But succeeding in these elements, companies are realizing additional revenue opportunities

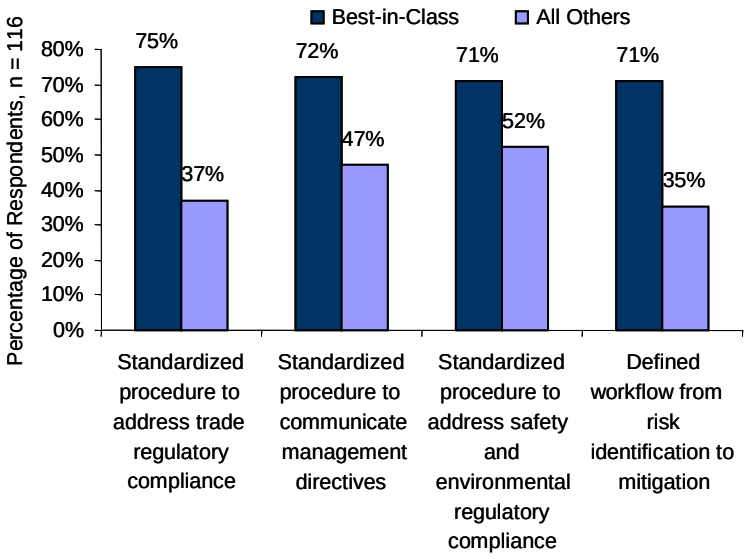
© 2010 Aberdeen Group.

by being able to sell into global markets, and competitively differentiate themselves as a low-risk business partner.

Process

Some of the greatest differentiators between the Best-in-Class companies and their competitors are the capabilities around standardization (Figure 6). Global companies with distributed teams are often working with disparate enterprise IT systems, and have different communication protocols when addressing GRC. Top companies have taken the initiative to standardize all these processes to enable better trade, safety, and environmental compliance, as well as improve their abilities to quickly identify risk elements to expedite mitigation actions. Finally, executives must be able to understand the impact of risk on overall corporate performance. By communicating openly with their department leaders on the dollar-value impact of the various risks throughout the organization, these executives can better prioritize mitigation strategies, as well as validate the effectiveness of their directives.

Figure 6: Best-in-Class Process Capabilities



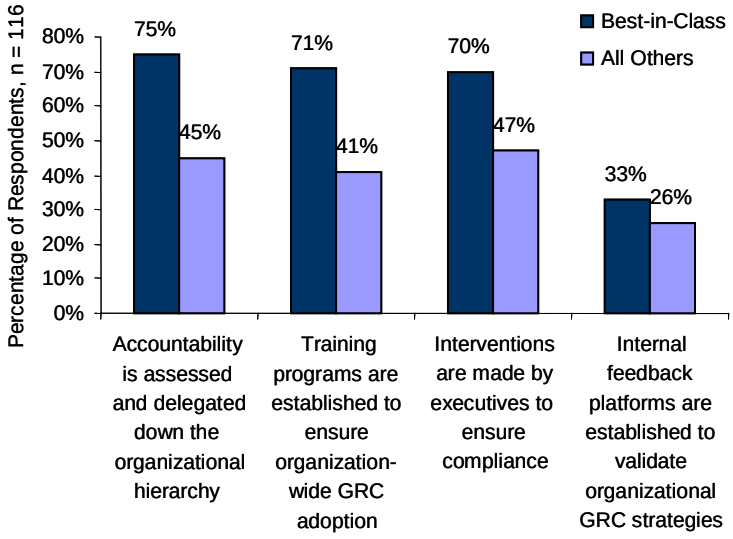
Source: Aberdeen Group, December 2010

Organization

It is safe to say that with any major corporate initiative, the first step towards success is attaining executive support. Conversely, if anything were to go wrong at the organizational level, it is critical that executives intervene and provide a corrective path (Figure 7). In order to do so, company leaders must have access to GRC data and information that help them identify the source of failure. Whether a new strategy is implemented as part of this corrective action or an existing strategy is evaluated for its effectiveness, both qualitative and quantitative feedback should be collected from various departments, at various levels, to validate the success of the strategy.

© 2010 Aberdeen Group.

Figure 7: Best-in-Class Organization Capabilities

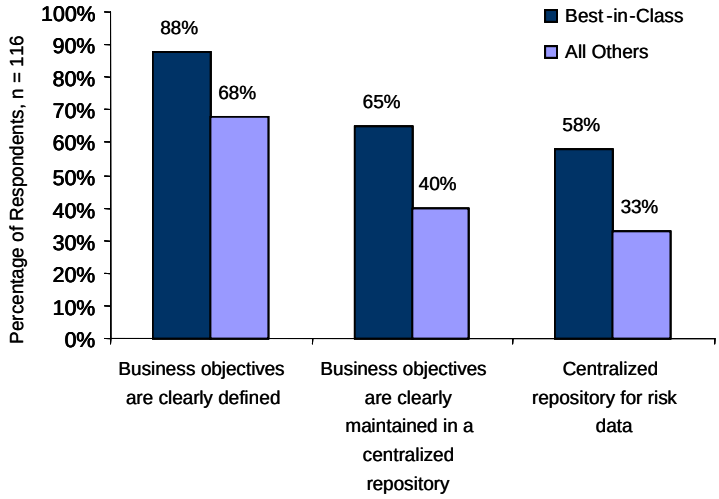


Source: Aberdeen Group, December 2010

Knowledge Management

The centralizing of risk data and compliance information facilitates stakeholder access, particularly in situations where the organization is dispersed geographically and operating in different time zones. For organizations that conduct a fair amount of field operations, and possess or require mission-critical risk data that impacts corporate objectives, this centralized repository becomes of great value in terms of real-time access. Additionally, Best-in-Class companies are more likely than their competitors to leverage this centralized repository to maintain GRC information (Figure 8). This enables stakeholders the effective visibility to management directives, risk elements, and regulatory changes.

Figure 8: Best-in-Class Knowledge Management Capabilities



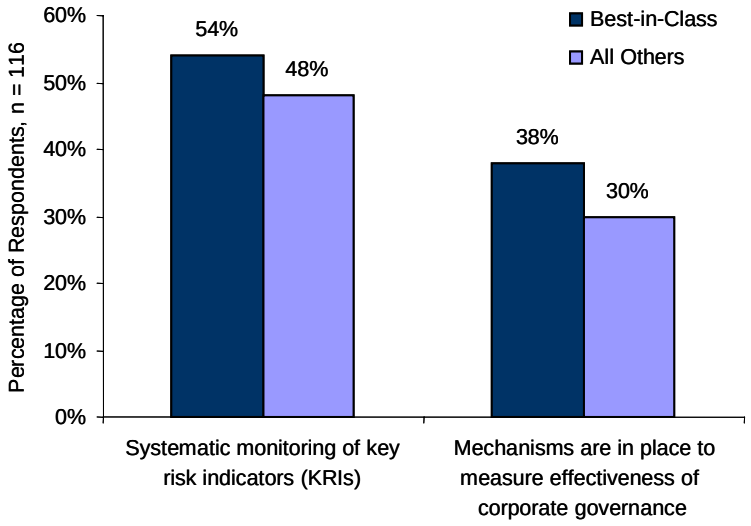
Source: Aberdeen Group, December 2010

© 2010 Aberdeen Group.

Performance Management

Identifying KRIs is critical in establishing risk mitigation strategies (Figure 9). Thus, by possessing a platform that systematically monitors these indicators, organizations can consistently get a pulse on the health of the business. Ultimately, by tracking and measuring the risk level of their various business segments, executives are able to validate the effectiveness of their mitigation strategies. Additionally, Best-in-Class companies are better at measuring how well their staff is following management directives. By tracking the effectiveness of corporate governance, executives can ultimately ensure the alignment of staff execution to enterprise objectives. That said, organizational leaders must be vigilant in identifying shifts in business performance. By leveraging real-time data and information, executives can become more proactive, rather than reactive, in managing GRC.

Figure 9: Best-in-Class Performance Management Capabilities



Source: Aberdeen Group, December 2010

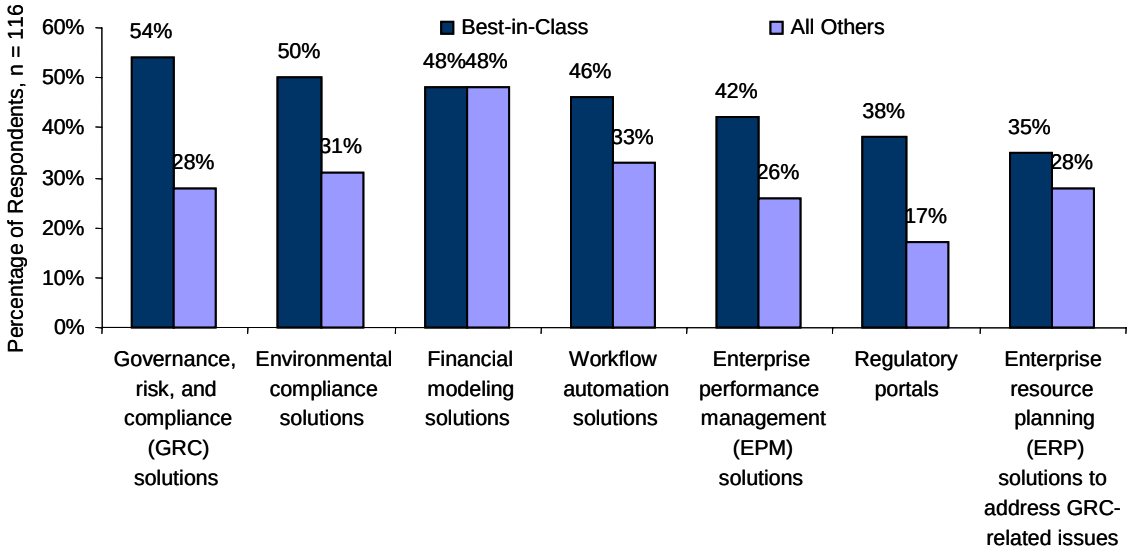
Technology

In a heavily competitive environment, where decisions have to be made in a quick and informed manner, it becomes apparent that those relying completely on people for communication are at a disadvantage when compared to software-enabled collaboration. Software has facilitated human communication in many industry-specific applications, and has grown to enable connectivity amongst stakeholders. Despite distributed stakeholders working in all global time zones, and around the clock, technology has enabled the capture and use of GRC data / information to expedite financial and operational decisions. Prior to the availability of enterprise-level GRC management solutions, departmental data / information were often siloed, with visibility reduced to only the department heads and their constituents. Consequently, during executive meetings, department-level reports would be generated and compiled, leaving senior management struggling to

© 2010 Aberdeen Group.

understand the risk impact between the departments, and on the company as a whole. By providing an infrastructure that allows executives to concurrently access GRC data / information, companies are effectively positioning themselves for performance improvements. Figure 10 takes a look at the current technologies that are being leveraged to manage governance, risk, and compliance among organizations.

Figure 10: Best-in-Class Technology Capabilities



Source: Aberdeen Group, December 2010

Aberdeen Insights — Technology

The Best-in-Class companies are 47% more likely than their competitors to deploy GRC management solutions via the cloud (SaaS, or on-demand method). In terms of usage based on company size, the large enterprises ($1 billion and over in annual revenue) are 53% more likely than the small-to-medium-sized businesses (with under $1 billion in annual revenue) to deploy cloud-based GRC management solutions.

The growth in cloud-based GRC solutions, and other enterprise applications, can be attributed to the users' desire to reduce cost of IT investment. According to a recent enterprise application survey, 79% of the surveyed companies view that the cloud platform could lower the TCO on IT, 66% see the cloud offering as a way to reduce the cost and effort of upgrades, 57% view the cloud as a means to lower up-front costs, and 50% see cloud deployment as an alternative to employing their own IT staff / resources.

© 2010 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Chapter Three: Required Actions

Whether a company is trying to move its performance in GRC management from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur the necessary performance improvements:

Laggard Steps to Success

- **Establish external feedback platforms to better understand customer expectations** (12% of the Laggard companies currently have such capability in place, compared to 23% of Industry Average companies). A critical element to attracting new customers, and keeping current ones, is to stay tuned to their needs. Aside from understanding customer compliance requirements for doing business, companies should anticipate customer needs from analyzing their feedback - whether it is their desire for better "green" / sustainable practices, their concern for working with high-liability businesses, or their desire to reduce transaction-level risks. By establishing external feedback platforms to better understand customer expectations, Laggard companies can effectively increase business with targeted investments.
- **Centralize compliance audit and accountability information** (21% of the Laggard companies currently have such capability in place, compared to 31% of Industry Average companies). Having easy access to audit and accountability information allows companies to know who (individual or department) owns certain processes, and why the processes are / are not compliant. This type of information access / transparency allows executives to act appropriately before compliance problems become a corporate liability. By centralizing compliance audit and accountability information, Laggard companies can allow stakeholders to quickly identify faulty processes and / or procedures so that remediation strategies can be established.

Industry Average Steps to Success

- **Define workflow for conducting organizational audits** (39% of the Industry Average companies currently have such capability in place, compared to 64% of Best-in-Class companies). Many companies understand the importance of audits in ensuring compliance in procedures and processes. But the validity of the audit results is heavily dependent on the audit methodology. To that end, companies with a clear workflow for conducting GRC audits are in a position to obtain more accurate, valuable results. By defining workflow for conducting organizational audits, Industry Average companies can be more accurate in their audit results across the entire organization.
- **Centralize business process information** (39% of Industry Average companies currently have such capability in place,

Fast Facts

√ Best-in-Class companies are 80% more likely than Laggards to have a GRC solution in place

√ Best-in-Class companies are 36% more likely than Laggards to have a risk management solution in place, in addition to a GRC solution

How Does Your Performance Compare to the Best-in-Class?

- Compare your processes
- Receive a free, personal PDF scorecard
- Benefit from custom recommendations to improve your performance, based on the research

Take the Assessment

Receive Your Free Scorecard

compared to 61% of Best-in-Class companies). To facilitate the audit of business procedures and processes, it is helpful to have all business process information stored in a central location. This allows the stakeholders and auditors to access this information quickly, regardless of their time zone or geographic location. Furthermore, in dynamic business environment, business processes often change, making real-time access to updated information even more critical. By centralizing business process information, Industry Average companies can streamline the auditing process, and ensure that the organization is following the latest procedures.

Best-in-Class Steps to Success

- **Evaluate business process compliance systematically** (currently, 54% of the Best-in-Class have this capability in place). To maintain industry leadership, Best-in-Class companies should not only continue to evaluate their business processes or compliance, but to do so systematically. This enables executives to identify areas of inefficiency, and propose process re-engineering initiatives where required. This evaluation process is essentially a systematic audit, where stakeholders are encourage to participate. The objective is to validate processes for effectiveness and compliance towards current standards, directives, or regulations. If a process is ineffective, and not be changed (in the near-term), a risk assessment must be performed to identify impact on overall corporate liability.
- **Conduct quantified risk assessments systematically** (currently, 42% of Best-in-Class companies have this capability in place). To maintain industry leadership, Best-in-Class companies should continue to conduct risk assessments, in terms of monetary impact (even schedule impacts can be defined in terms of dollar-value). The objective is to provide executives the ability to quantify the risk, in order to prioritize their risk mitigation investments and initiatives. By doing so systematically not only keeps a constant pulse on the business, but facilitates the budget / investment forecast process for financial executives. Finally, this capability allows stakeholders to identify risks as soon as they appear, giving executives the ability to expedite mitigation decisions.

Aberdeen Insights — Summary

This study has stressed the importance of leveraging GRC initiative towards corporate growth, defining effective GRC management in terms of enabling new marketing opportunities, as well as attracting new customers. To ensure success in managing GRC, organizations must provide decision-makers with processes and tools that allow visibility and access to GRC information. More importantly, the resulting strategies and directives must be actionable by stakeholders, and the executives must be encouraged to intervene when necessary. These are core elements to business success, and if managed correctly, a powerful competitive differentiator.

"We use a first-class document management system for governance and compliance. A compliance calendar sends alerts in advance of key deadlines."

~ Director, Information Technology

© 2010 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Appendix A: Research Methodology

Between November and December 2010, Aberdeen examined the use, the experiences, and the intentions of more than 100 organizations implementing Governance, Risk, and Compliance (GRC) initiatives in a diverse set of disciplines across all industries.

Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on GRC strategies, experiences, and results.

Responding organizations included the following:

- *Job title:* The research sample included respondents with the following job titles: CEO / President (17%); CFO / CIO / COO / Chief Strategy Officer (5%); Director (22%); Manager (21%); Consultant (10%); IT Director (5%), VP/ Partner/ GM / Managing Director (13%); and other (7%).
- *Department / function:* The research sample included respondents from the following departments or functions: business development / sales (19%); corporate management (11%); information technology (18%); finance / administration (8%); procurement / purchasing (8%), operations (5%); auditor (4%); logistics / supply chain (5%); marketing (3%); and other (19%)
- *Industry:* Majority of the respondents came from IT consulting / services (22%), followed by software (8%) and financial services (5%). All remaining industries were equally represented and were represented in the range from 0% to 4%.
- *Geography:* The majority of respondents (56%) were from North America, followed by Europe (23%), Asia / Pacific (8%), Middle East / Africa (8%) and South / Central America and Caribbean (5%).
- *Company size:* Twenty- six percent (26%) of the respondents were from large enterprises (annual revenues above US $1 billion); 42% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 32% of respondents were from small businesses (annual revenues of $50 million or less).
- *Headcount:* Thirty-eight percent (28%) of respondents were from large enterprises (headcount greater than 1,000 employees); 22% were from midsize enterprises (headcount between 100 and 999 employees); and 40% of respondents were from small businesses (headcount between 1 and 99 employees).

Study Focus

Responding financial, operational, and IT executives completed an online survey that included questions designed to determine the following:

- √ The degree to which GRC initiatives are deployed in their operations, and the financial implications of the technology
- √ The structure and effectiveness of existing GRC initiatives
- √ Current and planned use of GRC to improve risk value and reduce compliance related costs
- √ The benefits, if any, that have been derived from GRC initiatives

The study aimed to identify emerging best practices for GRC implementation across different industries which companies could use to assess their own management capabilities.

© 2010 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Table 6: The PACE Framework Key

Overview
Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows: **Pressures —** external forces that impact an organization's market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive) **Actions —** the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product / service strategy, target markets, financial strategy, go-to-market, and sales strategy) **Capabilities —** the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing) **Enablers —** the key functionality of technology solutions required to support the organization's enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)

Source: Aberdeen Group, December 2010

Table 7: The Competitive Framework Key

Overview	
The Aberdeen Competitive Framework defines enterprises as falling into one of the following three levels of practices and performance: **Best-in-Class (20%) —** Practices that are the best currently being employed and are significantly superior to the Industry Average, and result in the top industry performance. **Industry Average (50%) —** Practices that represent the average or norm, and result in average industry performance. **Laggards (30%) —** Practices that are significantly behind the average of the industry, and result in below average performance.	In the following categories: **Process —** What is the scope of process standardization? What is the efficiency and effectiveness of this process? **Organization —** How is your company currently organized to manage and optimize this particular process? **Knowledge —** What visibility do you have into key data and intelligence required to manage this process? **Technology —** What level of automation have you used to support this process? How is this automation integrated and aligned? **Performance —** What do you measure? How frequently? What's your actual performance?

Source: Aberdeen Group, December 2010

Table 8: The Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact
Aberdeen research indicates that companies that identify the most influential pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute those decisions.

Source: Aberdeen Group, December 2010

© 2010 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Appendix B:
Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report includes:

- *The Executive Enterprise Risk Management (ERM) Agenda: Mitigate Risks, Improve Performance*; September 2010
- *The True Cost of Materials Compliance: Does the Good Outweigh the Bad?*; December 2009
- *Materials Compliance for Green Product Development: Balancing Social Responsibility with Profitability*; November 2009
- *IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs*; May 2009
- *Is Your GRC Strategy Intelligent? Analytics for Accurate, Real-Time Visibility and Decision Making*; July 2008

Information on these and any other Aberdeen publications can be found at www.aberdeen.com.

Author: William Jan, Senior Analyst, Financial Management & GRC, (William.Jan@Aberdeen.com)

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. (110810a)

Featured Underwriters

This research report was made possible, in part, with the financial support of our underwriters. These individuals and organizations share Aberdeen's vision of bringing fact based research to corporations worldwide at little or no cost. Underwriters have no editorial or research rights, and the facts and analysis of this report remain an exclusive production and product of Aberdeen Group. Solution providers recognized as underwriters were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

SecureAware® from Lightwave Security enables companies to continuously comply with multiple, complex regulations such as ISO27001, PCI DSS, WLA SCS, CoBIT, and Cloud Security Alliance (CSA) standards.

Implementing SecureAware® as the foundation of an Information Security Management System (ISMS) can reduce the costs of managing security policies, security awareness training, and streamlines your audit processes.

SecureAware® functions include quantitative risk assessments, policy management, awareness training, compliance workflow automation, and business continuity planning.

Lightwave Security is the exclusive distributor of SecureAware® in North America and supports its clients in government, energy, utility, financial services, IT services, insurance, and lotteries.

For additional information on Lightwave Security:

Lightwave Security

1200 Abernathy Road, Suite 1700

Atlanta, GA 30328

Telephone: 800.616.8597

www.lightwavesecurity.com

info@lightwavesecurity.com

© 2010 Aberdeen Group.

MEGA offers comprehensive governance, risk, and compliance solutions through its MEGA GRC Suite. The Suite helps companies improve audit quality and productivity to meet corporate and regulatory requirements, manage global and local operational risks, and meet reporting requirements through comprehensive compliance and control features.

MEGA also offers business process analysis and enterprise architecture solutions through its MEGA Modeling Suite.

Founded in 1991, MEGA has 70,000 software licenses worldwide. Clients include Aetna, BAE Systems, Cardinal Health, Choice Hotels, Cox Enterprises, DirecTV, JC Penney, Medco Health Solutions, Nissan, Procter & Gamble

For additional information on MEGA:

175 Paramount Drive - Suite 303

Raynham, MA 02767

Telephone: 781.784.7684

www.mega.com

mhedba@mega.com

© 2010 Aberdeen Group.

Neupart, an ISO 27001 certified company, provides an all-in-one solution allowing organizations to achieve continuous compliance by automating activities for IT governance, risk management and compliance management. Whether you need to comply with PCI DSS, ISO 27001, Sarbanes-Oxley, WLA SCS, or manage evolving business risks, Neupart allows you to respond effectively and "future proof" your compliance program. More than 300 organizations worldwide are using SecureAware from Neupart, including governments, energy and utility providers, banks and insurance firms, IT Service providers and lotteries.

For additional information on Neupart:

Lightwave Security

1200 Abernathy Road, Suite 1700

Atlanta, GA 30328

Telephone: 800.616.8597

www.lightwavesecurity.com

info@lightwavesecurity.com