

## **IT GRC**

Managing Risk, Improving Visibility, and Reducing Operating Costs

May 2009

Derek Brink

Sponsored by:



## Executive Summary

For all organizations with current or planned initiatives in the area of IT governance, risk management, and compliance (IT GRC), this report describes the policy, planning, process, and organizational elements of successful implementations. Companies with top results position themselves to make better-informed business decisions, in the context of the organization's requirements for compliance and also their appetite for risk.

### Best-in-Class Performance

---

To distinguish Best-in-Class companies from Industry Average and Laggard organizations in their respective IT GRC initiatives, Aberdeen used each respondent's estimated year-over-year changes in the following capabilities:

- Identification of weaknesses in existing risk management processes
- Ability to translate risk assessment data into actionable recommendations
- Flexibility to adjust to new or updated regulatory requirements

The first two criteria were selected as measures of an organization's performance in adapting and responding to risk, while the third was selected as an indicator of their ability to adjust to a dynamic compliance landscape. Companies with top performance based on these criteria earned Best-in-Class status.

### Competitive Maturity Assessment

---

Survey results show that the firms enjoying Best-in-Class performance in IT GRC shared several common characteristics, including the following:

- Consistent policies and procedures for IT compliance (73%) and IT risk management (70%)
- IT vulnerability assessments (70%) and IT risk assessments (58%)
- Responsible executive or team with primary ownership of IT GRC initiative (85%); communication of corporate policies, practices and expectations for ethical behavior (64%)
- Repository of log, information and event data (76%); of applicable laws and regulations (58%); of risks and related information (55%)
- Modeling of interconnections and dependencies of IT risks (36%); of how IT risks impact expenditures and corporate objectives (27%); of impact of unmitigated risk versus cost of mitigation (24%)

### Recommended Actions

---

In addition to the specific recommendations in Chapter Three, to achieve Best-in-Class performance companies should commit to managing IT as a strategic asset, and adopt a continuous improvement approach to IT GRC.

#### Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth look into process, procedure, methodologies, and technologies; identify best practices; and make actionable recommendations.

"My initial views about GRC? Audit, tick-box, let's take a job we didn't want to do in the first place and make it more automated."

~ IT Security Manager,  
Global Pharmaceutical  
Company

## Table of Contents

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Recommended Actions.....	2
Table of Contents .....	3
Chapter One: Benchmarking the Best-in-Class.....	5
Business Context: Managing IT to Support the Business .....	5
Maturity Class Framework: Defining the Best-in-Class .....	7
The Best-in-Class PACE Model .....	8
Best-in-Class Strategies and Results .....	9
Chapter Two: Benchmarking Requirements for Success.....	13
Competitive Assessment.....	13
Capabilities and Enablers.....	15
Chapter Three: Recommended Actions .....	24
Laggard Steps to Success.....	24
Industry Average Steps to Success .....	24
Best-in-Class Steps to Success.....	24
Appendix A: Research Methodology.....	26
Appendix B: Related Aberdeen Research.....	28

## Figures

Figure 1: Time IT GRC Initiatives Have Been in Place .....	6
Figure 2: Top Pressures Driving Current Investments in IT GRC* .....	7
Figure 3: Top Strategies Driving Current Investments in IT GRC.....	10
Figure 4: Best-in-Class IT GRC is Centralized and Automated.....	12
Figure 5: Consistent Policies; Regular Assessments .....	15
Figure 6: Standardization and Elimination of Root Causes.....	16
Figure 7: Linking Objectives, Risks, Controls, and Compliance.....	16
Figure 8: One Throat to Choke; Communication of Expectations .....	17
Figure 9: "Wiring" Organizations to Support IT GRC .....	18
Figure 10: Fact-Based Approach to IT GRC.....	18
Figure 11: Regular Monitoring, Analysis and Review .....	19
Figure 12: Increased Visibility and Actionable Recommendations .....	19
Figure 13: Modeling Risks, Dependencies, Cost and Objectives.....	20
Figure 14: Enabling Technologies Currently Used for IT GRC.....	21
Figure 15: Enabling Technologies Currently Used for IT GRC (continued).....	21
Figure 16: Identifying, Tracking, Verifying Relevant Information.....	22
Figure 17: Market Trends: Absolute versus Relative Adoption.....	23

## Tables

---

Table 1: Management's Discussion of Risk Factors in Recent SEC Filings (illustrative) .....	5
Table 2: Top Performers Earn Best-in-Class Status.....	8
Table 3: Best-in-Class PACE Framework for IT GRC .....	9
Table 4: Average Year-over-Year Changes in Risk Management and Compliance Capabilities .....	11
Table 5: Competitive Framework for IT GRC.....	14
Table 6: PACE Framework Key.....	27
Table 7: Competitive Framework Key.....	27
Table 8: Relationship Between PACE and the Competitive Framework .....	27

## Chapter One: Benchmarking the Best-in-Class

### Business Context: Managing IT to Support the Business

From an outsider's perspective, assessing the degree of focus and the level of sophistication a particular company gives to managing its most critical enterprise risks is *not* an easy task. For publicly traded companies, some insights are available through their standard SEC Form 10-K filings, which feature management's up-front discussion of the risk factors that could materially affect the company's business, operations, or financial condition. As an illustration, the risk factors from the most recent 10-K filing for a US-based high-tech company with greater than \$10 billion in annual revenue are summarized in Table I. To give structure to the original narrative, Table I also groups the risks into four high-level categories: *financial*, *strategic*, *operational*, and *other*.

#### Fast Facts

Adoption of a "continuous improvement" approach to their IT GRC initiative:

- √ Best-in-Class: 55%
- √ Industry Average: 28%
- √ Laggards: 24%

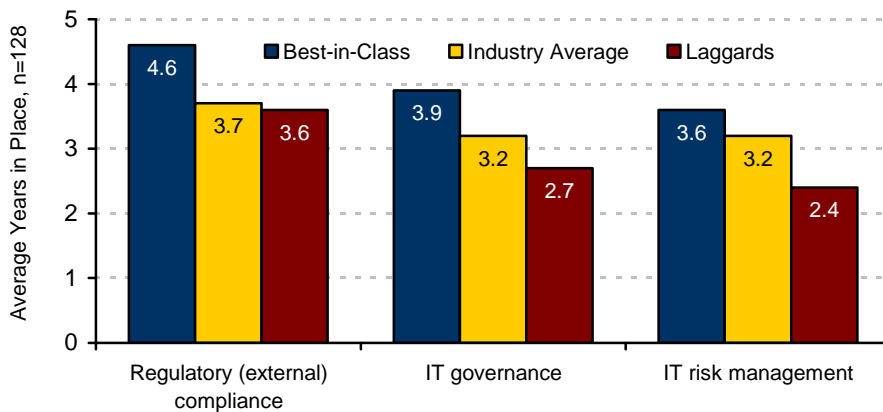
**Table I: Management's Discussion of Risk Factors in Recent SEC Filings (illustrative)**

Risks	High Tech Company, US-based, >\$10B Annual Revenue
<b>Financial</b>	<ul style="list-style-type: none"> <li>▪ Our business could be materially adversely affected as a result of general economic and market conditions, including the current economic crisis</li> <li>▪ Our investment portfolio could experience a decline in market value which could adversely affect our financial results</li> <li>▪ We may have exposure to additional income tax liabilities</li> <li>▪ Changes in generally accepted accounting principles may adversely affect us</li> <li>▪ Our business could be materially adversely affected as a result of the risks associated with acquisitions and investments</li> <li>▪ Our pension and retirement benefit plan assets are subject to market volatility</li> </ul>
<b>Strategic</b>	<ul style="list-style-type: none"> <li>▪ Our business could be materially adversely affected as a result of a lessening demand in the information technology market</li> <li>▪ Competitive pricing, sales volume, mix and component costs could materially adversely affect our revenues, gross margins, and earnings</li> <li>▪ We may be unable to keep pace with rapid industry, technological, and market changes</li> <li>▪ The markets we serve are highly competitive and we may be unable to compete effectively</li> <li>▪ Our business could be materially adversely affected as a result of the risks associated with alliances</li> </ul>
<b>Operational</b>	<ul style="list-style-type: none"> <li>▪ If our suppliers are not able to meet our requirements, we could have decreased revenues / earnings</li> <li>▪ We may have difficulty managing operations</li> <li>▪ Undetected problems in our products could directly impair our financial results</li> <li>▪ Our business may suffer if we cannot protect our intellectual property</li> </ul>
<b>Other</b>	<ul style="list-style-type: none"> <li>▪ Due to the international nature of our business, changes in foreign conditions or other factors could impair our international operations, future revenue, or financial condition</li> <li>▪ We may become involved in litigation that may materially adversely affect us</li> <li>▪ Changes in regulations could materially adversely affect us</li> <li>▪ Our business could be materially adversely affected by changes in regulations or standards regarding energy use of our products</li> <li>▪ Our business could be materially adversely affected as a result of war or acts of terrorism</li> </ul>

Source: Aberdeen Group, May 2009

Look closely at Table 1, and notice that not once is Information Technology (IT) mentioned directly. Yet IT plays a fundamental, foundational role in addressing many of these key risk factors, and indeed IT is responsible for supporting or enabling numerous aspects of any given company's business. The rise in importance of IT governance, risk management and compliance ("IT GRC") reflects an increasing recognition that the strategic value of IT lies not in the mere technology itself (which is generally accessible to everyone), but in how it is applied and managed most effectively.

**Figure 1: Time IT GRC Initiatives Have Been in Place**



Source: Aberdeen Group, May 2009

The current research shows that the "GRC" acronym is actually out of order, at least for the IT function. Based on the average length of time IT GRC-related initiatives have been in place (Figure 1), the *de facto* order for IT GRC has been **first compliance, then IT governance, then IT risk management**. This pattern holds true across all maturity classes, although the research does show that the companies with top performance in each of these initiatives have indeed been at it a longer time than their counterparts. The research also shows that the companies with top performance are 2.3-times more likely to have adopted a "continuous improvement" approach to their IT GRC initiatives, underscoring their commitment to managing IT as a strategic asset.

For the top performers **reducing total cost, providing greater visibility** to improve decision-making, and **mitigating technical and operational risks** are the strongest drivers of current investments in IT GRC initiatives (Figure 2). **Regulatory compliance** and **security of the IT infrastructure** were ranked lower by the top performers as drivers for current investments. This should not be taken as evidence of security and compliance being unimportant; on the contrary, it shows that companies with average and lagging performance are still in the process of getting their proverbial security and compliance houses in order. But the current findings add to the growing body of evidence in Aberdeen's benchmark research that Best-in-Class organizations first ensure that their IT foundations are

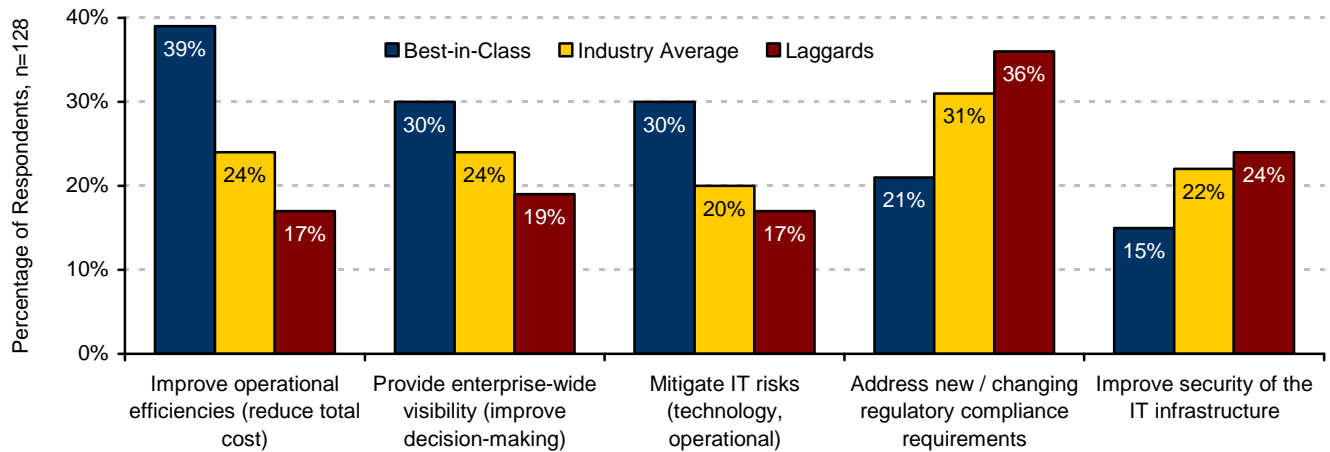
**Definitions**

In the context of this benchmark study:

- ✓ **Governance** refers to the frameworks, policies, procedures, controls, decision-making hierarchy, etc. which are employed to make decisions and manage the business
- ✓ **Risk Management** refers to the identification, prioritization and mitigation of risks that could potentially impact the organization
- ✓ **Compliance** refers to meeting and sustaining requirements for government regulations, industry regulations, and internal policies within the allotted timeframe
- ✓ **IT GRC** refers to a unified, comprehensive, and inter-connected approach towards Governance, Risk Management and Compliance as it relates to the organization's use of Information Technology (IT)
- ✓ **Enterprise Risk Management** refers to the assessment and strategic management of risks across the enterprise

secure and compliant, then turn their attention to seeing that they are optimized with respect to cost, decision-making agility, and management of risk. First order, then progress.

**Figure 2: Top Pressures Driving Current Investments in IT GRC\***



\* Respondents were asked to name their top two pressures  
Source: Aberdeen Group, May 2009

### Maturity Class Framework: Defining the Best-in-Class

To distinguish Best-in-Class companies from Industry Average and Laggard organizations in their respective IT GRC initiatives, Aberdeen used each respondent's estimated year-over-year changes in the following capabilities:

- Identification of weaknesses in existing risk management processes
- Ability to translate risk assessment data into actionable recommendations
- Flexibility to adjust to new or updated regulatory requirements

The first two criteria were selected as measures of an organization's performance in adapting and responding to risk, while the third was selected as an indicator of their ability to adjust to a dynamic compliance landscape.

Companies with top performance based on these criteria earned Best-in-Class status, as described in Table 2. (For additional details on the Aberdeen Maturity Class Framework, see Table 7 in Appendix A.)

**Table 2: Top Performers Earn Best-in-Class Status**

Definition of Maturity Class	Mean Class Performance (year-over-year change)
<p><b>Best-in-Class:</b> <b>Top 20%</b> of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ <b>11.2% increase</b> in identification of weaknesses in existing risk management processes</li> <li>▪ <b>9.6% increase</b> in ability to translate risk assessment data into actionable recommendations</li> <li>▪ <b>11.5% increase</b> in flexibility to adjust to new or updated regulatory compliance requirements</li> </ul>
<p><b>Industry Average:</b> <b>Middle 50%</b> of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ <b>7.1% increase</b> in identification of weaknesses in existing risk management processes</li> <li>▪ <b>5.8% increase</b> in ability to translate of risk assessment data into actionable recommendations</li> <li>▪ <b>4.8% increase</b> in flexibility to adjust to new or updated regulatory compliance requirements</li> </ul>
<p><b>Laggard:</b> <b>Bottom 30%</b> of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ <b>No change</b> in identification of weaknesses in existing risk management processes</li> <li>▪ <b>No change</b> in ability to translate risk assessment data into actionable recommendations</li> <li>▪ <b>No change</b> in flexibility to adjust to new or updated regulatory requirements</li> </ul>

Source: Aberdeen Group, May 2009

### The Best-in-Class PACE Model

Successful IT GRC initiatives require a combination of strategic actions, organizational capabilities, and enabling technologies – referred to by Aberdeen as the Best-in-Class PACE Framework (for a description of the Aberdeen PACE Framework, see Table 6 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this study are summarized in Table 3.

**Table 3: Best-in-Class PACE Framework for IT GRC**

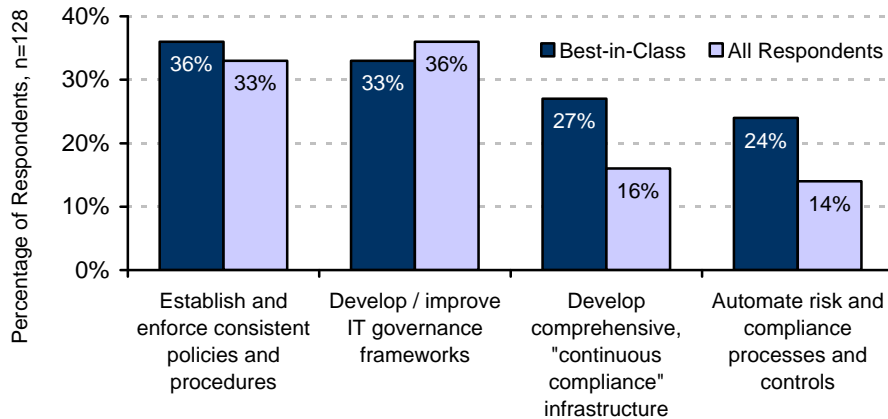
Pressures	Actions	Capabilities	Enablers (Percent of Best-in-Class Adoption)
<ul style="list-style-type: none"> <li>▪ Improve operational efficiencies (reduce total cost)</li> <li>▪ Provide enterprise-wide visibility (improve decision-making)</li> <li>▪ Mitigate IT risks (technology, operational)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Establish and enforce consistent IT policies and procedures</li> <li>▪ Develop / improve IT governance frameworks</li> <li>▪ Develop "continuous compliance" infrastructure</li> <li>▪ Automate risk and compliance processes and controls</li> </ul>	<ul style="list-style-type: none"> <li>▪ Consistent policies and procedures for IT compliance</li> <li>▪ Consistent policies and procedures for IT risk management</li> <li>▪ IT vulnerability assessments</li> <li>▪ IT risk assessments (qualitative and quantitative)</li> <li>▪ Responsible executive or team with primary ownership of IT GRC initiative</li> <li>▪ Communication of corporate policies, practices and expectations for ethical behavior</li> <li>▪ Repository of log, information and event data to support analysis, audit, reporting or investigation</li> <li>▪ Repository of applicable laws and regulations</li> <li>▪ Repository of risks and risk-related information</li> <li>▪ Modeling of interconnections and dependencies of IT risks</li> <li>▪ Modeling of how IT risks impact expenditures and corporate objectives</li> <li>▪ Modeling of impact of unmitigated risk versus cost of mitigation</li> </ul>	<ul style="list-style-type: none"> <li>▪ Log management (55%)</li> <li>▪ Security information and event management (49%)</li> <li>▪ e-Discovery tools (36%)</li> <li>▪ IT-GRC platform / software (33%)</li> <li>▪ Enterprise risk management platform / software (30%)</li> <li>▪ Case management / incident management tools (49%)</li> <li>▪ Legal matter management (39%)</li> <li>▪ Regulation-specific software solutions (39%)</li> <li>▪ Business process modeling (39%)</li> <li>▪ Economic scenario generation / forecasting software (24%)</li> </ul>

Source: Aberdeen Group, May 2009

### Best-in-Class Strategies and Results

Best-in-Class strategies to **establish consistent policies and develop IT governance frameworks** are similar to those of all respondents in the current study (Figure 3). But the top performers are differentiated by their commitment to **automation** of risk and compliance processes and controls, and by their commitment to the development of a “**continuous compliance**” infrastructure. As one project manager for a global services firm put it, the Best-in-Class companies understand that “if you stay compliant, you don’t have to get compliant.”

**Figure 3: Top Strategies Driving Current Investments in IT GRC**



Source: Aberdeen Group, May 2009

Given the relative maturity of their IT GRC initiatives, the Best-in-Class are now becoming more concerned with managing risk than with sustaining compliance and safeguarding critical data. Just over half (52%) of Best-in-Class companies cited **managing risks across the enterprise** as their leading concern over the next 12 months, which was nearly two-times higher than their second leading concern, **sustaining compliance with changing regulatory requirements** (27%).

Table 4 presents some of the advantages that the IT GRC initiatives of Best-in-Class organizations are yielding, in comparison to those of their Industry Average and Laggard counterparts. Respondents in the current study were asked to estimate the degree of change their organization had experienced over the last 12 months, across a number of dimensions related to IT governance, risk management and compliance. High-level conclusions that can be drawn from the findings in Table 4 include the following:

- Best-in-Class organizations are seeing significantly larger gains in their ability to identify, assess and prioritize risks
- Risk management initiatives at Best-in-Class organizations provide management with better access and visibility to current risk status, and better communication of risks to key stakeholders
- Best-in-Class companies have better capabilities to translate risk assessment data into actionable recommendations, enabling faster decision-making
- Best-in-Class organizations are significantly better than other respondents at compliance-related tracking and reporting, and report better flexibility to adjust to new or updated regulatory requirements
- Compliance initiatives at Best-in-Class organizations provide management with better access and visibility to current compliance

status, and better communication of compliance status to key stakeholders

**Table 4: Average Year-over-Year Changes in Risk Management and Compliance Capabilities**

Capabilities in Risk Management and Compliance		Best-in-Class	Average	Laggards
<b>Risk Management</b>	Effectiveness of risk detection and assessment	11.9%	7.8%	1.4%
	Identification of weaknesses in existing risk management processes	11.2%	7.1%	0.0%
	Precision of risk prioritization	10.5%	3.2%	1.7%
	Elimination of redundant risk management activities / processes	8.5%	2.9%	-0.8%
	Management's ability to access current risk status	11.1%	8.0%	1.5%
	Ability to provide clear, timely communication of risks to shareholders and board of directors	8.9%	4.9%	0.7%
	Ability to translate risk assessment data into actionable recommendations	9.6%	5.8%	0.0%
	Speed at which business-critical decisions are able to be made based on enhanced visibility into current risk thresholds	9.8%	4.8%	-2.0%
<b>Compliance</b>	Efficiency of compliance tracking and reporting	12.0%	7.5%	1.9%
	Flexibility to adjust to new or updated regulatory requirements	11.5%	4.8%	0.0%
	Elimination of redundant compliance activities / processes	6.5%	3.8%	0.2%
	Detection of gaps and weaknesses in internal compliance controls and procedures	6.0%	3.5%	0.0%
	Management's ability to access company's current compliance status	12.2%	5.0%	1.0%
	Communication of current compliance status to board of directors and shareholders	9.3%	4.8%	0.1%
	Speed at which business-critical decisions are able to be made resulting from improved visibility into company's current compliance status	8.9%	4.9%	-0.8%

Source: Aberdeen Group, May 2009

**Aberdeen Insights – Strategy**

The rise in importance of IT governance, risk management and compliance ("IT GRC") reflects the increasing recognition that the strategic value of IT lies not in the mere technology itself (which is generally accessible to everyone), but in how it is applied and managed most effectively. For the IT function, the "GRC" acronym is not listed in the actual order of appearance of formal corporate initiatives.

*continued*

"There's probably a smarter way to do things, but we're doing the easier things first."

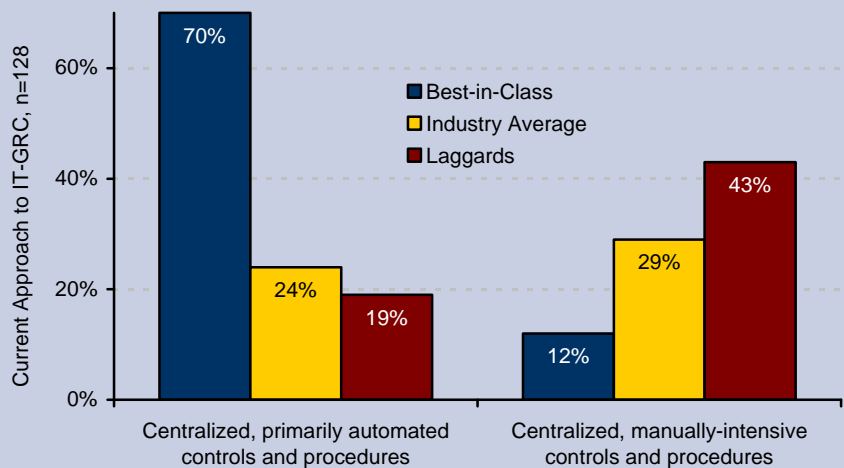
~ Information Risk Manager, US-based discount retailer

### Aberdeen Insights – Strategy

Based on the findings from Aberdeen's benchmark research, the *de facto* order for IT GRC has been **first compliance, then IT governance, then IT risk management**, a pattern which holds true across all maturity classes. The research also shows that Best-in-Class organizations are 2.3-times more likely to have adopted a "continuous improvement" approach to their IT GRC initiatives, underscoring their commitment to managing IT as a strategic asset.

In addition, Best-in-Class companies are significantly more likely than Industry Average or Laggards to describe their current approach to IT GRC as "centralized" and "primarily automated" (Figure 4). Two-thirds of the Best-in-Class further characterize their IT GRC initiatives using attributes such as "risk-based," "event-driven," and featuring "automated workflows for incident response." In contrast, Laggards in the current study are 3.5-times more likely to be using "manually intensive" controls and procedures. While this is consistent with the general "Crawl, Walk, Run" pattern commonly seen in Aberdeen's information technology research, the point is not to be good at the process of compliance, or governance, or risk management for its own sake – the point is to harness IT more effectively in support of achieving business objectives and managing financial, strategic, and operational risks.

**Figure 4: Best-in-Class IT GRC is Centralized and Automated**



Source: Aberdeen Group, May 2009

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

## Chapter Two: Benchmarking Requirements for Success

Strategies to make well-informed business decisions in the context of the organization's requirements for compliance and appetite for risk ultimately lead to the selection and deployment of one or more specific enabling technologies. These choices – along with the policy, planning, process, and organizational elements of implementation – are critical factors in the success of an organization's IT GRC initiatives.

### Case Study – Mid-Size High Tech, Northeastern US

A mid-size high tech company, with headquarters in the northeastern United States, provided some historical insight into the evolution of its IT GRC initiatives as they have unfolded over the past several years.

"Our first steps in this area were definitely driven by compliance, in particular SOX," noted the organization's CIO. "Like many companies during that period, we went down a tremendous learning curve as a number of internal processes were being documented for the first time." With each annual planning and budgeting cycle, incremental steps were taken with the goal of better aligning the company's IT investments with its strategy and financial plans. A formal IT governance committee, comprised of leaders from multiple functional areas, was convened quarterly to evaluate the current portfolio of IT projects ("which were always more in both number and cost than we had resources to do") in light of strategic objectives, impact on revenue and expense, and available project resources. Recommendations made by the committee were still taken to the CEO and his staff for review and final approval, but with the prior benefit of the cross-functional discussion, evaluation of alternatives, and eventual buy-in. Successive annual iterations have led to steady improvements in automation, structure, consistency, speed and cost.

### Competitive Assessment

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

### Fast Facts

Percentage of companies that enforce formal separation of duties:

- √ Best-in-Class: 67%
- √ Industry Average: 33%
- √ Laggards: 29%

"Our earliest IT governance meetings were extremely time-intensive, based primarily on manually prepared information. And the discussions were basically subjective, such as the relative importance of an SAP project to close the books more quickly in our Japanese subsidiary versus a secure Web portal project to streamline transactions with our value-added resellers. But we were successful in getting the company's business leaders to think and work together in terms of strategy, financials, operations, compliance, and risk. That has been and remains the real win for IT GRC."

~ CIO,  
Mid-Size High Tech Company

**Table 5: Competitive Framework for IT GRC**

	<b>Best-in-Class</b>	<b>Average</b>	<b>Laggards</b>
<b>Process</b>	Consistent policies, procedures for IT compliance		
	73%	50%	45%
	Consistent policies, procedures for IT risk management		
	70%	48%	45%
	IT vulnerability assessments		
	70%	45%	31%
<b>Organization</b>	IT risk assessments (qualitative and quantitative)		
	58%	35%	29%
	Responsible executive or team with primary ownership of IT GRC initiative		
	85%	55%	49%
	Communication of corporate policies, practices and expectations for ethical behavior		
	64%	51%	38%
<b>Knowledge Management</b>	Repository of log, information and event data to support analysis, audit, reporting or investigation		
	76%	39%	29%
	Repository of applicable laws and regulations		
	58%	36%	28%
	Repository of risks and risk-related information		
55%	29%	22%	
<b>Technology</b>	Modeling of interconnections and dependencies of IT risks		
	36%	24%	10%
	Modeling of how IT risks impact expenditures and corporate objectives		
	27%	12%	4%
	Modeling of impact of unmitigated risk versus cost to mitigate		
24%	12%	8%	
For IT GRC-related solutions in current use, refer to Figure 14 and Figure 15			
<b>Performance Management</b>	Collection of all information required for auditing and reporting		
	64%	50%	31%
	Compliance with frequency required for auditing and reporting		
	61%	33%	29%
	Confirmed accuracy of collected compliance data		
52%	26%	19%	

Source: Aberdeen Group, May 2009

## Capabilities and Enablers

Based on the comparisons within the Competitive Framework and interviews with select respondents, analysis of the Best-in-Class highlights the degree to which they have developed their IT GRC initiatives beyond those of their Industry Average and Laggard counterparts.

### Process

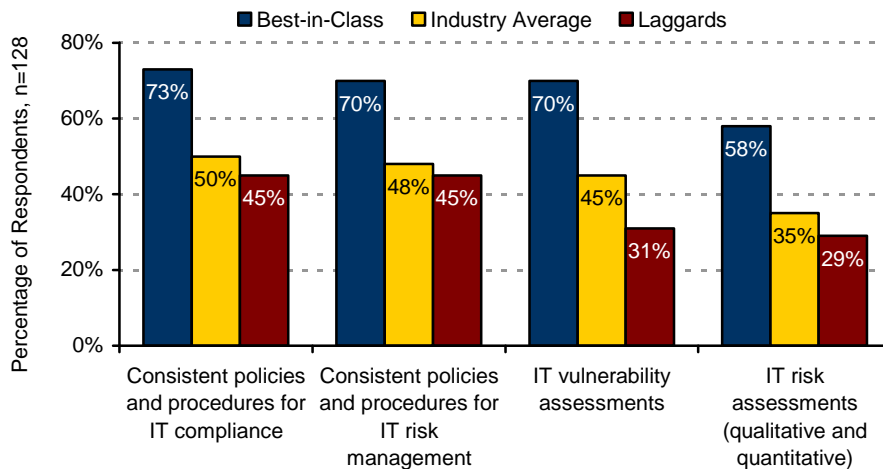
**Consistent policies for compliance and risk management** are a foundation for successful IT GRC initiatives, as are **IT vulnerability assessments** and **IT risk assessments** (Figure 5). Of these, risk assessments – both qualitative and quantitative – are seen to be the most difficult. Just three out of five (58%) Best-in-Class organizations indicate this as a current capability, although this still is two-times more so than Laggards.

For Best-in-Class organizations, IT GRC initiatives are more likely – by a factor of between two-times and three-times compared to Laggards – to have incorporated industry standard frameworks and best practices such as ISO, ITIL, COBIT and COSO. A clear advantage of not reinventing the wheel is that one gets to spend more time and energy rolling forward.

"There is no business advantage whatsoever to building a new business process, when you can build on accepted frameworks such as ISO, ITIL and COBIT."

~ CIO,  
US Manufacturing Company

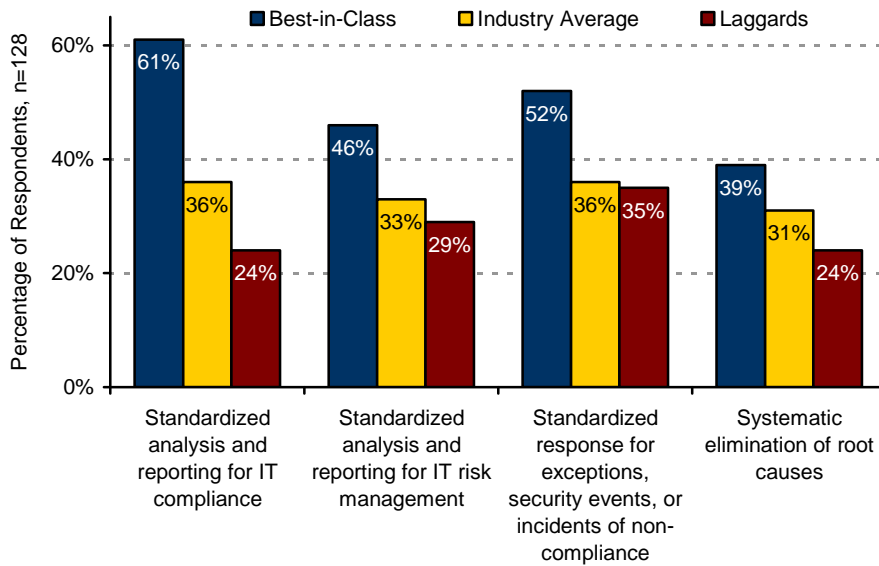
**Figure 5: Consistent Policies; Regular Assessments**



Source: Aberdeen Group, May 2009

Aberdeen's research continues to show that **standardization** is the friend of enterprise-wide initiatives, not only in analysis and reporting but also in response to exceptions, events, or incidents of non-compliance (Figure 6). Also consistent with previous research, **systematic elimination of root causes** is an obvious opportunity for ongoing improvement. Industry Average and Laggard companies try to get more proficient at catching the dogs running around in their back yards, but Best-in-Class companies take steps to keep the dogs from getting loose the next time.

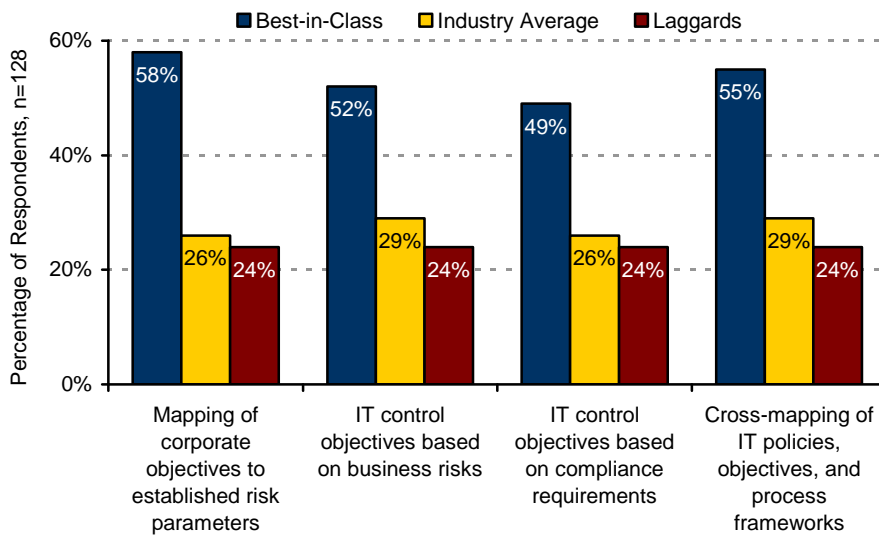
**Figure 6: Standardization and Elimination of Root Causes**



Source: Aberdeen Group, May 2009

**Establishing the links between the organization's business objectives, risk parameters, IT controls, and external compliance requirements** is the very heart of successful IT GRC initiatives, and Best-in-Class companies are more than twice as likely as their Industry Average and Laggard counterparts to note this as a current capability (Figure 7). Still, less than three out of five of the top performers are currently doing so, indicating a nearly universal opportunity for improvement.

**Figure 7: Linking Objectives, Risks, Controls, and Compliance**

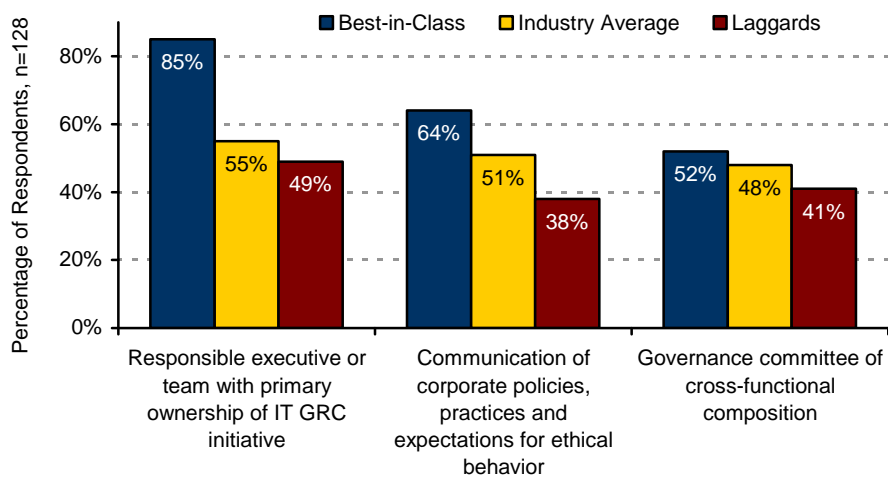


Source: Aberdeen Group, May 2009

## Organization

Time and again, Aberdeen's research confirms that **establishing primary ownership** for any important cross-enterprise initiative is a distinguishing characteristic of the companies with top results. The current study follows the same pattern: 85% of Best-in-Class companies have assigned primary ownership of their IT GRC initiatives to a responsible executive or team (Figure 8) – the "one throat to choke" principle. In addition, the typical good news / bad news pattern holds true in terms of investments in end-user training. The good news: the Best-in-Class are 1.7-times more likely than Laggards to invest in communication of corporate policies, practices, and expectations for ethical behavior. The bad news: just two-thirds (64%) of the Best-in-Class currently make such an investment.

**Figure 8: One Throat to Choke; Communication of Expectations**



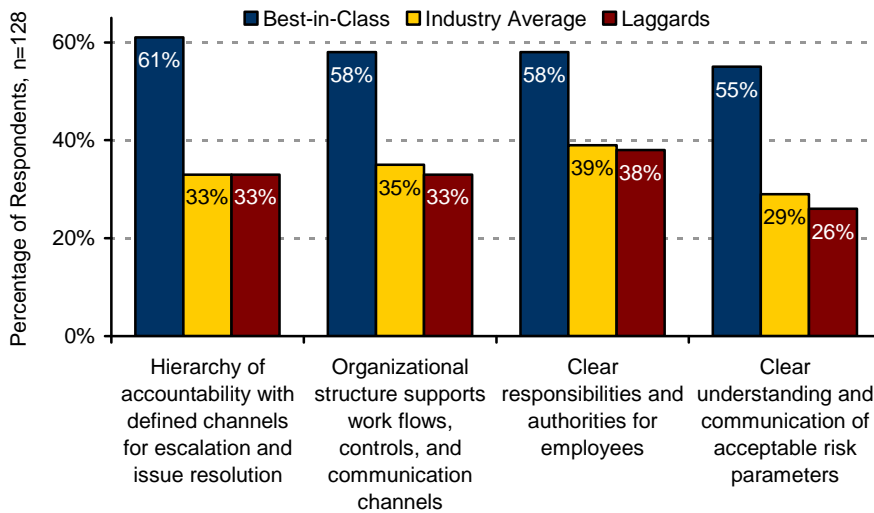
Source: Aberdeen Group, May 2009

In the more successful IT GRC initiatives, organizational structures are "wired" for work flow, problem escalation, and problem resolution (Figure 9). Best-in-Class companies support the **responsibility and authority** given to individual employees with **communication and clarity** around what the company views as acceptable parameters of risk. These best practices are arguably even more important for the less centralized, less automated early days of most IT GRC initiatives, although the research shows that diffused responsibility and poor communications too often go hand-in-hand.

Leadership for IT GRC initiatives tends to be provided by the highest levels of Best-in-Class organizations, i.e., in the majority of top performers the CEO, Chief Compliance Officer, CIO, CFO, CTO, CISO, Chief Risk Officer, or COO is identified as either the leader or as a key contributor. For all other respondents, leadership and contributions for IT GRC initiatives is more widely dispersed. Interestingly, the research shows that budgetary decisions for IT GRC initiatives are predominantly at the CIO and CEO level – not with the CFO – in Best-in-Class organizations. Once again, this

highlights the commitment of top performers to managing IT as a strategic asset that enables the company's pursuit of rewarded risks, rather than as a tactical expense.

**Figure 9: "Wiring" Organizations to Support IT GRC**

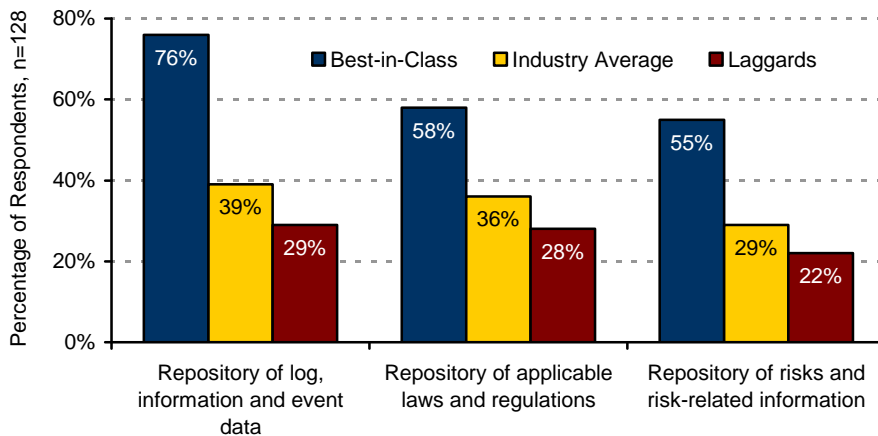


Source: Aberdeen Group, May 2009

### Knowledge Management

Best-in-Class organizations take a **fact-based** approach to IT GRC, for example by establishing central repositories for *log, information and event data*; for applicable *laws and regulations*; and for *risks and risk-related information* (Figure 10). Aberdeen's benchmark study on [Leveraging Logs, Information and Events](#) (March 2009) provides additional insights into how Best-in-Class companies derive more value from the complex IT environments and services that are the foundations for running and growing their business.

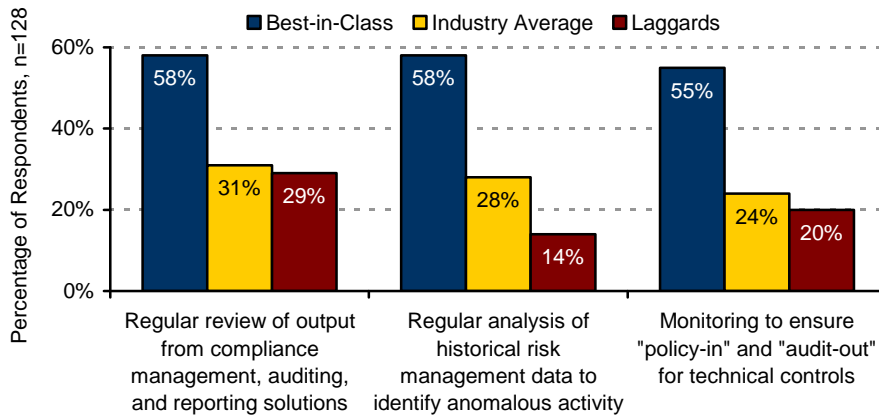
**Figure 10: Fact-Based Approach to IT GRC**



Source: Aberdeen Group, May 2009

Best-in-Class organizations not only gather the facts, but also are twice as likely as all others to **review and analyze** the facts they have gathered (Figure 11). About three out of five (58%) Best-in-Class organizations regularly review the auditing and reporting output from their compliance and risk management solutions, compared to less than one-third of all other respondents.

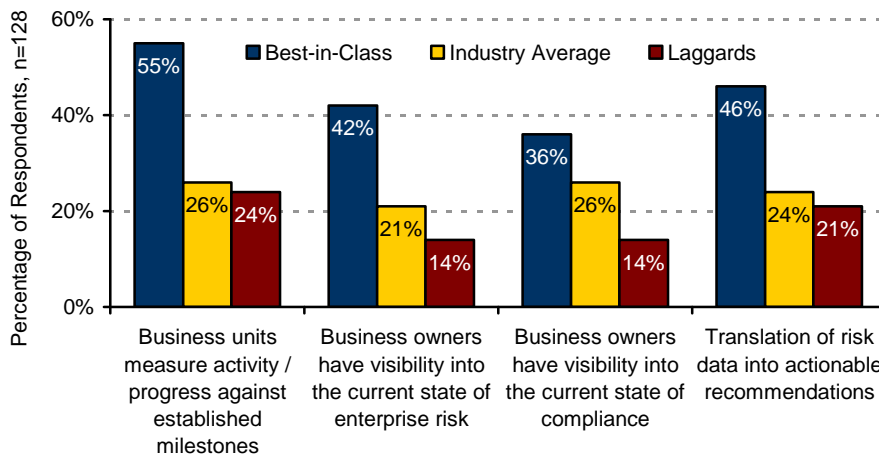
**Figure 11: Regular Monitoring, Analysis and Review**



Source: Aberdeen Group, May 2009

Along the same lines, Best-in-Class organizations are more than twice as likely as all others to provide their business owners with better **visibility** into the current state of risk, compliance, and progress against established strategic milestones...as well as to translate risk data into actionable recommendations (Figure 12). This is where real "governance" takes place.

**Figure 12: Increased Visibility and Actionable Recommendations**

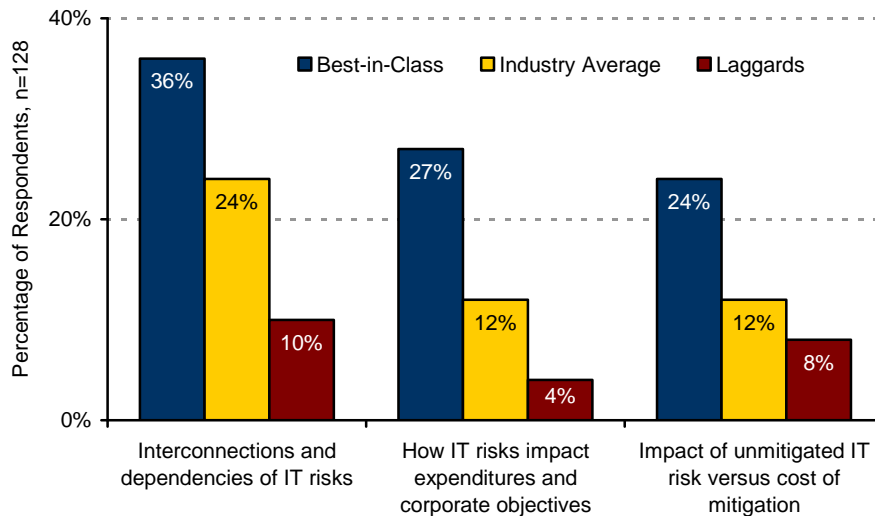


Source: Aberdeen Group, May 2009

## Technology

Modeling the interconnections and dependencies between IT risks, understanding how they impact budgets and corporate objectives, and the ability to conduct “what-if” analysis regarding the costs and benefits of mitigation are newly emerging capabilities, but their use is significantly higher among the companies with top results (Figure 13). In individual interviews with select survey respondents, for most companies this is currently an area of open-ended discussion, intuition and ultimately judgment calls by the decision-making body, though all were quick to acknowledge the appeal of a more analytical approach.

**Figure 13: Modeling Risks, Dependencies, Cost and Objectives**

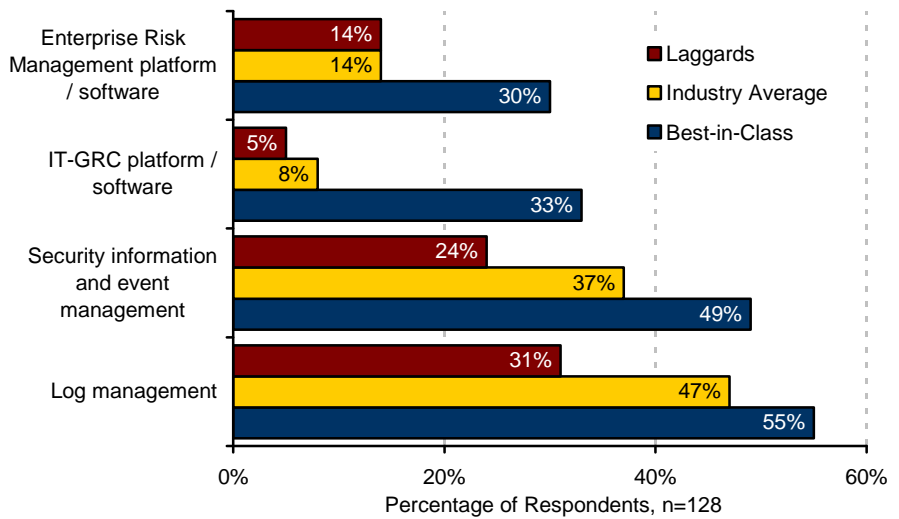


Source: Aberdeen Group, May 2009

**Log management and security information and event management (SIEM)** solutions are becoming more mainstream in Best-in-Class IT GRC initiatives (Figure 14), and in [Leveraging Logs, Information and Events](#) (March 2009) Aberdeen described how Best-in-Class organizations are using these technologies to enhance security, to achieve and sustain regulatory compliance, and to improve the efficiency and cost-effectiveness of their ongoing operations. [The Role of SIEM in GRC](#) (March 2008) also provides useful insight in this area.

The research shows that **IT GRC software** and **Enterprise Risk Management software** are in early adoption by the organizations with top results, with about 30% of Best-in-Class companies indicating current use (Figure 14). Using planned deployments in the next 12 months versus current deployments as a proxy for near-term market opportunity, the research indicates strong (greater than 50%) growth rate for both types of solutions, off a modest current base. In addition, the relatively high percentage of respondents indicating that they are currently evaluating these solutions further illustrates a high level of market interest in both of these areas.

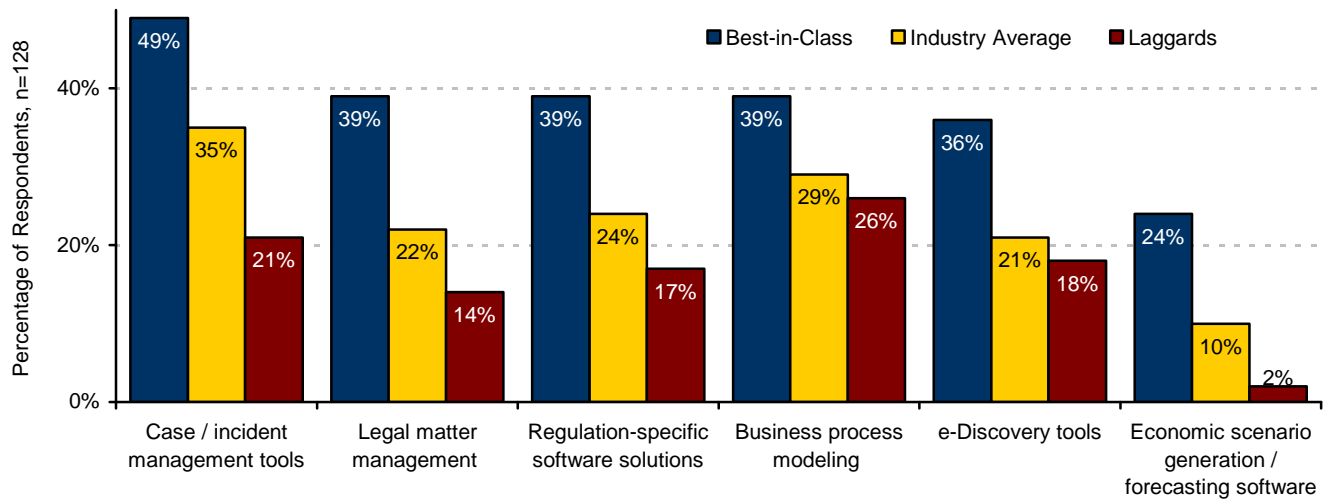
**Figure 14: Enabling Technologies Currently Used for IT GRC**



Source: Aberdeen Group, May 2009

Current use data for several additional enabling technologies related to IT GRC initiatives was gathered in this study, as summarized in Figure 15.

**Figure 15: Enabling Technologies Currently Used for IT GRC (continued)**



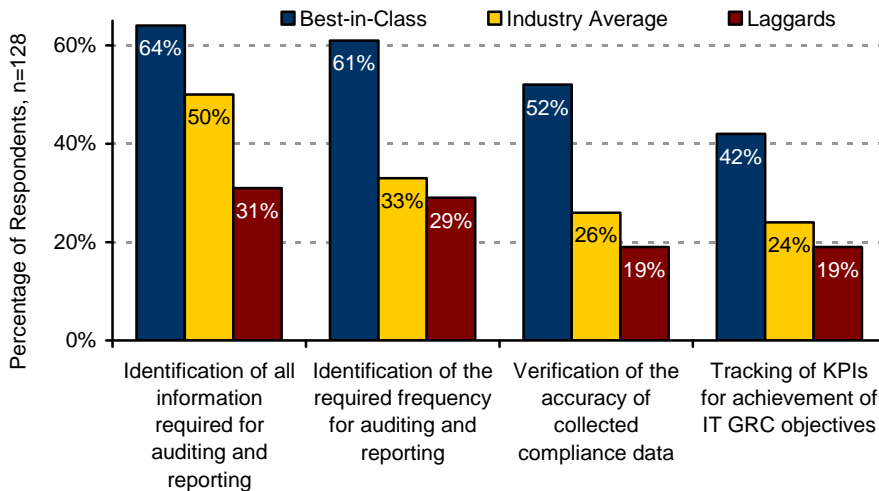
Source: Aberdeen Group, May 2009

### Performance Management

Best-in-Class organizations **identify both the type and the frequency** of the data they need for auditing and reporting (Figure 16). In addition, **measuring and tracking** of the relevant key performance indicators necessary for the achievement of the company's IT GRC objectives is an emerging capability that distinguishes top performance. The practical wisdom noted in a song from *Ain't Misbehavin'* – "find out what they like, and

how they like it, and let them have it just that way" – also holds true for top performance in IT GRC.

**Figure 16: Identifying, Tracking, Verifying Relevant Information**



Source: Aberdeen Group, May 2009

**Aberdeen Insights – Technology**

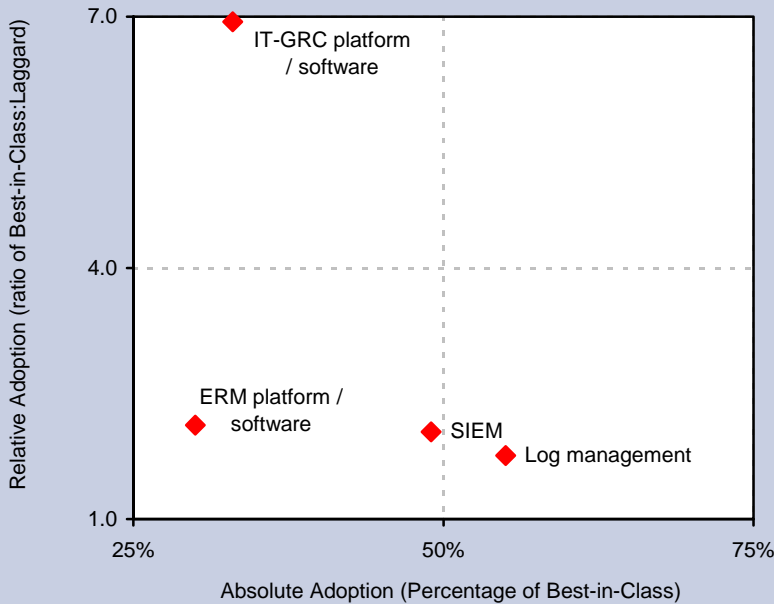
In the context of IT GRC initiatives, **log management** and **security information and event management (SIEM)** are becoming *baseline* technologies, in the sense that they are becoming used not only by a majority of the Best-in-Class but also by a relatively high proportion of other respondents (Figure 17). Aberdeen’s March 2009 benchmark on [Leveraging Logs, Information and Events](#) describes how Best-in-Class organizations are using these technologies to enhance security, to achieve and sustain regulatory compliance, and to improve the efficiency and cost-effectiveness of their ongoing operations.

**IT-GRC “platform” solutions** are in the *early adoption* phase by the Best-in-Class (modest absolute adoption; high relative adoption), while **Enterprise Risk Management “platform” solutions** are in the *emerging* quadrant for the Best-in-Class companies in this dataset.

*continued*

**Aberdeen Insights – Technology**

**Figure 17: Market Trends: Absolute versus Relative Adoption**



Source: Aberdeen Group, May 2009

For all respondents, **integration with existing technology investments** and **flexibility of configuration** are the leading selection criteria for IT-GRC or Enterprise Risk Management solutions. With respect to attributes of the solution provider, **domain expertise** and **comprehensiveness of offering** are the selection criteria that top the list. With respect to the total cost of ownership, **cost of deployment** and **cost of ongoing management** outweigh the cost of acquisition, underscoring the longer-term perspective of the companies adopting these technologies.

## Chapter Three: Recommended Actions

Whether a company is trying to move its performance in IT GRC from Laggard to Industry Average, or Industry Average to Best-in-Class, the research shows that the following actions will help bring about the desired performance improvements.

### Laggard Steps to Success

- **Lay the foundation.** Less than one-third of Laggards currently conduct regular IT vulnerability assessments (31%) and IT risk assessments (29%); these will provide a good jumping off point for new compliance, governance, or risk management initiatives.
- **Establish consistent policies.** Less than half (45%) of Laggard organizations have established consistent policies for compliance and risk management. Industry standard frameworks and best practices such as ISO, ITIL, and COBIT provide a solid reference and will significantly accelerate progress.
- **Assign an owner.** Less than half (49%) of Laggards have established an executive or team with primary ownership of their IT GRC initiatives. Time and again, Aberdeen's research confirms that the "one throat to choke" principle is highly correlated with the achievement of top results.

### Industry Average Steps to Success

- Industry Average organizations should also follow the three recommendations for Laggards as noted above. As summarized in Table 5, the current differences between Industry Average and Laggards in these particular areas are small.
- **Set up repositories for the facts.** Fewer than two out of five Industry Average organizations have established central repositories for log, information, and event data (39%); for applicable laws and regulations (36%); and for risks and risk-related information (29%). These repositories enable a fact-based approach to IT GRC, and set up the ability to regularly review and analyze the auditing and reporting output from compliance and risk management solutions.

### Best-in-Class Steps to Success

- **Increase the focus on risk.** Risk assessments – both qualitative and quantitative – are noted as a current capability by just three out of five (58%) of Best-in-Class organizations in the study. As IT GRC initiatives mature from compliance, to IT governance, to IT risk management, such assessments represent the jumping off point for the next phase.

#### Fast Facts

Largest projected budget increases in the next fiscal year (all respondents):

- ✓ Risk management assessment and consulting services: 5.3%
- ✓ Risk-based analytic tools (e.g. tracking and reporting): 4.8%
- ✓ IT GRC platform / software: 4.8%

"IT sometimes overinvests in controls that are currently in vogue. What we always need to keep in top of mind is that the business needs what the business needs."

~ Director of Information Security Governance, Regional Health Services Provider

- **Expand repositories for the facts.** Although three-fourths (76%) of Best-in-Class companies have currently established central repositories for log, information and event data, just over half have currently done so for applicable laws and regulations (58%) and for risks and risk-related information (55%).
- **Expand the ability to model.** Modeling the interconnections and dependencies between IT risks, understanding how they impact budgets and corporate objectives, and the ability to conduct “what-if” analysis regarding the costs and benefits of mitigation are newly emerging capabilities. Less than two out of five of the top performers currently exploit these kinds of technologies, indicating sizeable opportunities for improvement.

### Aberdeen Insights – Summary

Best-in-Class organizations are making greater strides in their IT GRC initiatives than the other companies in the study, which translates to strategic and operational benefits that include the following:

- Significantly larger year-over-year improvements in their ability to identify, assess and prioritize risks
- Better access and visibility for business owners regarding current risk status
- Better communication of risks to key stakeholders
- Better capabilities to translate risk assessment data into actionable recommendations, enabling faster decision-making
- Significantly greater year-over-year improvements in compliance-related tracking and reporting
- Better flexibility to adjust to new or updated regulatory requirements
- Better access and visibility for business owners to current compliance status
- Better communication of compliance status to key stakeholders

Aberdeen's current research demonstrates that IT GRC initiatives are continuing to grow in relevance, as a direct result of their ability to apply and manage IT more effectively and thereby to maximize its strategic value to the organization.

## Appendix A: Research Methodology

Between April and May 2009, Aberdeen examined the use, the experiences, and the intentions of more than 130 enterprises in a diverse set of industries with respect to their approach to IT Governance, Risk Management and Compliance (IT GRC). Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on their respective strategies, experiences, and results.

Responding enterprises had the following demographics:

- *Job title / function:* The research sample included respondents with the following job titles: C-level (22%); Vice President / General Manager (14%); Director (8%); Manager (25%); Staff / Consultant (21%); and other (10%). The largest segment by functional responsibility was IT, representing 33% of the total sample.
- *Industry:* The research sample included respondents from a wide range of industries. The largest segments included financial services (14%), government / aerospace / defense (9%), and insurance (6%).
- *Geography:* A majority of respondents (49%) were from the Americas. Remaining respondents were from the Asia-Pacific region (18%) and Europe / Middle East / Africa (33%).
- *Company size:* Twenty-eight percent (28%) of respondents were from large enterprises (annual revenues above US \$1 billion); 40% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 33% of respondents were from small businesses (annual revenues of \$50 million or less).

### Focus of the Study

Respondents completed an online survey that included questions designed to determine the following:

- √ The degree to which technologies used to enable IT GRC initiatives are currently deployed, and the financial impact of those technologies
- √ The efficiency and effectiveness of existing implementations
- √ Benefits that have been derived with respect to enhancing security, sustaining compliance, managing risk, and optimizing ongoing operations

The study aimed to identify current and emerging best practices for IT GRC, and to provide a framework by which readers can assess their own current capabilities.

**Table 6: PACE Framework Key**

Overview
<p>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:</p> <p><b>Pressures</b> – external forces that impact an organization’s market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive)</p> <p><b>Actions</b> – 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)</p> <p><b>Capabilities</b> – the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p><b>Enablers</b> – 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)</p>

Source: Aberdeen Group, May 2009

**Table 7: Competitive Framework Key**

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

Source: Aberdeen Group, May 2009

**Table 8: Relationship Between PACE and the Competitive Framework**

PACE and the Competitive Framework – How They Interact
<p>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.</p>

Source: Aberdeen Group, May 2009

## Appendix B: Related Aberdeen Research

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

- [LogLogic Rolls Forward with the Acquisition of Exaprotect](#); May 2009
- [Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data](#); March 2009
- [NitroSecurity Expands SIEM Integration](#); March 2009
- [Secure, Compliant and Well-Managed: The IT Security Approach to GRC](#); February 2009
- [Enterprise Risk Management: The Art of Avoiding Unpleasant Surprises](#); February 2009
- [Continuously Compliant: Ensuring Proactive, Comprehensive Compliance](#); September 2008
- [Is Your GRC Strategy Intelligent? Analytics for Accurate, Real-Time Visibility and Decision Making](#); July 2008
- [Driving Sustainable Business Advancements through GRC: The Convergence of Governance, Risk, and Compliance](#); April 2008
- [The Role of SIEM in GRC](#); March 2008
- [Security Governance and Risk Management](#); November 2007

Information on these and any other Aberdeen publications can be found at [www.aberdeen.com](http://www.aberdeen.com).

Author(s): Derek E. Brink, Vice President and Research Fellow, IT Security, ([derek.brink@aberdeen.com](mailto:derek.brink@aberdeen.com)) with Stephen Walker

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.