

## **Sustaining Compliance**

How I Learned to Stop Worrying and Love the Security Audit

September 2007



## Executive Summary

This research benchmark provides insight and recommendations for all organizations that are compelled to manage, audit, and report on security-related systems and information for purposes of demonstrating compliance with industry regulations, government regulations, industry standards and best practices, or internal policies. By doing so on a more consistent and repeatable basis, Best-in-Class organizations have demonstrated their ability to lower operational costs, support higher scale, reduce security risks, and maintain consistent policies for security and compliance.

### Research Benchmark

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

### Best-in-Class Performance

---

Aberdeen used the following performance criteria to distinguish Best-in-Class organizations from Industry Average and Laggard organizations:

- Decrease in the number of non-compliance incidents, number of security-related incidents, and number of false positives
- Decrease in the time required to complete a compliance-related audit
- Increase in the number of systems requiring updates, patches, and configuration changes actively being managed, and increase in the number of systems generating logs actively being managed

Companies with top performance based on these criteria (on a year-over-year basis) earned Best-in-Class status.

### Competitive Maturity Assessment

---

Survey results show that the organizations achieving Best-in-Class performance shared several common characteristics, including:

- 85% have consistent security and compliance policies
- 83% have a responsible executive or team with primary ownership for security-related compliance initiatives
- 61% regularly review and analyze data from compliance management, auditing, and reporting solutions
- 83% have enabled update / patch facilities on all appropriate devices
- 67% have enabled logging on all appropriate sources
- 58% have implemented controls to monitor and verify that policy and regulatory requirements are being satisfied

"They would ask me, 'are we compliant?' and I had to say to myself, I don't really know... at three o'clock on Tuesday we were, but who knows what's come along since then, or where our systems may have drifted?"

~Chief Security Officer, Midsize Health Services Company

### Required Actions

---

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance organizations should recognize that security and compliance initiatives are a journey, not a destination, and dedicate resources for sustained programs and continuous improvement.

## Table of Contents

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Required Actions.....	2
Chapter One: Benchmarking the Best-in-Class .....	4
Business Context .....	4
Aberdeen's Maturity Class Framework .....	5
The Best-in-Class PACE Framework .....	6
Best-in-Class Strategies.....	7
Chapter Two: Benchmarking Requirements for Success .....	10
Competitive Assessment.....	11
Capabilities and Enablers.....	13
Process.....	13
Organization .....	13
Knowledge Management.....	13
Technology.....	13
Performance Management.....	13
Chapter Three: Required Actions .....	16
Laggard Steps to Success.....	16
Industry Average Steps to Success .....	16
Best-in-Class Steps to Success.....	16
Appendix A: Research Methodology.....	18
Appendix B: Related Aberdeen Research.....	20

## Figures

Figure 1: Leading Drivers for Security-Related Compliance.....	5
Figure 2: Strategic Approach to Security-Related Compliance.....	7
Figure 3: Strategic Actions Driving Current Investments in Compliance Initiatives.....	8
Figure 4: Selected Enabling Technologies Deployed in Support of Security and Compliance Initiatives .....	14

## Tables

Table 1: Organizations with Top Performance Earn Best-in-Class Status .....	5
Table 2: Best-in-Class PACE Framework.....	6
Table 3: Competitive Framework.....	11
Table 4: PACE Framework Key.....	19
Table 5: Competitive Framework Key.....	19
Table 6: Relationship Between PACE and Competitive Framework.....	19

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

### Business Context

---

Network and security infrastructures have greatly increased both the volume and the variety of deployed systems – systems which require updates, patches, and configuration changes, and which generate logs of security information and events. At the same time, industry and government regulations have compelled organizations of all types and sizes to manage, audit, and report on security-related systems and information on a more consistent and repeatable basis for purposes of demonstrating compliance.

Today, tactical deployment of point solutions for addressing compliance on an as-needed basis is still the most prevalent approach for organizations across the board. Best-in-Class organizations, however, have begun to view compliance not as an event, but as a strategic, sustainable program – which in addition to helping them to achieve and maintain compliance requirements, also helps them to:

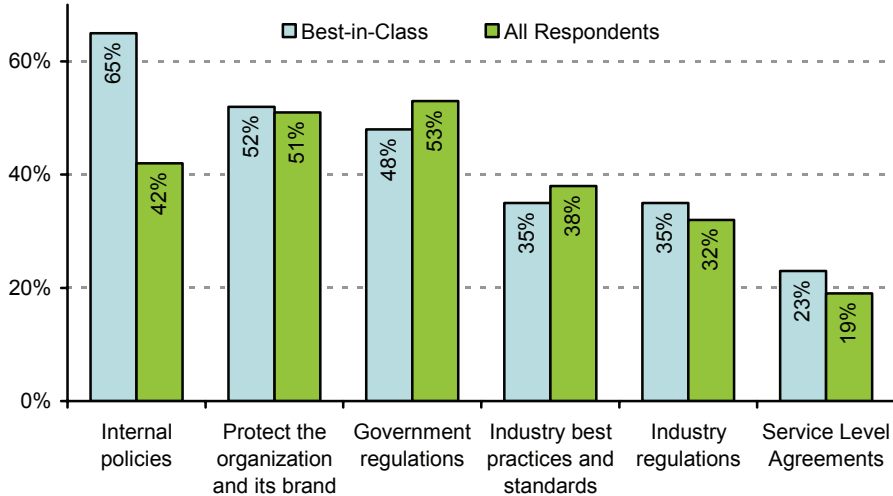
- Lower operational costs – 44% of Best-in-Class organizations reduced the cost of addressing non-compliance incidents over the last year; 26% reduced the cost of addressing security-related incidents. Both of these measures are up to 15-times higher than those for all respondents.
- Support higher scale – 86% of Best-in-Class organizations reported an increase in the number of systems requiring updates, patches, and configuration changes actively under management over the past year; 71% reported an increase in the number of systems generating logs actively under management. Both of these measures are more than 40% higher than those for all respondents.
- Reduce security risk – 48% of Best-in-Class organizations reduced the number of actual security incidents over the past year, compared to an **increase** by a net 7% of all respondents.
- Maintain consistent security policies – 85% of Best-in-Class organizations have established consistent policies for security and compliance, compared to only 68% of all respondents.

"Compliance," taken in all of its dimensions – including compliance with **internal policies, government regulations, industry regulations, and industry standards and best practices** – is understandably the leading driver of current investments in security and compliance initiatives. Another leading driver – protect the organization and its brand – is indicative of the attention organizations are now paying to security and compliance in the wake of frequent public disclosures of security breaches involving consumer data (Figure 1).

### Fast Facts

- √ 59% of all respondents reported an increase in the total number of systems requiring updates, patches, and configuration changes, compared to a year ago; 62% reported an increase in the number actively under management
- √ 58% of all respondents reported an increase in the total number of systems generating logs, compared to a year ago; just 46% reported an increase in the number actively under management

**Figure I: Leading Drivers for Security-Related Compliance**



Source: Aberdeen Group, September 2007

### Aberdeen's Maturity Class Framework

To distinguish Best-in-Class companies from Industry Average and Laggard organizations, Aberdeen used the following performance criteria:

- Decrease in the number of non-compliance incidents, number of security-related incidents, and number of false positives, compared to a year ago
- Decrease in the time required to complete a compliance-related audit, compared to a year ago
- Increase in the number of systems requiring updates, patches, and configuration changes actively being managed, and increase in number of systems generating logs actively being managed, compared to a year ago

Companies with top performance based on these criteria earned Best-in-Class status, as described in Table I. (For additional details on the Aberdeen Maturity Class Framework, see Table 5 in Appendix A.)

**Table I: Organizations with Top Performance Earn Best-in-Class Status**

Definition of Maturity Class	Mean Class Performance
<p><b>Best-in-Class:</b> Top 20% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ 56% decreased the number of security-related incidents in the last 12 months</li> <li>▪ 58% decreased the number of false positives</li> <li>▪ 53% decreased the number of non-compliance incidents</li> <li>▪ 28% decreased the time required to complete an audit</li> <li>▪ 86% increased the number of systems requiring updates, patches, and configuration changes actively being managed</li> <li>▪ 77% increased the number of systems generating logs actively being managed</li> </ul>

Definition of Maturity Class	Mean Class Performance
<p><b>Industry Average:</b> Middle 50% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ 12% decreased the number of security-related incidents in the last 12 months</li> <li>▪ 6% decreased the number of false positives</li> <li>▪ 7% decreased the number of non-compliance incidents</li> <li>▪ 1% decreased the time required to complete an audit</li> <li>▪ 79% increased the number of systems requiring updates, patches, and configuration changes actively being managed</li> <li>▪ 55% increased the number of systems generating logs actively being managed</li> </ul>
<p><b>Laggard:</b> Bottom 30% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ 0% decreased the number of security-related incidents in the last 12 months</li> <li>▪ 0% decreased the number of false positives</li> <li>▪ 0% decreased the number of non-compliance incidents</li> <li>▪ 0% decreased the time required to complete an audit</li> <li>▪ 15% increased the number of systems requiring updates, patches, and configuration changes actively being managed</li> <li>▪ 3% increased the number of systems generating logs actively being managed</li> </ul>

Source: Aberdeen Group, September 2007

### The Best-in-Class PACE Framework

Achieving superior performance in developing and sustaining enterprise security and compliance initiatives requires 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 4 in Appendix A.) The characteristics exhibited by Best-in-Class organizations in this survey are summarized in Table 2.

**Table 2: Best-in-Class PACE Framework**

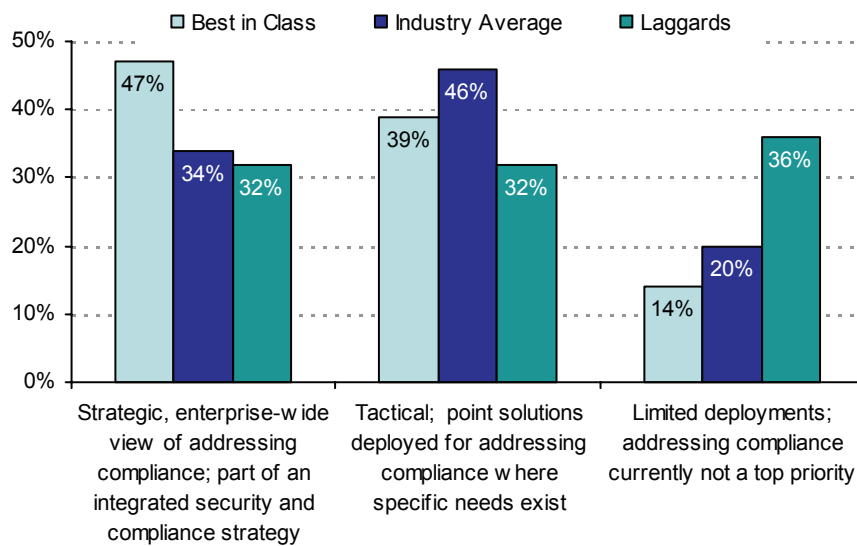
Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> <li>▪ Compliance with internal policies, government regulations, industry regulations, and industry standards and best practices</li> <li>▪ Protect the organization and its brand</li> </ul>	<ul style="list-style-type: none"> <li>▪ Establish and enforce consistent policies and procedures for audit, reporting and management</li> <li>▪ Develop a sustainable, "continuous" compliance infrastructure through automation and streamlining of management, audit, and reporting processes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Formal risk assessments</li> <li>▪ Consistent security and compliance policies</li> <li>▪ Repeatable process for determining the organization's security posture (e.g., self-assessment and measurement of IT controls)</li> <li>▪ Standardized audit, analysis, and reporting</li> <li>▪ Regular review and analysis of data from compliance management, auditing, and reporting solutions</li> <li>▪ Responsible executive or team with primary ownership for security-related compliance initiatives</li> </ul>	<ul style="list-style-type: none"> <li>▪ Patch management</li> <li>▪ Configuration and change management</li> <li>▪ Vulnerability management</li> <li>▪ Unified Threat Management (UTM)</li> <li>▪ Log management</li> <li>▪ Security Information Management (SIM)</li> <li>▪ Security Event Management (SEM)</li> <li>▪ Network Access Control (NAC)</li> <li>▪ Network behavior analysis</li> <li>▪ Database monitoring and auditing</li> <li>▪ Identity and Access Management (IAM)</li> </ul>

Source: Aberdeen Group, September 2007

## Best-in-Class Strategies

As shown in Figure 2, tactical deployment of point solutions for addressing compliance where specific needs exist is still the most prevalent approach for companies falling within the Industry Average maturity class (46%). For the majority of Laggards (36%), deployments of solutions for addressing compliance are limited and compliance is currently not a top priority. In contrast, Best-in-Class organizations (47%) lead the way in taking a more strategic, enterprise-wide approach to addressing compliance as part of an integrated security and compliance strategy.

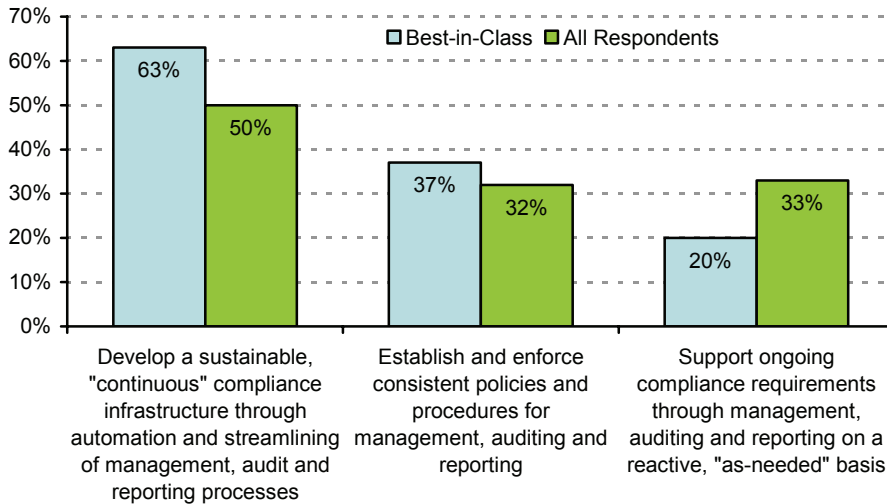
**Figure 2: Strategic Approach to Security-Related Compliance**



Source: Aberdeen Group, September 2007

Compared to all respondents, Best-in-Class organizations are 1.7-times less likely to support ongoing compliance requirements through management, auditing, and reporting on a reactive, as-needed basis. On the contrary, the Best-in-Class are 1.4-times more likely to develop a sustainable, continuous compliance infrastructure through automation, and by streamlining their management, audit and reporting processes (Figure 3).

**Figure 3: Strategic Actions Driving Current Investments in Compliance Initiatives**



Source: Aberdeen Group, September 2007

"I've learned the hard way that one needs to go to senior management and the board with a strategy ... a framework ... a plan that will be implemented and executed over time, with discrete milestones and demonstrable results. You just can't give the impression that we've just now thought of these things, and funding approval is needed yet again on an exception basis. Since recent high-profile data breach disclosures, our board is definitely being proactive at asking questions about our level of security and compliance."

~Business Unit VP,  
Large High-Tech Company

As noted, Best-in-Class organizations employ these strategies not only to achieve and sustain compliance requirements, but also to lower operational costs, support higher scale, reduce security risk, and maintain consistent security and compliance policies. In the next chapter, we will examine in more detail what the leading companies are doing to achieve superior performance in sustaining compliance.

**Aberdeen Insights - Strategy**

"Crawl, Walk, Run" is sound guidance for implementing a successful solution to any number of complex problems. Based on the survey data and direct interviews with respondents from a variety of organizations, it also describes the sequence of strategic approaches taken on the topic of sustaining compliance.

In practice, there is also a discrete strategy that precedes "crawl." Although some might refer to it unkindly as "ignore" or "avoid," but let us politely call it "defer," a strategy identified by some 7% of all respondents. "First they have to hurt," said one exasperated Chief Security Officer, "then you can show them how to make it better."

At some point, however, many compliance initiatives begin as **projects** in which companies scramble to meet deadlines to achieve initial compliance with a specific government or industry regulation. In the survey, 46% of all respondents indicated a current strategy of achieving initial compliance.

*continued*

### Aberdeen Insights - Strategy

Upon initial achievement of compliance, many companies then linger in a mode of supporting ongoing compliance reporting requirements on a reactive, as-needed basis ("to satisfy the audit *du jour*" and "to keep the auditors off our backs" were commonly expressed sentiments). One-third of all respondents indicated this mode as an element of their current strategy. None of the end-users interviewed indicated that they found it satisfactory.

However, Best-in-Class organizations are the first to recognize that compliance is not a one-time event, but an ongoing business **process**. Nearly half of Best-in-Class companies indicated that their current strategy is to develop a sustainable "continuous" compliance infrastructure through the streamlining of management, audit, and reporting processes. Although this is still a relatively modest number, it is strong evidence of a gradually maturing market. More importantly, by designing their compliance programs as efficient, repeatable business processes, Best-in-Class organizations are proving themselves to be more cost-effective, more consistent and more secure, while successfully supporting greater complexity and higher scale. Compliance is the means, not the end.

"Crawl, Walk, Run" ... and what comes next? In the view of one particularly hard-driving CEO: "Run Faster."

"We now view compliance as a program, not as an event."

~ Program Manager, Fortune  
500 Software Company

## Chapter Two: Benchmarking Requirements for Success

The selection and deployment of enabling technologies, and their successful integration with existing business processes, plays a vital role in the ability to support higher scale, reduce operational costs, manage security risk, maintain consistent policies, and sustain compliance with internal policy and external regulations, standards, and best practices.

### Case Study - ARC, Arlington, Virginia

The Airlines Reporting Corporation (ARC) is an airline-owned company serving the travel industry with financial services, data products and services, ticket distribution, and settlement in the United States, Puerto Rico and the U.S. Virgin Islands. ARC provides ticket distribution, reporting, and settlement services for over 150 air and rail carriers and more than 20,000 ARC-accredited Travel Agency locations and Corporate Travel Departments. Annual processing volumes exceed \$77 billion.

Devin Bhatt, Chief Security Officer for ARC, freely shares his journey of addressing, then sustaining, compliance. "When I first brought up the topic of compliance to the line of business owners, what do you think I heard?" he recalls. "They said: You're out of your mind! We don't have time! We're trying to survive in this competitive business environment, and you want to talk about compliance? In the beginning, compliance can be viewed as a burden, one that distracts the company from its core business."

Bhatt advocates that the tone for successful compliance initiatives starts from the leaders of the business. "You really have to communicate to the management team that compliance is a business decision, not a technology decision – the impetus needs to come from the top."

While Bhatt and his team systematically identified and met the technical challenges of their compliance initiative (in this case, with the Payment Card Industry Data Security Standard), they also paid close attention to the human element of a successful program. "We made sure that every person in the company got awareness on PCI compliance issues," he explained. "What is it, why are we doing it, what is their role, what is expected."

"We also made compliance part of the bonus / incentive program ... believe me, my phone started ringing the next day with people saying 'how can I help you?' But be cautious: many people will also hate you, as you are directly affecting their pocketbook with some tasks that they may feel are not in their direct control."

Bhatt and his program at ARC also exemplify Best-in-Class performance in their attitude towards continuous improvement. While some people seem to think that if the minimum wasn't good enough, it wouldn't be the minimum, ARC has chosen to raise the bar now. "Raise the bar voluntarily," he advises. "Don't water down the objectives for your compliance programs out of fear that you won't be able to meet it and sustain it."

### Fast Facts

- √ 116% projected growth in leveraging compliance initiatives for auditing and enforcing employee behavior
- √ 97% projected growth in intent to demonstrate the impact (positive or negative) of compliance activities on the business

"In the beginning, the compliance person is often seen as coming in from the outside ... imposing more work on an already overburdened staff ... causing more problems for the IT and operations teams."

~Devin Bhatt, CSO,  
Airlines Reporting Corp.

## Competitive Assessment

The aggregated performance of all companies surveyed determined whether they ranked as Best-in-Class, Industry Average, or Laggard in the Aberdeen Maturity Class Framework. In addition to having common levels of performance, each class also shared characteristics in five key categories: **process** (the ability to detect and respond to changing conditions without placing additional burdens on the organization), **organization** (corporate focus and collaboration among stakeholders), **knowledge management** (leveraging data in context, and exposing it appropriately to key stakeholders), **technology** (the selection of appropriate tools, and intelligent deployment of those tools) and **performance management** (the ability of the organization to measure the benefits of technology deployment, and to use the results to further improve key business processes). These characteristics, as identified in Table 3, serve as a guideline for best practices and correlate directly with Best-in-Class performance across the key performance metrics.

**Table 3: Competitive Framework**

	Best-in-Class	Average	Laggards
<b>Process</b>	Consistent security and compliance policies		
	85%	71%	48%
	Formal risk assessments		
	63%	54%	45%
	Standardized audit, analysis, and reporting		
	62%	48%	38%
	Standardized response for exceptions, security events, or incidents of non-compliance		
<b>Organization</b>	54%	45%	38%
	Systematic elimination of root causes for exceptions, security events, or incidents of non-compliance		
	51%	37%	33%
<b>Organization</b>	Responsible executive or team with primary ownership for security-related compliance initiatives		
	83%	63%	49%
	Formal documentation, awareness and end-user training programs around compliance		
<b>Knowledge</b>	60%	41%	36%
	Identification of all information required for auditing and reporting		
	54%	38%	36%
	Identification of required frequency of auditing and reporting		
	58%	45%	44%
	Regular review and analysis of data from compliance management, auditing and reporting solutions:		
61%	43%	40%	
<b>Knowledge</b>	Repeatable process for determining the organization's security posture (e.g., self-assessment and measurement of IT controls)		
	61%	37%	31%

	Best-in-Class	Average	Laggards	
<b>Technology</b>	Update / patch facilities are enabled on all appropriate devices throughout the organization			
	83%	66%	61%	
	Logging is enabled on all appropriate sources throughout the organization			
	67%	55%	49%	
	Data captured includes all of the key event and activity logs required by policies and standards			
	58%	46%	36%	
	Enabling technologies / solutions currently in use			
	<ul style="list-style-type: none"> <li>▪ Vulnerability management 63%</li> <li>▪ Configuration and change management 64%</li> <li>▪ Patch management 80%</li> <li>▪ Unified threat management 35%</li> <li>▪ Database monitoring and auditing 69%</li> <li>▪ Log management 56%</li> <li>▪ Security information management 39%</li> <li>▪ Security event management 47%</li> <li>▪ Network access control 67%</li> <li>▪ Network behavior analysis 47%</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vulnerability management 55%</li> <li>▪ Configuration and change management 56%</li> <li>▪ Patch management 74%</li> <li>▪ Unified threat management 23%</li> <li>▪ Database monitoring and auditing 44%</li> <li>▪ Log management 45%</li> <li>▪ Security information management 32%</li> <li>▪ Security event management 33%</li> <li>▪ Network access control 45%</li> <li>▪ Network behavior analysis 28%</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vulnerability management 53%</li> <li>▪ Configuration and change management 50%</li> <li>▪ Patch management 67%</li> <li>▪ Unified threat management 16%</li> <li>▪ Database monitoring and auditing 40%</li> <li>▪ Log management 38%</li> <li>▪ Security information management 31%</li> <li>▪ Security event management 32%</li> <li>▪ Network access control 38%</li> <li>▪ Network behavior analysis 24%</li> </ul>	
	<b>Performance</b>	Controls to monitor and verify that requirements of internal policies and external regulations are being satisfied		
		58%	44%	44%
Monitoring / verification of end-user behavior conducted in accordance with established policies				
43%		40%	31%	
Compared to one year ago				
<ul style="list-style-type: none"> <li>▪ 26% decreased the cost of addressing security-related incidents</li> <li>▪ 18% decreased the cost of addressing non-compliance incidents</li> <li>▪ 14% decreased time spent on management, auditing, and reporting on a reactive, "as-needed" basis</li> </ul>		<ul style="list-style-type: none"> <li>▪ 2% decreased the cost of addressing security-related incidents</li> <li>▪ 3% decreased the cost of addressing non-compliance incidents</li> <li>▪ 5% decreased time spent on management, auditing, and reporting on a reactive, "as-needed" basis</li> </ul>	<ul style="list-style-type: none"> <li>▪ 0% decreased the cost of addressing security-related incidents</li> <li>▪ 0% decreased the cost of addressing non-compliance incidents</li> <li>▪ 3% decreased time spent on management, auditing, and reporting on a reactive, "as-needed" basis</li> </ul>	

Source: Aberdeen Group, September 2007

## Capabilities and Enablers

---

Based on the comparisons of the Competitive Framework and interviews with select end-user organizations, analysis of the Best-in-Class highlights the discipline with which they have developed their security and compliance infrastructure and automated their management, auditing, and reporting processes.

### Process

Consistent security and compliance policies are necessary, but not sufficient. In addition to establishing what ought to be done, Best-in-Class companies have established what to do when an incident occurs and are also more likely to find and eliminate root causes to prevent incidents from occurring in the future.

### Organization

Clear ownership and accountability for security and compliance initiatives (“one throat to choke”) is a well-known success factor, so it comes as no surprise that 83% of Best-in-Class organizations report this capability. What is surprising, however, is that so few (60%) of even the Best-in-Class companies provide formal documentation, awareness, and end-user training programs around compliance. Given the significant investments organizations make in technical solutions to address security and compliance, it also makes sense for them to invest commensurately in educating their people.

“A security or compliance awareness program may be the best ROI there is. If everybody doesn’t know what to do, nobody is going to do it.”

~Senior VP, Top 10 US Bank

### Knowledge Management

Best-in-Class organizations identify what information they need for auditing and reporting, and how frequently they need it ... and most importantly, they actually review and analyze it on a regular basis.

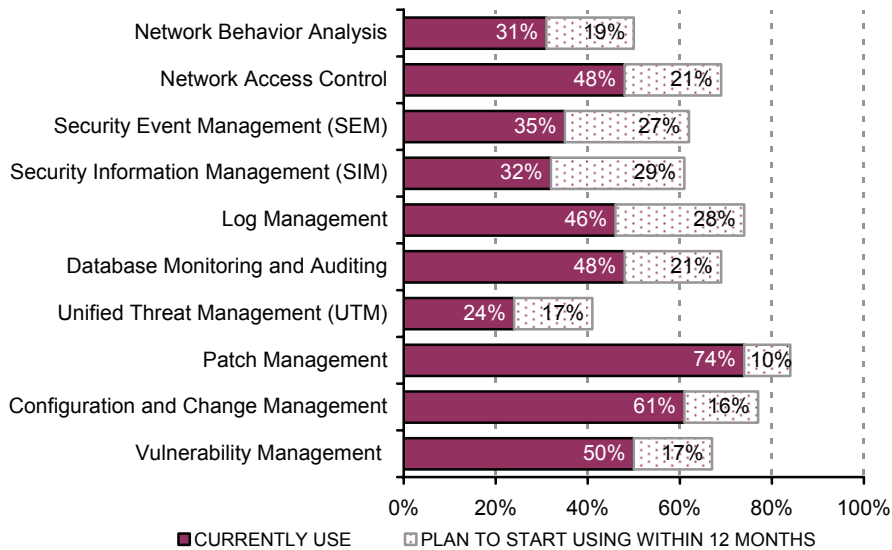
### Technology

While Best-in-Class organizations deploy enabling technologies to a slightly higher degree than either the Industry Average or Laggards, the most meaningful difference is that they make more complete use of them. Update and patch facilities are more likely to be enabled on all devices, logging is more likely to be enabled on all devices, and captured data is more likely to include all of the information and events required by policies and standards.

### Performance Management

“Trust, but verify.” Best-in-Class organizations are more likely to implement controls to monitor and verify that the requirements of their internal policies and external regulations are being satisfied. They are only slightly more likely than the Industry Average to monitor and verify that end-user behavior is in accordance with established policies (although this is actually in alignment with the relatively low rates of end-user awareness and training noted earlier).

**Figure 4: Selected Enabling Technologies Deployed in Support of Security and Compliance Initiatives**



Source: Aberdeen Group, September 2007

### Aberdeen Insights - Technology

Companies surveyed have deployed a diverse suite of technologies in support of their security and compliance initiatives, as shown in Figure 4. Across nearly 200 respondents, data was collected on 59 specific vendors / solutions, representing over 800 current deployments. The next year will bring continued growth in deployments in support of compliance – the survey data identified nearly 200 solutions planned for deployment in the next 12 months, and another 400 solutions currently under evaluation.

Solutions for patch management (74% of all respondents), configuration and change management (64%), and vulnerability management (50%) are currently the most widely used. Projected incremental growth in these areas is therefore relatively lower on a percentage basis, although in absolute terms deployments planned over the next 12 months remain strong. Look for future Aberdeen Research Briefs to examine current users of these solutions in comparison to the Best-in-Class.

Another interesting grouping of solutions includes log management (currently deployed at 54% of all respondents), security information management (32%), and security event management (35%). The highest year-over-year growth in deployments indicated by the survey data is in this category of solutions, in both absolute and relative terms. Future Aberdeen Research Briefs will also examine current users of this category of solutions in comparison to the Best-in-Class.

*continued*

### Aberdeen Insights - Technology

Other solution categories of note include unified threat management (24% current use, 71% projected year-over-year growth), network access control (48% current use, 44% projected year-over-year growth), and identity and access management (37% current use, 68% projected year-over-year growth). Aberdeen's near-term security research agenda includes Research Benchmarks focused specifically on each of these areas.

In general, the diversity of solutions competing for mindshare in addressing security and compliance initiatives is a breeding ground for unnecessary confusion in the market, as vendors (and many analysts) invent new categories in an effort to differentiate themselves. Vendors and solution providers who sharpen their messaging and support end-user organizations across all stages of their "crawl, walk, run" journey to compliance stand to gain the most share during the high growth indicated over the next 12 months.

In addition, the preponderance of tactical, project-oriented point solutions often has the effect of end-user organizations acting as their own systems integrators – or absorbing the operational inefficiencies of managing a hodge-podge of discrete systems. Forward-looking vendors and solution providers are building out a “platform” or “ecosystem” approach, starting with a consistent architecture to facilitate integration and interoperability for collection, archival, correlation, analysis, monitoring, auditing and reporting on security- and compliance-related data. This vision is consistent with the Best-in-Class view of compliance as a strategic, sustainable program.

## Chapter Three: Required Actions

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

### Laggard Steps to Success

---

- Commit to compliance - the journey starts with a strategic commitment to achieve initial compliance, with a long-term goal to develop a repeatable, sustainable business process. The majority of Laggard organizations indicated that compliance is currently not a top priority.
- Assign ownership - less than half of Laggard organizations had identified an executive or team with primary ownership for security-related initiatives. This is a critical success factor for any meaningful initiative.
- Establish a baseline - only 36% of Laggards had identified all of the information required for auditing and reporting. Likewise, only 36% are currently capturing data that includes all of the key events and activities required by policies and standards. Regular and repeatable evaluation of systems on the network to a baseline policy is the foundation for consistent, “continuous” compliance.

### Industry Average Steps to Success

---

- Take steps to standardization - the majority of Industry Average organizations had deployed point solutions and were managing and reporting on an as-needed basis. Transforming compliance from a never-ending series of projects to a sustainable business process involves standardizing on audit, analysis, and reporting; standardizing on responses for exceptions, security events, and incidents of non-compliance; and systematically finding and eliminating root causes.
- Educate - only 41% of the Industry Average are currently providing formal documentation, awareness, and end-user training programs around compliance. “If everybody doesn't know what to do, nobody is going to do it.”
- Turn it on - only two-thirds of Industry Average organizations had enabled update / patch facilities throughout the organization, and only 55% had enabled logging on all appropriate sources. Better to use it than lose it.

### Best-in-Class Steps to Success

---

- Raise the bar - as shown in Table 3, Best-in-Class organizations still have significant opportunities to standardize with regard to audit,

#### Fast Facts

- √ 88% projected growth in use of compliance initiatives to support incident investigation and forensics
- √ 69% projected growth in use of compliance initiatives to support real-time threat detection and mitigation

“We learned that identifying which logs to collect and turning on auditing before full-scale implementation allowed us to ease the reporting process and to get the most value out of our compliance and security information management initiative.”

~Data Security Analyst,  
Leading Supermarket Chain

analysis, and reporting; on responses for exceptions, security events, and incidents of non-compliance; and on systematically finding and eliminating root causes.

- **Educate** - 60% of the Best-in-Class are currently providing formal documentation, awareness, and end-user training programs around compliance. People who understand clearly what must be done, why it must be done, and what role they have in doing it will make a much larger contribution to a successful compliance initiative.
- **Leverage** - Best-in-Class companies can take advantage of repeatable business processes to add value to other activities, such as investigation and forensics of security and compliance incidents, detection and mitigation of threats in real-time, and demonstrating the impact of compliance on the bottom line of business.

“Raise the bar voluntarily. Don’t water down the objectives for your compliance programs out of fear that you won’t be able to meet it and sustain it.”

~Devin Bhatt, CSO,  
Airlines Reporting Corporation

### Aberdeen Insights - Summary

Companies of all sizes and from virtually all industries are beset with pressures to demonstrate compliance with government regulations, industry regulations, industry standards and best practices, and with their own internal policies. At the same time, network and security infrastructures have introduced more diversity, more complexity, and higher scale.

Addressing and sustaining compliance in this environment calls for a committed program, not a one-time event. Although tactical deployment of point solutions for addressing compliance on an as-needed basis is currently the most prevalent approach, Best-in-Class organizations have begun to view compliance as a strategic, sustainable program – which in addition to helping them to achieve and maintain compliance requirements, also helps them to lower operational costs, support higher scale, reduce security risk, and maintain consistent security policies. By virtue of their active management of compliance as a strategic business process, Best-in-Class organizations have not only decreased the number of non-compliance incidents, the number of security-related incidents, and the number of false positives, but also the time required to complete a compliance-related audit.

Leading vendors and solutions providers are beginning to look beyond the point product mentality, to extend their solutions as part of a higher-level “platform” or ecosystem that will contribute to operational and management efficiencies, better security, and continuous compliance.

Leaders in Best-in-Class organizations position compliance as a journey, not a destination. Going forward, the activities supported by Best-in-Class security and compliance initiatives will expand from investigation, forensics, detection, and prevention to include proactive tasks such as capacity planning to maximize performance and uptime, support and validation for customer SLAs, and improvements in internal communications between the network, security, and operations teams. Like all journeys, sustaining compliance begins with a single step – in this case, a strategic commitment to management, auditing, and reporting as part of an integrated security and compliance strategy.



## Appendix A: Research Methodology

In September 2007, Aberdeen examined the range of approaches currently being taken to address security and compliance requirements. The experiences and intentions of more than 190 organizations from a diverse set of enterprises are represented in this study.

Aberdeen supplemented this online survey effort with telephone and in-person interviews with select survey respondents, gathering additional information on their compliance strategies, experiences, and results.

Responding organizations had the following demographics:

- *Job title / Function:* The research sample included respondents with the following job titles: C-level (21%); VP (5%); director (12%); manager (25%); staff / consultant (29%); and other (8%). The largest segment by functional responsibility was IT, representing 65% of the sample.
- *Industry:* The research sample included respondents from a wide variety of industries. The largest individual segments were financial services (11%), telecom (11%), high-tech (22%), and government / aerospace / defense (13%).
- *Geography:* The majority of respondents (61%) were from North America. Remaining respondents were from Europe (27%) and the Asia-Pacific region (12%).
- *Company size:* Twenty-four percent (24%) of respondents were from large enterprises (annual revenues above US \$1 billion); 40% were from mid-size enterprises (annual revenues between \$50 million and \$1 billion); and 36% were from businesses with annual revenues of \$50 million or less.

Solution providers recognized as sponsors of this report were solicited after the fact and had no substantive influence on the direction of the Sustaining Compliance benchmark report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

### Study Focus

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

- √ The degree to which organizations view compliance not as an event, but as a strategic, sustainable program
- √ The activities currently being supported by compliance initiatives, and functions deriving the highest value from compliance initiatives
- √ The degree to which investments are being driven by compliance with government regulations, industry regulations, industry standards and best practices, and internal policies
- √ The amount of time and resources spent in management, auditing and reporting to address security and compliance requirements

The study aimed to identify emerging best practices for management, auditing and reporting for security-related compliance, and to provide a framework by which readers can assess their own capabilities in these areas.

**Table 4: 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, September 2007

**Table 5: 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 (top 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 (middle 50%)</b> — Practices that represent the average or norm, and result in average industry performance.</p> <p><b>Laggards (bottom 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, September 2007

**Table 6: Relationship Between PACE and Competitive Framework**

PACE and the Competitive Framework – How They Interact
<p>Aberdeen research indicates that companies that identify the most impactful 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, September 2007

## Appendix B: Related Aberdeen Research

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

- *[Encryption & Key Management; August 2007](#)*
- *[The Ins and Outs of Email Vulnerabilities; July 2007](#)*
- *[Protecting Cardholder Data: Best-in-Class Performance at Addressing the PCI Data Security Standard; June 2007](#)*
- *[Thwarting Data Loss; May 2007](#)*

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

Author: Derek E. Brink, Vice President & Research Director, IT Security,  
[Derek.Brink@aberdeen.com](mailto:Derek.Brink@aberdeen.com)

Founded in 1988, Aberdeen Group is the technology- driven research destination of choice for the global business executive. Aberdeen Group has 400,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services. This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provides 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.

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>