



Aberdeen *Group*

[Send to a Friend](#) 

## Identity and Access Management Critical to Operations and Security

*Users Find ROI, Increased User Productivity, Tighter Security*

March 2007

— Underwritten, in Part, by —

 **beta**systems

 **imanami**

 **imprivata**<sup>®</sup>

 **QUEST  
SOFTWARE**<sup>®</sup>

## Executive Summary

The point of identity and access management (IAM) solutions is to limit access to an organization's resources to those with legitimate access. Without it, organizations are at risk. The larger the organization, the more resources in need of protection, the greater the stakes. The more users, the more discrete resources to access, the greater the complexity. Unless mitigated by automation, the greater the complexity, the longer it takes to grant access and to deny access. Decreasing time to granting legitimate access translates to a gain in productivity. Decreasing time to revoking access translates to narrowing a window of vulnerability. Aberdeen research has determined that the two leading drivers for the adoption of IAM identity management and access solutions are **increased productivity** and **compliance with security policies**.

In researching the use of IAM solutions, Aberdeen found that Best in Class companies:

- Have lowered administrative costs and
- Are significantly better at measuring policy compliance.

Comparing Best in Class users with Laggards in our study:

CHARACTERISTIC	LAGGARDS	BEST IN CLASS
Time to de-provision account access	Some take more than 30 days	Averages less than 4 hours
% having consolidated identity directories to one	0%	19%
% of orphaned accounts between 250 and 500	25%	4%

At least 83% of all organizations surveyed say compliance with policies and regulations is important, and some estimate the magnitude of the risk for failing to comply at more than \$5 million. "As an organization, we are bound by secrecy and privacy legislation that dictates that we must ensure that we do not disclose information to unauthorized third parties," an information technology consultant to a government agency says.

Yet, despite strong pressure to adopt identity and management solutions, 48% of survey respondents said their companies are still evaluating solutions or plan to deploy them within the next 12 months.

In gathering best practices from our research, Aberdeen recommends the following actions:

- Select solutions with automated, role-based account provisioning/de-provisioning and policy enforcement;
- Use strong authentication to establish trusted user identities; and
- Establish compliance, risk management, and privacy advocates to ensure quality.

[Send to a Friend](#) 



## Table of Contents

Executive Summary .....	i
<i>Chapter One: Issue at Hand</i> .....	1
Complex Systems Are Potentially More Vulnerable .....	2
Features in Demand .....	3
<i>Chapter Two: Competitive Maturity Assessment</i> .....	5
Process, Organization, and Knowledge .....	6
<i>Chapter Three: Recommendations for Action</i> .....	8
Laggard Steps to Success .....	9
Industry Average Steps to Success .....	9
Best in Class Next Steps .....	9
Featured Underwriters .....	10
<i>Appendix A: Research Methodology</i> .....	12

## Figures

Figure 1: The Number of Separate Identity Directories .....	3
Figure 2: Best in Class Have Fewer Identity Stores .....	4

## Tables

Table 1: Companies with Top Performance Scores Earn Best-in-Class Status ....	1
Table 2: Use of Centralized Identity Management/Provisioning .....	2
Table 3: Identity and Access Management Competitive Framework .....	5

## Chapter One: Issue at Hand

### Key Takeaways

- To meet regulatory mandates to limit and verify access, organizations say identity and access management is critical. They augment identity management with strong authentication to ensure users who ultimately gain access are who they say they are.
- Complex, distributed organizations are especially vulnerable without robust identity and access management.
- Organizations are choosing solutions that favor automation and integration, and prioritize role-based access control, centralized management, and ease of integration with existing infrastructure as selection criteria.

Identity and access management play a critical role in any corporate security effort. From identity creation to access termination, identity and access management systems bring together people, processes and technologies, enabling organizations to manage the lifecycles of the identities of both internal and external users. Every organization must have a reliable way to identify computer users and an efficient way to regulate what applications, data, and other computing resources each user can access. Increasingly, organizations are turning to role-based administration to expedite the provisioning of legitimate access to corporate resources. Where terminating access is critical, that is, *when denial of access to users whose access must be terminated is deemed vital to security*, automated de-provisioning is key.

Strategies to maximize the value of identity and access management solutions are only as good as the results they deliver. Aberdeen used four key performance criteria to distinguish Best in Class companies from Industry Average and Laggard organizations. These key performance indicators (KPIs) represent *process measures*, represented by account provisioning/de-provisioning time, and *quality measures*, represented by the ability to measure compliance of processes with policy, level of synchronization between directories, and average amount of orphaned accounts discovered during audits (Table 1).

**Table 1: Companies with Top Performance Scores Earn Best-in-Class Status**

Definition of Maturity Class	Mean Class Performance
<b>Best in Class:</b> Top 20% of aggregate performance scorers	<ul style="list-style-type: none"> <li>• Account provisioning/de-provisioning in <b>less than 4 hours</b></li> <li>• <b>29%</b> report excellent compliance of processes to policy</li> <li>• <b>22%</b> report complete synchronization between directories</li> <li>• <b>33%</b> report no orphaned accounts</li> </ul>
<b>Industry Average:</b> Middle 50% of aggregate performance scorers	<ul style="list-style-type: none"> <li>• Account provisioning/de-provisioning in <b>3 days or less</b></li> <li>• <b>9%</b> report excellent compliance of processes to policy</li> <li>• <b>11%</b> report complete synchronization between directories</li> <li>• <b>17%</b> report no orphaned accounts</li> </ul>
<b>Laggard:</b> Bottom 30% of aggregate performance scorers	<ul style="list-style-type: none"> <li>• Account provisioning/de-provisioning in <b>4 days or more</b></li> <li>• No reports of excellent compliance of processes to policy</li> <li>• <b>8%</b> report complete synchronization between directories</li> <li>• <b>13%</b> report no orphaned accounts</li> </ul>

Source: Aberdeen Group, March 2007



Companies that use centralized identity and access management solutions are demonstrating superior process and quality performance. **Best in Class organizations are nearly four times more likely to use a centralized identity management/provisioning solution than Laggard organizations** (Table 2).

**Table 2: Use of Centralized Identity Management/Provisioning**

Current or Future Adoption Plans	% Selected BIC	% Selected Laggard
Currently in use	35%	9%
Planned in next 12 months	30%	55%
Currently assessing	5%	18%
No, due to budget	20%	9%
No, not applicable	10%	0%

Source: Aberdeen Group, March 2007

In addition, Best in Class organizations are seeing reduced account provisioning/de-provisioning times, better compliance of identity processes to policy, and they are less likely to find orphaned user accounts during identity system audits.

Laggard organizations appear to be aware of the issue at hand, and are almost twice as likely to be currently assessing or planning to deploy centralized identity management/provisioning in the next 12 months.

### Complex Systems Are Potentially More Vulnerable

Managing identity and access across multiple independent identity structures is an administrative challenge and a potential source of serious vulnerability. Preventing inappropriate access on many fronts is no trivial problem. De-provisioning access to people who once had legitimate access is time-sensitive; the longer unwelcome users have access, the more damage they can potentially inflict.

“We were trying to create an integrated sign-on capability as part of an effort to repatriate and repurpose/redevelop a large number of quite small applications developed within the health program/business areas,” said a technology architect for a large health-care services provider. “Each application had its own (or lacked an) authorization scheme and IAM provided a way to create a common authorization, authentication, and sign-on security policy.”

---

“Each application had its own (or lacked an) authorization scheme and IAM provided a way to create a common authorization, authentication, and sign-on security policy.”

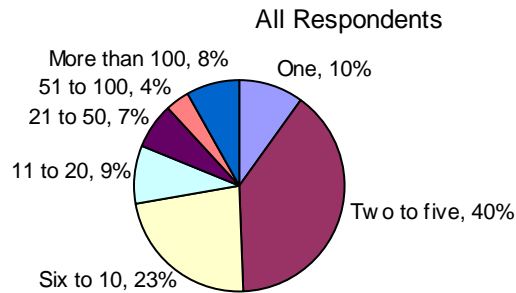
~ Technology architect,  
large health care services provider

---

Aberdeen research found organizations with hundreds of **orphaned accounts**; that is, accounts with access that should have been revoked. Some organizations take more than 30 days to decommission accounts and others have no defined process to discover if orphaned accounts even exist.

A key to reducing complexity is reducing the number of independent identity stores. Respondents to the survey on which this report is based varied widely, with 10% having a single identity directory and 8% having more than 100 (Figure 1).

**Figure 1: The Number of Separate Identity Directories**



Source: Aberdeen Group, March 2007

## Features in Demand

Despite widespread recognition of the need for identity and access management, some 48% of organizations we surveyed are still in the assessment or planning stage with IAM solutions. Survey respondents stated that their top two criteria in selecting identity management were:

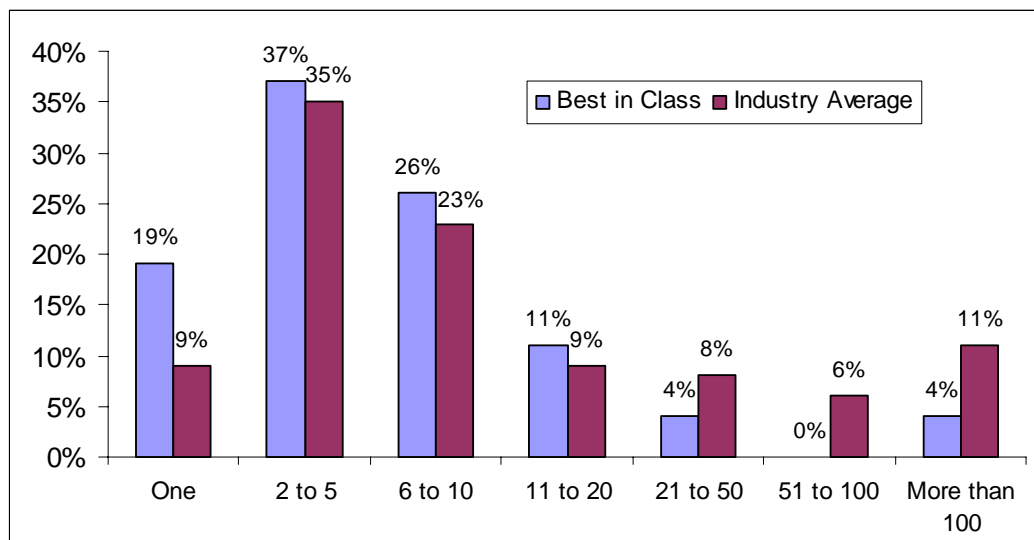
1. **Support for role-based user administration** (56%) and
2. **Centralized management** (52%).

Role-based administration capabilities allows companies to provision access to resources based on an employee’s role (or roles), thereby reducing the administrative overhead of a case-by-case provisioning effort and accelerating user productivity. For example, all support personnel are provisioned with e-mail, word-processing and spreadsheet software when they are identified by the role of “support personnel.” “Procurement personnel” are provisioned in the same way as “support personnel,” but also given access to the procurement system. New employees gain access to the resources they need based on the roles associated with their unique user identities. In addition, roles help enforce the clear separation of duties necessary to ensure the integrity of auditing required by regulations.

**Centralized management** allows organizations to manage multiple directories from a unified management console and addresses the integration of identity information across systems and applications. With 90% of the organizations we surveyed are currently managing multiple directories, centralized management is key. When identity information in one system changes, corporate policies ensure that all systems update the appropriate user information and access rights in real time, closing a window of vulnerability and providing 24/7 visibility into who is accessing company information. Figure 2 compares the number of identity stores in Best in Class companies to the number found in the Industry Average.



**Figure 2: Best in Class Have Fewer Identity Stores**



Source: Aberdeen Group, March 2007

Also important to buyers of identity management solutions are **ease of integration with current infrastructure** (39%), as well as **high availability** and **dedicated audit/compliance functions** (each at 28%).

If identity and access management systems are susceptible to outages, provisioning or de-provisioning requests are delayed, reducing productivity and opening windows of vulnerability. End users are looking for high availability for systems that span various systems and applications.

Organizations are purchasing identity and access management solutions to address compliance with such legislation as Sarbanes-Oxley, Basel II, the EU Data Protection Directive, and the Health Insurance Portability and Accountability Act (HIPAA). With movement toward mandated disclosure, there is mounting pressure for verifiable compliance, and these buyers often look for specific audit and compliance capabilities.

## Chapter Two: Competitive Maturity Assessment

**Key Takeaways**

- Best in Class firms are 20% more likely to reduce staffing levels through implementation of an identity and access management solution.
- The Best in Class are four times more likely to report customer confidence as a reason why they conduct audits of their identity management systems.
- Best in Class firms are twice as likely to report satisfaction with the implementation time of solutions.

Aberdeen’s survey respondents fell into one of three categories – Laggard, Industry Average, and Best in Class — based on their characteristics in four key categories: (1) **process** (responsiveness to organizational needs, such as account provisioning and de-provisioning); (2) **organization** (level of coherence in the organization as indicated by synchronization of identity directories and scope of authentication solutions); (3) **knowledge** (visibility into policy compliance); and (4) **technology** (scope of automation).

In each category, survey results show that organizations exhibiting Best in Class identity and access management usage characteristics also enjoy Best in Class security compliance.

**Table 3: Identity and Access Management Competitive Framework**

	Laggards	Industry Average	Best in Class
<b>Process</b>	Provisioning time: <b>4 days or longer</b> De-provisioning time <b>4 days, with 15% exceeding 30 days</b> Audits result in highest number of orphaned accounts.	Average provisioning time: <b>1 to 3 days.</b> Average de-provisioning time: <b>1 to 7 days.</b> Audits result in minimal number of orphaned accounts.	Provisioning and de-provisioning times: <b>less than 4 hours</b> Average de-provisioning time: <b>less than 4 hours</b> Audits result in lowest number of orphaned accounts.
<b>Organization</b>	<b>8%</b> report complete directory synchronization. <b>All report using multiple directories.</b>	<b>11%</b> report complete directory synchronization. <b>Approximately 90% use multiple directories.</b>	<b>22%</b> report complete directory synchronization. <b>Only 81% use multiple directories.</b> BIC companies are successfully combining identity directories



	Laggards	Industry Average	Best in Class
<b>Knowledge</b>	No reports of excellent ability to measure compliance of identity management processes to policy. Only 8% consider IT administration costs a top driver.	9% report excellent ability to measure compliance of identity management processes to policy. 33% consider IT administration costs a top driver.	29% report excellent ability to measure compliance of identity management processes to policy 44% consider IT administration costs a top driver.
<b>Technology</b>	Dedicating the most amount of staff toward managing identities and directories.	Dedicating average amount of staff toward managing identities and directories.	Dedicating the least amount of staff toward managing identities and directories.

Source: AberdeenGroup, March 2007

### Process, Organization, and Knowledge

Best in Class firms consider identity and access management solutions part of a multi-layer approach toward increased security and auditable compliance. Twenty-nine percent of these companies are already using some sort of biometrics, smartcards, or token authentication, and another 43% are planning or considering their use. These technologies help ensure that those gaining access in the first place really are who they claim to be. Once they've been granted access, their identity within the scope of systems under identity management is assured.

Implementing identity and access management has allowed Best in Class companies to realize the highest level of complete synchronization of their corporate identity directories. Wherever there are directories that are not synchronized, vulnerability exists. Until the identity and access information is up-to-date on all systems, users who should be denied access may continue to gain access and exploit system resources. Synchronizing directories and reducing the actual number of separate identity directories reduces or eliminates the lag time needed to disseminate the denial of access.

Best in Class firms report **an increased capability to measure process to policy compliance, lowest number of orphaned accounts, and fewest staff needed to maintain the solution.** They are four times more likely than the Industry Average to report customer confidence as a reason they conduct audits of their identity management systems. The Best in Class report the highest usage of end-user self-service password reset solutions, and, as a result, claim the shortest turnover time for a password reset request.

Companies contending with regulatory compliance are frequently faced with establishing authorization criteria for all applications that access sensitive information. They must restrict access and be able to prove compliance to policies. For organizations facing these

---

"We will have ROI. Tangible in operational savings (streamlining user access/authorization, provisioning/de-provisioning, flowing from the central IDMS, reduced management cost, increased user productivity) and intangible through improved ability to both comply and demonstrate compliance ..."

- Information security coordinator,  
defense Industry

---



challenges, identity and access management becomes a pivotal part of their strategy. “IAM provides a way to create a common authorization, authentication and sign-on security policy,” according to a technology architect in the health services industry. “Many of the applications were in use by the broader health sector, and having a common security mechanism became an imperative.” Because of HIPAA’s requirement to protect patient privacy, tight control over access to sensitive information is paramount in the health care industry.



## Chapter Three: Recommendations for Action

### Key Takeaways

- Identify roles and align specific access with specific roles.
- Select solutions that provide automated role-based account provisioning and de-provisioning, as well as automated policy enforcement.
- Develop a tiered approach to access and identity that ensures strong authentication as well as identity management.
- Select solutions that integrate well with existing systems

Ultimately, organizations need identity and access management to ensure that access to systems and resources is limited to legitimate users. To secure an organization from insider and outsider threats, and to establish compliance with policies and regulations, organizations need to architect access to resources (systems, processes, and data) to align legitimate access with specific roles. No one should be granted carte blanche access and mechanisms must be established to ensure audit capabilities cannot be compromised by anyone in a position to abuse access to log files and data.

But beyond security and compliance imperatives, identity and access management are crucial to user productivity and thus to an organization's overall efficiency.

Organizations that have yet to begin their identity and access management initiatives should assess their vulnerabilities from the perspective of what damage someone with unauthorized access could do. Likewise, they should pay attention to delays in productivity and gather the data they need to gain support for identity and access management strategies. Solutions that provide self-service password reset and enterprise single sign-on can help reduce help desk costs.

Beyond the automated provisioning and de-provisioning of user accounts, organizations should look at the following:

- Role-based user administration;
- Centralized management of all corporate directories;
- Integration with current infrastructure; and
- Dedicated compliance reporting.

Companies should evaluate their processes and work to establish the following:

- Systems that provide automated policy enforcement and support advanced features such as single sign-on, self-service, two-factor authentication, and biometrics;
- Training on identity and account management policies and procedures as part of new employee training or as an ongoing training program; and
- Procedures that generate the information needed for management reports that support implementing or improving identity and access management solutions.



Whether a company is trying to move its organization from “Laggard” to “Industry Average,” or from “Industry Average” to “Best in Class,” the following actions can help improve performance:

### Laggard Steps to Success

1. *Take action to reduce the number of separate identity directories and synchronized separate directories.*
2. *Define user roles and the legitimate access associated with each role.*
3. *Use technology to automate provisioning and de-provisioning of user accounts and reduce the time required for each task.*
4. *Create processes to identify and eliminate orphaned accounts.*
5. *Document lack of productivity and windows of vulnerability to garner support for identity and access management solutions.*

### Industry Average Steps to Success

1. *Continue to reduce the number of separate identity directories and synchronized separate directories.*
2. *Refine user roles.*
3. *Ensure stronger identity management by leveraging additional authentication technologies.*

### Best in Class Next Steps

1. *Further refine user roles.*
2. *Establish checks and balances tied to user identities to ensure audit data cannot be compromised.*
3. *Integrate identity and access management, policy management, and auditing capabilities to establish efficient, flexible, accountable systems.*

Organizations should consider identity and access management solutions as a cornerstone of their security and operational strategies. As organizations move toward more flexible systems, enabled by business process management and service oriented architectures, the need for tight controls over identity increases. Without tight control over user identity and access, organizations leave themselves vulnerable to exploits from both within and outside.

Depending on an organization’s size and complexity, determining an identity and access management strategy and selecting and deploying identity and access management can represent a large investment in time and money. Yet, verifiable security and business flexibility (the ability for an organization to change its own processes) depend on an organization’s control over its users’ access. One respondent from a globally distributed company with significant outsourcing requiring different kinds of needs said, “Without identity management we would not be able to run the company.”

[Send to a Friend](#) 



## Featured Underwriters

---

This research report was made possible, in part, with the financial support of our underwriters. These individuals and organizations share Aberdeen's vision of bringing fact based research to corporations worldwide at little or no cost. Underwriters have no editorial or research rights and the facts and analysis of this report remain an exclusive production and product of Aberdeen Group.

**betasystems** Beta Systems provides high-quality software products and services for secure and efficient processing of large quantities of data, with 1,300 customers and over 3,000 running installations at major businesses in Europe and North America. Beta Systems' market leading SAM Identity Management Product Suite considerably drives down the **cost of user management and access rights administration**, and enhances **end user productivity**. It enforces corporate security policies in IT systems and is a key solution for **regulatory compliance**. The SAM Suite includes the most comprehensive set of role-based user provisioning functions, and components for identity audit, password management, enterprise single sign-on and directory synchronization.

**For more information on Beta Systems, contact:**

Beta Systems of North America  
2201 Cooperative Way, 3rd Floor; Herndon, VA 20171  
1-703-889-1240; fax: 1-703-889-1241  
<http://www.betasystems.com>  
[idm@betasystems.com](mailto:idm@betasystems.com)

**imanami** Imanami delivers fast-ROI point solutions for Identity & Group Management. Our solutions allow an organization to automate Distribution Lists and Security Groups with accurate data, ensuring that individuals have access to the correct information as soon as they need it. A Microsoft Gold Certified Partner, Imanami is a leader in providing software solutions that significantly reduce costs and increase productivity and security for organizations around the world. Take control of your Distribution Lists and Security Groups.

**For more information on Imanami Corp., contact:**

Imanami Corporation  
5099 Preston Avenue; Livermore, CA 94551  
1-925-371-3000  
<http://www.imanami.com>  
[Edward.killeen@imanami.com](mailto:Edward.killeen@imanami.com)



Imprivata helps companies solve the complex problems of user network authentication and application access management, resulting in strengthened corporate security, lower help desk support costs, and ability to help demonstrate regulatory compliance. Imprivata® OneSign™ is an award-winning appliance-based solution for easily securing user access to networks and applications, helping organizations of all sizes to:

- Increase security by replacing Windows and remote access passwords with a range of strong authentication options;
- Quickly and effectively solve password management and user application access issues;
- Enhance enterprise security by converging identities from both the network and building access systems.

Imprivata makes authentication and access management easy, smart, and affordable through innovative technology that improves security and compliance, without sacrificing convenience.

**For more information on Imprivata, Inc., contact:**

Imprivata, Inc.  
10 Maguire Road; Lexington, MA 02421-3120  
1-781-674-2700  
<http://www.imprivata.com>  
[leonardi@imprivata.com](mailto:leonardi@imprivata.com)



Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructures. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 50,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows Management solutions simplify, automate and secure Active Directory, Exchange, and Windows, as well as integrate Unix, Linux, and Java into the managed environment. Quest Software can be found in offices around the globe and at [www.quest.com](http://www.quest.com).

**For more information on Quest Software, contact:**

Quest Software  
5 Polaris Way; Aliso Viejo, CA 92656  
1-800-306-9329  
<http://www.quest.com>  
[sales@quest.com](mailto:sales@quest.com)



## Appendix A: Research Methodology

---

In January 2007, Aberdeen Group examined the identity and access management procedures, experiences, and intentions of more than 120 enterprises in aerospace and defense (A&D), automotive, high-tech, industrial products, and other industries to determine the state of adoption of identity and access management solutions as well as user experiences from more mature identity and access management deployments.

The study aimed to identify emerging best practices for identity and access management and provide a framework by which readers could assess their own identity and access management capabilities.

Responding enterprises included the following:

- **Job title/function:** The research sample included respondents with the following job titles: C-level (CEO, COO, president, CIO) (21%); management (vice president, director, manager) (45%), and staff and consultants (27%).
- **Industry:** The research sample included respondents from the high tech/software industry (36%), telecommunications equipment and services (26%), finance, banking and accounting (18%), computer equipment manufacturers (15%), and aerospace and defense manufacturers 9%. Other sectors responding included the public sector, transportation and logistics, insurance and real estate, medical equipment, and retail and distribution.
- **Geography:** 42% of all study respondents were from North America, 31% from Europe, the Middle East and Africa (EMEA), 25% from Asia-Pacific and 2% from Latin America and the Caribbean.
- **Company size:** About 37% of respondents were from large enterprises (annual revenues above US\$1 billion); 26% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 37% of respondents were from small businesses (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 this benchmark report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

## *Appendix B:* **Related Aberdeen Research & Tools**

---

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

- [\*Automated Security Configuration Management\*](#); January 2007
- [\*2006 Messaging Security Benchmark Report\*](#); September 2006
- [\*The Value of User Provisioning for SOX Compliance\*](#); February 2005

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

---

*Aberdeen Group, Inc.  
260 Franklin Street  
Boston, Massachusetts  
02110-3112  
USA*

*Telephone: 617 723 7890  
Fax: 617 723 7897  
[www.aberdeen.com](http://www.aberdeen.com)*

*© 2007Aberdeen Group, Inc.  
All rights reserved  
March 2007*

Founded in 1988, Aberdeen Group is the technology-driven research destination of choice for the global business executive. Aberdeen Group has over 100,000 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.

The information contained in this publication has been obtained from sources Aberdeen believes to be reliable, but is not guaranteed by Aberdeen. Aberdeen publications reflect the analyst's judgment at the time and are subject to change without notice.

The trademarks and registered trademarks of the corporations mentioned in this publication are the property of their respective holders.

