

June 2011

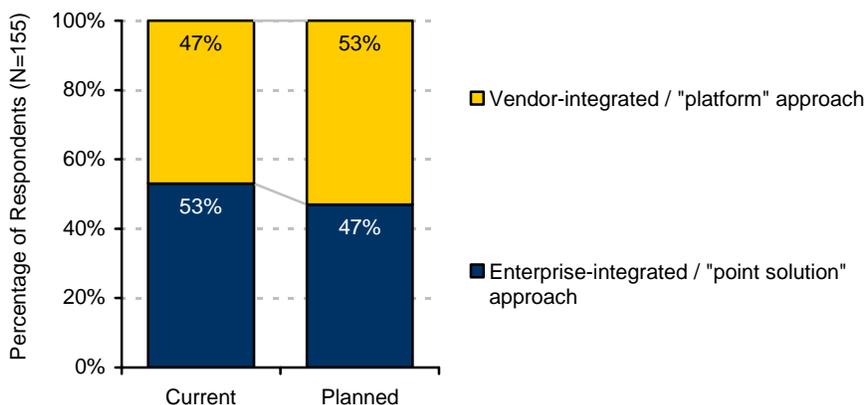
## IAM Integrated: Analyzing the "Platform" versus "Point Solution" Approach

Based on more than 160 respondents from its *Managing Identities and Access* study (February 2011), Aberdeen's analysis of 32 enterprises which have adopted the vendor-integrated (*Platform*) approach to identity and access management, and 39 organizations which have adopted the enterprise-integrated (*Point Solution*) approach, showed that the vendor-integrated approach correlates with the realization of significant advantages – including **increased end-user productivity, reduced risk, increased agility, enhanced security and compliance, and reduced total cost.**

### Business Context: Solution Provider, Integrate Thyself

In Aberdeen's study on *Managing Identities and Access: Intelligence and Automation for Higher Scale at Lower Cost* (February 2011), the findings revealed the beginnings of a distinct shift in the strategic approach that enterprises are taking to the selection and deployment of identity and access management (IAM) solutions. Across all respondents, there was a discernable move away from **enterprise self-integration** of point solutions for IAM toward more of a **vendor-integrated** approach (Figure 1). Some solution providers refer to the latter as an IAM "platform" or "suite"; others emphasize vendor integration but feel that the term "platform" implies an inherent lack of flexibility and choice. Given that the average number of individual or point IAM solutions currently deployed among the study's respondents was between 4 and 5, any approach that shifts the burden of integration from the enterprise to the solution provider is a welcome trend.

Figure 1: Shift from Enterprise-Integrated to Vendor-Integrated



Source: Aberdeen Group, February 2011

### Research Brief

Aberdeen's Research Briefs provide a deeper exploration of the principal findings derived from primary research, including key performance indicators, Best-in-Class insight, and vendor insight.

### Research Demographics

This Research Brief is based on Aberdeen's study of more than 160 enterprises from a diverse set of industries. Demographics of responding organizations include the following.

#### Annual revenue

- √ Small (<\$50M): 32%
- √ Mid-Size (\$50M-\$1B): 36%
- √ Large (>\$1B): 32%

#### Geography

- √ Americas: 56%
- √ EMEA: 30%
- √ Asia / Pacific: 14%

For additional details, see Aberdeen's full benchmark study on *Managing Identities and Access* (February 2011).

## Platform or Best-in-Breed: Which Yields Better Results?

Based on more than 160 respondents from its *Managing Identities and Access* study, Aberdeen analyzed 32 enterprises which have adopted the *Platform* approach to IAM, and 39 organizations which have adopted the *Point Solution* approach, to gain insights into which approach yielded the better results.

### Advantage: Platform Approach

A high-level summary of Aberdeen's analysis of these two groups is provided in Table 1. **Increased end-user productivity, reduced risk, increased agility, enhanced security and compliance, and reduced total cost** are among the significant advantages realized by the organizations adopting the Platform approach – as compared to those adopting the Point Solution approach – to identity and access management.

**Table 1: High-Level Summary of Adopting the “Platform” vs. “Point Solution” Approach to IAM**

Benefits	Description and Derivation of Benefits	Platform vs. Point Solution
<b>Increased end-user productivity</b>	Timely provisioning and modification of end-user access to existing applications or services can save companies hundreds of dollars per end-user per year in terms of convenience, productivity and downtime, and significantly enhance the overall end-user experience.	<i>Advantage: Platform approach</i>
<b>Reduced risk</b>	Rapid de-provisioning of end-user access, on the other hand, is more about <i>cost avoidance</i> than it is about <i>cost savings</i> – e.g., by reducing the window of vulnerability from orphaned accounts and minimizing the potential for downstream misuse. Periodic attestation of access privileges and enforcement for separation of duties are also critical elements of reducing risk.	<i>Advantage: Platform approach</i>
<b>Increased agility</b>	Given the dynamic changes in enterprise end-user populations and application portfolios, faster time to integrate a new application or integrate a new end-user role with the enterprise's IAM infrastructure translates to flexibility and agility to compete more effectively. Pre-integration and workflow spanning IAM components cuts out the complexity and overhead of synchronization.	<i>Advantage: Platform approach</i>
<b>Enhanced security and compliance</b>	Fewer incidents of unauthorized access to enterprise resources related to IAM translates to a huge benefit in terms of cost avoidance, particularly given the high average cost per incident found in Aberdeen's studies. Consistent enforcement of policies and consistent, consolidated reporting for compliance translates to fewer audit deficiencies related to IAM, and the liberation of IT resources for more strategic projects.	<i>Advantage: Platform approach</i>
<b>Reduced total cost</b>	Efficiency of the vendor-integrated approach translates to support for higher scale with fewer FTE admin resources, at lower total annual cost per end-user per year. Common management interfaces across components enable policies which are consistent and easier to administer. Both "internal" and "external" end-users are managed by the same system.	<i>Advantage: Platform approach</i>

Source: Aberdeen Group, June 2011

### Analysis Detail: Vendor-Integration Trumps Self-Integration

The details of Aberdeen's analysis of vendor-integration versus self-integration are summarized in Table 2. On average, companies adopting the Platform approach to managing identities and access consistently realized tangible business value in comparison to those adopting the Point Solution approach, in several important areas.

**Table 2: Adoption of the Platform Approach to IAM Translates to Tangible Business Value**

Average for Each Respective Metric		Platform (N=32)	Point Solution (N=39)	Platform Advantage
<b>Increased end-user productivity</b>	Provide emergency access (e.g., forgotten username or password)	2.0 hours	2.3 hours	11% faster
	Reset a password or PIN (e.g., help desk or end-user self-service)	1.1 hours	1.6 hours	30% faster
<b>Reduced risk</b>	Suspend / revoke / de-provision an existing end-user identity	4.9 hours	5.8 hours	14% faster
	Suspend / revoke / de-provision end-user access to an existing application	3.7 hours	6.8 hours	46% faster
	Average dormant / orphaned accounts found (as a % of total number of accounts)	3.7%	6.5%	44% faster
	Average dormant / orphaned accounts found = none	13%	3%	4.3-times higher
<b>Increased agility</b>	Integrate a new application with the enterprise's IAM solution	43 hours	118 hours	64% faster
	Integrate a new end-user role into the enterprise's IAM solution	19 hours	70 hours	73% faster
<b>Enhanced security and compliance</b>	Unauthorized access to enterprise resources (per 10K users)	0.64	0.74	14% fewer
	Audit deficiencies related to IAM (per 10K users)	0.56	0.87	35% fewer
<b>Reduced total cost</b>	Total annual cost related to IAM initiatives (e.g., including all people, process, technology, hardware, software, services, training, support)	\$8.90 per end-user per year	\$17.10 per end-user per year	48% lower
	Total end-users per FTE IAM administrator	5,500	2,000	2.75-times more

Source: Aberdeen Group, June 2011

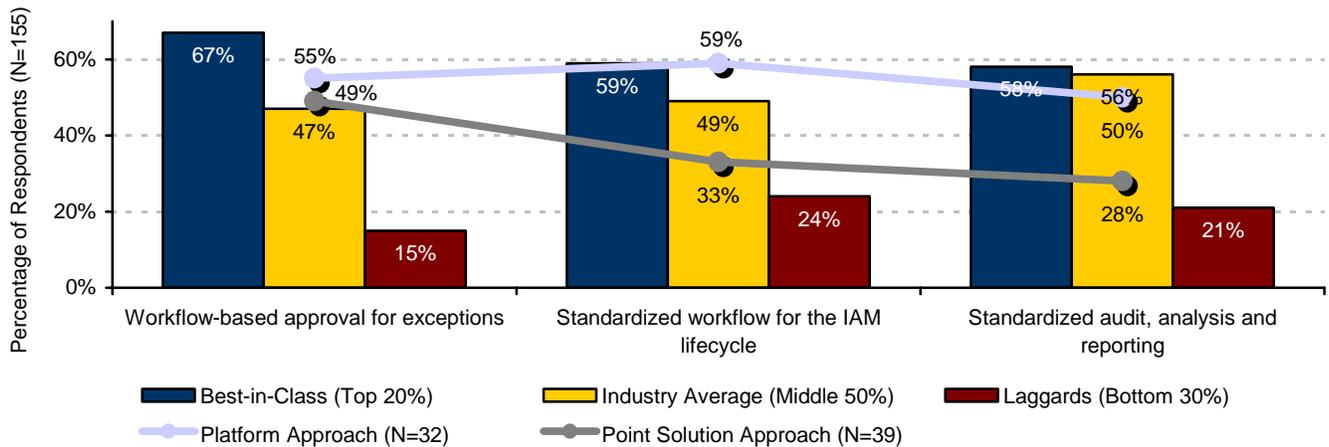
### IAM Capabilities that Differentiate Top Performance

As found in *Managing Identities and Access*, the leading performers are 2-times more likely than lagging performers to have **standardized workflow** for the IAM lifecycle, more than 4-times more likely to have **workflow-based approval for exceptions**, and nearly 3-times more likely to have **standardized audit, analysis and reporting** for IAM-related activities and events (Figure 2). *Automation* of these processes is essential not only to

increasing efficiencies, but also to establishing a higher degree of visibility and control over an increasingly diverse and complex IT infrastructure.

Enterprises adopting the Platform approach are seen to be closest to Best-in-Class (top 20% of all respondents) in terms of current capabilities in these areas, while those adopting the Point Solution approach are between Industry Average (middle 50%) and Laggards (bottom 30%).

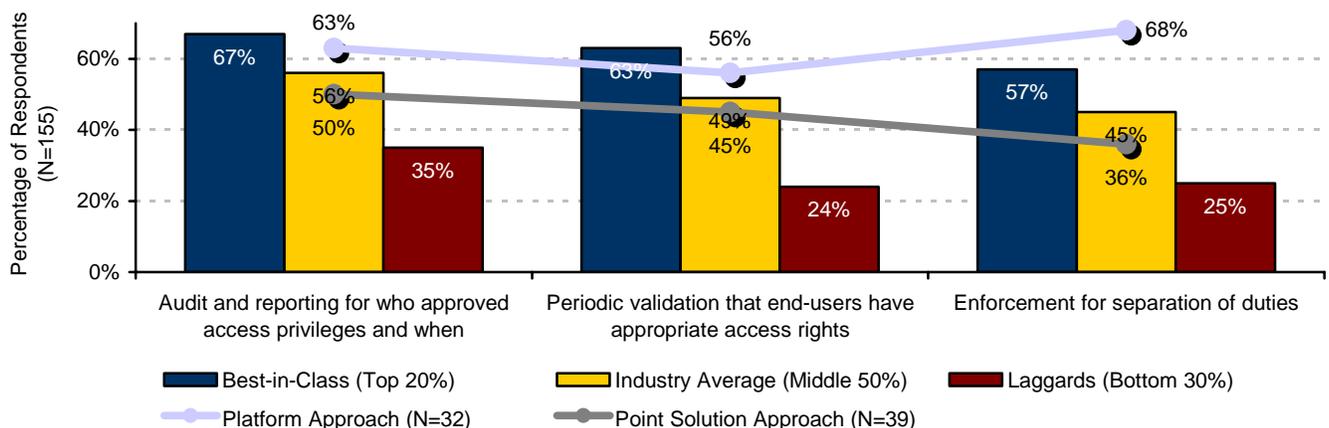
**Figure 2: Standardized Workflow; Workflow-based Exceptions; Standardized Audit and Reporting**



Source: Aberdeen Group, June 2011

A critical part of the opportunity to transform IAM from an IT tool to a business enablement tool is the *increased involvement and accountability of business owners* in the workflow for the IAM lifecycle. **Auditing and reporting** for who approved access privileges and when, periodic validation that end-users have appropriate access rights (i.e., **attestation**), and enforcement for **separation of duties** are capabilities that are strongly correlated with the achievement of Best-in-Class results (Figure 3).

**Figure 3: Auditing and Reporting; Attestation; Enforcement for Separation of Duties**

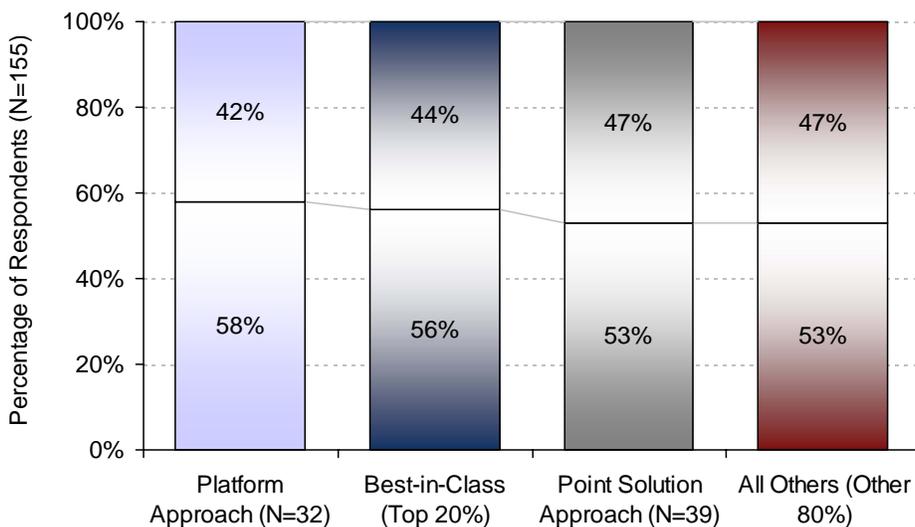


Source: Aberdeen Group, June 2011

Once again, enterprises adopting the Platform approach are seen to be closest to Best-in-Class in terms of current capabilities in these areas, while those adopting the Point Solution approach are between Industry Average and Laggards.

Another important insight about the current state of IAM deployments is gleaned from respondent estimates for the proportion of IAM capabilities that have been achieved by **configuration** (i.e., out-of-the-box) versus **customization** (e.g., custom coding and services) – with the top performers only slightly more able (56%) than all others (53%) to achieve IAM capabilities through configuration (Figure 4). Adopters of the Platform approach have pushed this advantage a bit further (58%); there was no incremental impact for organizations implementing Point Solutions. In general, the promise of a vendor-integrated, field-configured IAM platform is as a delivery vehicle for a collection of IAM capabilities in a more efficient, cost-effective manner than the enterprise-integrated, customized approach – a trend which logically will extend to delivery of these capabilities in the Cloud, in an IAM-as-a-Service model.

**Figure 4: How IAM Capabilities are Achieved – Configuration versus Customization**



Customization  
 Configuration

Source: Aberdeen Group, June 2011

The favorable cost implications of a shift towards configuration rather than customization are numerous, and vendor enhancements in this area will undoubtedly receive strong market welcome. **Consistency** – for example, in policy enforcement, role enforcement, end-user authentication, administrator authentication, visibility into end-user assignments and activities, audit, analysis, reporting, and general manageability – is high among the many tangible and highly desirable benefits. Aberdeen plans to provide a deeper exploration and analysis of the capabilities associated with configuration versus customization – and their positive consequences – in a follow-on Research Brief ([IAM Intelligent: Configuration or Customization?](#)).

## **Case in Point: Business and Financial Management**

---

For a leading provider of business management and financial management solutions, the management of identities plays a critical role – not only for its nearly 8,000 employees and hundreds of millions of online customers, but also for a seasonal population of contractors. The company was looking to address the identity management lifecycle from beginning to end, integrating both events (e.g., hire, change of role or location, termination) and other database-driven attributes (e.g., level, geography, role) from multiple sources.

Starting about two years ago, company architects began an exhaustive, year-long search of IAM solutions – including a formal request for proposal process with over 700 dimensions for product selection, along with formal proof of concept implementations – from leading vendors such as IBM, Oracle and Sun. "It was difficult to resolve to a single solution," noted one of the enterprise architects. "We actually favored one for our enterprise users, and one for our customers." Based on a combination of existing relationships on other projects, the current and likely integration of critical applications, and an assessment of the vendor's vision for the future, the company decided to go with Oracle.

The company's previous IAM implementation (based on custom scripts) had "pretty aggressive service level agreements; they were not always as reliable as we liked, but we were able to bring people on board in less than 10 minutes." The new solution includes the same targets (i.e., < 10 minutes) but has also added reliability, a comprehensive audit trail for visibility and compliance, and integration with a wider range of systems – all of which enable support for higher scale at lower cost.

Work required to implement the new solution was significantly more extensive than expected, but "we opted for doing the right things, even if they took longer time." In terms of lessons learned, the architects suggested that one thing they might have done differently is to identify the top 3-5 areas that absolutely needed to work as expected (i.e., focus on the greatest risks), and force more detailed evaluations and demonstrations (i.e., resolve the most critical uncertainties). "This would have led to a more accurate project plan, and would have helped us to identify where to do more modeling, where to focus our resources, and maybe where to acquire temporary resources." But overall, the company is "pretty happy with the process" ... and with the results.

## Summary and Recommendations

Based on more than 160 respondents from its [Managing Identities and Access](#) study (February 2011), Aberdeen's analysis of 32 enterprises which have adopted the vendor-integrated (*Platform*) approach to identity and access management, and 39 organizations which have adopted the enterprise-integrated (*Point Solution*) approach, showed that the vendor-integrated approach correlates with the realization of significant advantages – including **increased end-user productivity, reduced risk, increased agility, enhanced security and compliance, and reduced total cost.**

Aberdeen's research consistently confirms the merits of a pragmatic "Crawl, Walk, Run" approach as the basic template for successful enterprise-wide initiatives; in the case of managing identities and access, this includes:

- **Adopt a primary strategic focus.** Which of the following strategies supports the most compelling business case for your organization's investments in IAM: *convenience and productivity* for end-users? *Compliance and security* requirements? *Consistency of policies* for managing identities and access to corporate resources? *Cost savings and cost avoidance* through greater efficiency and effectiveness? The essential first step is to identify the strategy that is most compelling for your organization to get started, and begin.
- **Put someone in charge.** Having a responsible executive or team with primary ownership for important enterprise-wide initiatives is consistently correlated with the achievement of top results. IAM initiatives are consistent with this pattern.
- **Prioritize security control objectives** as a function of requirements for risk, audit and compliance. Emphasizing security before compliance, rather than the other way around, reduces the probability of overlaps in controls (which waste resources) or gaps (which increase vulnerabilities).
- **Establish consistent policies** for end-user identities and end-user access to enterprise resources. As the expression of management's intent for the business, consistent policies are the foundation for any successful IAM initiative.
- **Standardize the workflow** for the IAM lifecycle, including workflow-based approval for exceptions. Standardization and automation of workflow should not mean automatic approval, however – on the contrary, increased involvement and accountability for approvals puts a greater responsibility on the *business owners* rather than on the IT staff.
- **Standardize audit, analysis and reporting** for IAM projects, including reporting for who approved access and when, periodic validation that end-users have appropriate access, and enforcement for separation of duties. Quarterly attestation reviews, for example, are common to address requirements for regulatory compliance.

### Determining the Best-in-Class

To distinguish Best-in-Class companies (top 20%) from Industry Average (middle 50%) and Laggard organizations (bottom 30%) in managing identities and access, Aberdeen used the estimated number of the following incidents actually experienced in the last 12 months, along with the estimated year-over-year change in the number of such incidents.

Unauthorized access to enterprise resources

√ Best-in-Class: 2.6 (year-over-year decrease of 5.7%)

√ Industry Average: 3.2 (-3.7%)

√ Laggards: 5.4 (+5.6%)

Audit deficiencies related to IAM initiatives

√ Best-in-Class: 3.0 (-9.7%)

√ Industry Average: 4.5 (-4.3%)

√ Laggards: 5.8 (+5.1%)

Data loss or data exposure related to IAM initiatives

√ Best-in-Class: 1.1 (-6.6%)

√ Industry Average: 1.2 (-2.4%)

√ Laggards: 3.4 (+6.1%)

For additional information, see Aberdeen's full benchmark study on [Managing Identities and Access](#) (February 2011).

- Evaluate and select IAM solutions.** Pay special attention to the level of integration and intelligence provided by the IAM solution provider(s), versus the degree of integration that remains to be completed by the enterprise. Another critical consideration is the proportion of capabilities that can be achieved by *configuration* (i.e., out-of-the-box) versus *customization* (i.e., coding and services). Proposals which are disproportionately heavy with professional services from vendors or their third-party business partners do *not* move a given solution from the enterprise-integrated category to the vendor-integrated category.

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

Related Research	
<a href="#"><i>Governing Access, Controlling Costs</i></a> ; March 2011 <a href="#"><i>Managing Identities and Access: Intelligence and Automation for Higher Scale at Lower Cost</i></a> ; February 2011 <a href="#"><i>Secure Remote Access: From the Outside In, to the Inside Out</i></a> ; January 2011 <a href="#"><i>The Zen of Network Access: First There Was a Border, Then There Was No Border ... Then There Was</i></a> ; December 2010 <a href="#"><i>Access Management: Efficiency, Confidence and Control</i></a> ; June 2010 <a href="#"><i>The CIO's View of Security and Cloud Computing</i></a> ; June 2010 <a href="#"><i>Balancing Enterprise Risk and Reward</i></a> ; January 2010	<a href="#"><i>Managing Access: Roles, Rules, Privileges and Entitlements</i></a> ; August 2009 <a href="#"><i>Selecting Single Sign-On: Four Questions</i></a> ; July 2009 <a href="#"><i>IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs</i></a> ; May 2009 <a href="#"><i>Secure, Complaint and Well-Managed: The Best-in-Class Approach to IT GRC</i></a> ; February 2009 <a href="#"><i>One-Time Passwords for Two-Factor Authentication</i></a> ; January 2009 <a href="#"><i>Managing Privileged Users</i></a> ; April 2008 <a href="#"><i>Strong User Authentication: Best-in-Class Performance at Assuring Identities</i></a> ; March 2008
Author: Derek E. Brink, Vice President and Research Fellow, IT Security ( <a href="mailto:Derek.Brink@aberdeen.com">Derek.Brink@aberdeen.com</a> )	

For more than two decades, 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 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen's research provides insight and analysis to the Harte-Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 854-5200, 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. (2011a)