

# Getting it right.\*

Resolving the complexities of Identity and Access Management



# Table of contents

---

The heart of the matter	4
<b>Resolving the complexities of Identity and Access Management</b>	
<hr/>	
An in-depth discussion	6
<b>Companies that take a holistic approach more efficiently solve today's complex IAM issues</b>	
<hr/>	
A blueprint for planning a solid IAM solution	
New frontiers for IAM solutions	
How IAM can achieve cost savings across the enterprise	
Building a holistic identity and access management strategy	
<hr/>	
What this means for your business	14
<b>How to solve the IAM puzzle</b>	

The heart of the matter

# Resolving the complexities of Identity and Access Management

Has this happened at your company? A manager was terminated in July, but a year-end IT user-access audit reveals his account is still valid on several systems. A tech-savvy employee could easily exploit that account to perform fraud or misappropriate company assets. He could breach security and cause substantial financial losses, as well as violate compliance with regulatory mandates such as the Sarbanes-Oxley Act of 2002 (SOX).

It's your responsibility as a security officer to guarantee that access rights are precise and up-to-date, and your managers and C-level officers must attest to that. But how can they be sure you've done your job?

Assurance can be shaky, given the complexities of identity management. But one thing is certain: Yesterday's ways of managing access don't work anymore.

PricewaterhouseCoopers and its technology partners have the experience to deliver identity and access management (IAM) solutions that help meet business requirements – for today and tomorrow. Our IAM strategy takes a holistic approach to provide automated management of user access, responsibilities, and roles company-wide. This solution streamlines provisioning and deprovisioning as users are hired, terminated, or transferred. It also delivers the critical ability to monitor, review, and test change history, user permissions, and user authorization to sustain compliance.

Although a significant component, technology is only one part of the equation. People – the organization's Identity and Access Management stakeholders – are vital because they will define and ultimately put the IAM solution into service. And unlike some other enterprise solutions, IAM has touch points into the entire organization.

Accordingly, communications to employees and end-user training are an essential part of the process and should be mapped out as the solution is developed, not afterward. A communications plan should take a top-down approach, with C-level executives voicing support for the IAM project from inception to completion. Throughout the process, executives should embrace the IAM project and emphasize the organization's commitment to it, as well as benefits to the company and its employees.

Process is an equally essential component when implementing an IAM solution. Access management processes are often duplicative across the enterprise. What's more, existing user access, management and audits are time-consuming and costly to execute, and often do not provide adequate assurance that the right users have the right access at the right time. Enhancing and, when possible, automating, existing processes will reduce the time and overall complexity of managing user access and result in greater adoption among end users.

These diverse requirements of IAM have left many organizations with an IT infrastructure that resembles an incomplete puzzle: Some applications and solutions fit and interlock, while others are askew or absent. To assemble the pieces of the puzzle, PricewaterhouseCoopers believes that companies must create a holistic, centralized IAM solution that aligns with the existing IT platform, regulatory needs, and business goals. Only then can they resolve the challenges of identity management.

An in-depth discussion

Companies that take a holistic approach more efficiently solve today's complex IAM issues

Identity and access management isn't a new concept. Over the past 10+ years, companies have begun to address identity management through a variety of solutions that have focused on provisioning and web-based single sign-on activities.

Often these tactical initiatives were driven by the need for cost reduction and greater efficiency; but as SOX and other regulatory mandates were introduced, compliance became a key catalyst. Given the current economic environment, the focus is shifting back to cost and efficiency, although the need for compliance has certainly not diminished. These co-existing imperatives demand a solution that addresses the three issues with equal efficacy.

As companies deal with the IAM business drivers, it becomes immediately apparent that holistic, rather than piecemeal, approaches better address their needs. Vendors have recognized this shift in focus and now offer solutions that extend beyond the security organization and aim to improve efficiency and control costs for the entire enterprise. This new breed of identity-management solution provides the foundation to support key areas, such as access control and certification, helping to reduce costs from overlapping compliance requirements and safeguard organizations from insider security breaches.

Given these benefits, it's no surprise that implementation of centralized IAM programs is on the rise. In fact, IAM is among the highest areas of spending in the security budget today. Forrester predicts that the IAM market will grow from nearly \$2.6 billion in 2006 to more than \$12.3 billion in 2014<sup>1</sup> (that figure includes revenue from both products and implementation services).

<sup>1</sup> Identity Management Market Forecast: 2007 to 2014, February 2008, Forrester Research

## **A blueprint for planning a solid IAM solution**

Historically, security solutions have been created and deployed on an application-by-application basis. So, for instance, an employee might eventually accrue a dozen security sign-ons for different applications, which can create confusing – and time-consuming – challenges for users who simply want to get their work done. It also is a costly burden to the help-desk staff responsible for assisting users.

An effective IAM solution can help by ensuring that application development security controls are consistent. Instead of reinventing the wheel each time, customized off-the-shelf, web-based applications and in-house applications alike can leverage the access control model that is critical to any IAM solution.

When planning a solution, the first step is to create a common framework that serves as the foundation on which to build cost and compliance efficiencies. This framework must be built upon user data that is accurate, clean, and consistent in order to yield a successful identity management system. As a leading industry practice, IAM should be established on a foundation of accurate data for identity management, making core identity data available in a uniform manner to downstream applications. This identity data is essential to the success of IAM deployments.

A thorough framework also allows organizations to establish real-time, consistent processes for managing user information across the enterprise. For instance, automated provisioning and deprovisioning of users as they are hired, terminated, or transferred can greatly contribute to the efficiency of user management.

A thorough IAM solution also helps solve the compliance conundrum by delivering visibility into individual access and flagging activities that are out of policy. In addition, it enables monitoring and reviewing (or testing) of change history, user permissions, and authorization – all of which are critical for compliance.

# Companies that take a holistic approach more efficiently solve today's complex IAM issues

## New frontiers for IAM solutions

Mature organizations are looking beyond IAM's basic compliance and cost-saving benefits to harness more advanced capabilities: automated user-access certification and role management. These applications assist in yielding a centralized and detailed view of people, roles, and privileges.

Demand for user-access certification solutions – the capability to help ensure that access is limited to what's appropriate for a person's job function – is skyrocketing. Partly, that's because organizations are more aware of security breaches that can result from inaccurate internal access controls.

As employee roles and responsibilities change over the course of a career, it is difficult for the IT department to monitor access rights to applications and data. Longtime employees often have more access than is appropriate for their current job, simply because there is no automated process to clean up their user-access privileges. And that's when the situation can progress from unmanageable to untenable; because regulations such as SOX require that user access is precise and up to date.

When user-access records are inaccurate or incomplete, a company may face compliance violations, because managers may not be able to attest that employees – as well as third parties, contractors, and temporary staff – have the right access to the right resources.

This new focus on certification highlights a gap that was not addressed by most organizations' typical IAM efforts: leveraging IAM to support certification. Certification should be performed every year – or multiple times a year – to help facilitate regulatory compliance. Companies typically carry out these certifications by manually cross-checking access rights lists that are stored on spreadsheets across the enterprise. Automated solutions, however, now can extract that information from spreadsheets, then centralize and correlate the data of each employee in a systemized way.

As organizations move to certify user access, they may concurrently begin implementing a role-management solution. Role management organizes and automates user-access rights by putting users into manageable groups, each of which has specific access rights that correspond to duties associated with a business function. This enables the organization to more quickly carry out provisioning and simplify the enforcement of security policy and segregation of duties (SoD).

Segregation of duties (also known as separation of duties) is the concept of having more than one person required to complete a task. SoD helps prevent fraud and error by providing controls that assist in reducing the potential damage from the actions of one person. For instance, allowing an employee who sets up vendor accounts to pay those same accounts would violate SoD principles, so a control must separate the roles. And as mentioned above, longtime employees often have more access than is appropriate for their current jobs, and that can introduce the risk of fraud. Role-management solutions can consistently monitor and apply access and segregation-of-duty principles.

Additionally, identity and access management provides support for organizational changes such as mergers or reorganizations by rapidly integrating user communities and standardizing identity and access change mechanisms. An effective, holistic IAM program can also help the organization rapidly bring new products to market by making use of repeatable modules and services.

Outside the enterprise, IAM solutions enable easier integration with lines of business and strategic partners through the secure exchange of user identity information, which allows companies to work more seamlessly with one another.

# Companies that take a holistic approach more efficiently solve today's complex IAM issues

## How IAM can achieve cost savings across the enterprise

IAM has touch points in almost every aspect of business. Consequently, we believe organizations that put the IAM puzzle pieces in place will gain substantial savings – not just in compliance, but also throughout the enterprise. User-access management and controls will balance compliance needs with additional objectives, such as improving operational effectiveness, reducing operating costs, and enhancing agility among business and strategic partners.

Organizations that start their IAM initiatives with access certification typically see the most success with cost reduction related to user-access reviews. That's because IAM provides greater visibility into users' access across the enterprise, and certifications help ensure that access-related user data is accurate and up to date. This holistic approach can save money through increased efficiencies, such as uniform enforcement of information access policies and timely application of termination and access change procedures.

Furthermore, end users will be more productive, thanks to a streamlined single (or reduced) sign-on and the ability to self-administer their access with consistent tools and processes. From a user-access administration perspective, organizations that have effectively implemented IAM will be able to free up their IT staff for other projects.

A repeatable, service-based approach also will bring the organization economies of scale and enable it to reduce the time required to onboard new employees, boost overall efficiency of access management, and speed the process of certification. The use of uniform modules and application security services will help reduce technology development costs and hasten implementation.

### **Building a holistic identity and access management strategy**

There is no shortage of IAM technology solutions on the market, yet you won't find a one-size-fits-all implementation. Instead, you need to shape a well-planned strategy that focuses on risk assessment.

First, perform a thorough analysis of your processes and technologies to develop an IAM framework based upon your company's maturity. Alternately, some companies favor establishing a framework based on a common risk and control analysis that prioritizes risks related to access, roles, and responsibilities across the enterprise. Because it's sometimes difficult for an organization to step back and impartially examine its own processes and risks, this is an optimal time to engage a seasoned professional who can provide advice on best practices for IAM frameworks.

The next step: Take a hard look at your existing business systems to determine whether they work in concert. It's also vital to align the organization's goals to the strategy. Our experience shows that linking an IAM framework directly to business requirements gives companies a much better chance of realizing their goals.

## Companies that take a holistic approach more efficiently solve today's complex IAM issues

It's also essential to focus on governance and map out responsibilities among the stakeholders. You must also assign ownership for each phase of the initiative. Experience shows that the failure (or delay) of IAM implementations can often be traced to a clear lack of ownership.

To address this, first establish a governance structure committee charged with aligning the IAM vision, strategy, and operational tasks. Be certain that the planning includes the necessary stakeholders. Resources from information security, risk and compliance, and internal audit teams should be included, but also reach out to human resources, legal counsel, finance, and business-unit leaders. Engage them to get buy-in and make the project a win for everyone.

Companies typically roll out IAM initiatives in phases, so if they initially pilot a smaller effort and achieve an initial "win," ensuing projects are easier. Basing these subsequent effort on repeatable processes that can be re-created for other areas of the business will help facilitate success while minimizing duplicative costs. When new regulations and requirements roll around, simply extend the existing processes.

What this means for your business

# How to solve the IAM puzzle

PricewaterhouseCoopers believes that companies must adopt a holistic, centralized strategy to create an IAM solution aligned with their IT platform, regulatory needs, and business goals. The successful IAM solution will create a series of centralized services that empower organizations to effectively manage user access across their enterprises and serve as an enabler to lines of business and strategic partners.

The biggest challenge to solving the identity management puzzle is finding, in a single company, the experience to put the pieces in place to draw a full picture of security options. PricewaterhouseCoopers can supply the technology experience and business knowledge and fuse them with our proficiency at solutions integration. And that will give you an IAM solution with one primary investment and reduce the complexity of integrating components.

We can help you design a compelling, aggressive strategy around identity management that aligns people, processes, and technology to solve the complete IAM puzzle. PricewaterhouseCoopers can analyze your IAM needs and help develop an end-to-end solution that will yield a streamlined, enterprise-wide approach to address your business requirements, reduce costs, and improve performance.

Our view is that companies must create a holistic IAM solution that is centralized but reaches across the entire IT platform, regulatory needs, and business goals. Only then can you resolve the complexities of identity management.

To have a deeper conversation on the topic mentioned, please contact:

Brad Bauch	Principal	Houston	<a href="mailto:brad.bauch@us.pwc.com">brad.bauch@us.pwc.com</a>
Rik Boren	Partner	St. Louis	<a href="mailto:rik.boren@us.pwc.com">rik.boren@us.pwc.com</a>
Kevin Campbell	Principal	Atlanta	<a href="mailto:kevin.campbell@us.pwc.com">kevin.campbell@us.pwc.com</a>
Michael Compton	Principal	Detroit	<a href="mailto:michael.d.compton@us.pwc.com">michael.d.compton@us.pwc.com</a>
Shawn Connors	Principal	New York	<a href="mailto:shawn.joseph.connors@us.pwc.com">shawn.joseph.connors@us.pwc.com</a>
Scott Evoy	Principal	Boston	<a href="mailto:scott.evoy@us.pwc.com">scott.evoy@us.pwc.com</a>
Kurt Gilman	Principal	New York	<a href="mailto:kurt.gilman@us.pwc.com">kurt.gilman@us.pwc.com</a>
Joe Greene	Principal	Minneapolis	<a href="mailto:joe.greene@us.pwc.com">joe.greene@us.pwc.com</a>

John Hunt	Principal	Washington	john.d.hunt@us.pwc.com
Jerry Lewis	Principal	Dallas	jerry.w.lewis@us.pwc.com
Mark Lobel	Principal	New York	mark.a.lobel@us.pwc.com
Sloane Menkes	Principal	Washington	sloane.menkes@us.pwc.com
Joe Nocera	Principal	Chicago	joseph.nocera@us.pwc.com
Chris O'Hara	Principal	San Jose	christopher.ohara@us.pwc.com
Fred Rica	Principal	New York	frederick.j.rica@us.pwc.com
Andy Toner	Principal	New York	andrew.toner@us.pwc.com





[pwc.com/us](http://pwc.com/us)

To have a deeper conversation on the topic mentioned, please contact:

Gary Loveland  
Principal, National Security Leader  
[gary.loveland@us.pwc.com](mailto:gary.loveland@us.pwc.com)

This publication is printed on Mohawk Options PC. It is a Forest Stewardship Council (FSC) certified stock using 100% post-consumer waste (PCW) fiber and manufactured with renewable, non-polluting wind-generated electricity.



Recycled paper