From people to process*

Unlocking the value of Identity and Access Management with Oracle Technology

*connectedthinking

PRICEWATERHOUSECOOPERS

Table of contents

October 2008

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 and 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 way of managing access doesn't work anymore.

PricewaterhouseCoopers and its technology partner Oracle have the experience to deliver identity and access management (IAM) solutions that help meet business requirements--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, analyze, and test change history, user permissions, and user authorization to sustain compliance.

User-access controls are also essential ways to manage risk, protect sensitive information assets, and improve business performance.

Although a significant component, technology is only one part of the equation. People — the organization's technology staff and the end-users — are vital to the initiative's success. To meet goals, technology staff must be equipped to begin and support the IAM solution.

And don't overlook preparation: Communications and end-user training should be defined as the solution is developed, not afterward. It's vital that this communication comes from the top. C-level executives should blanket the enterprise with emails to introduce the IAM project and describe the commitment to it. Otherwise, results will be lackluster at best.

Similarly essential is process: the design, implementation, and operation of controls that lay a foundation for IAM deployment. IAM solutions require that processes can be extended to other regulations or areas of the business.

Oracle gives you the puzzle pieces to assemble a solution. To put it together, you'll need to take a strategic look at your organization. This is where PwC and Oracle can help. PwC's proficiency in enterprise security, fused with Oracle's suite of solutions, can deliver a robust, holistic solution that tames IAM's complexity.

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

Enterprise security has never been more essential to effectively meet objectives. However, providing timely, secure access to data and systems across the enterprise continues to challenge many organizations. Protecting the organization from external security threats, managing access to internal resources, and addressing regulatory compliance requirements remains daunting. Yet as the pressure to improve security increases, so too does the drive for additional cost savings.

As many companies know, IAM initiatives can help improve control over internal and external resources. A holistic IAM approach incorporates a range of supporting people, process, and technology imperatives that work together. Companies that take a holistic approach more efficiently and effectively solve today's complex IAM issues.

Identity and access management is not a new concept. Over the past 10 years, companies have taken a tactical approach to IAM by focusing largely on user provisioning and web-based, single sign-on programs. Initially, IAM initiatives were driven mainly by the need to reduce costs, enhance security, and improve the user experience. But as SOX and other regulatory mandates were introduced, regulatory compliance became the primary catalyst behind IAM initiatives. Today, the business drivers behind IAM are shifting back to cost, security, and efficiency, although the need for compliance has certainly not diminished.

As these business drivers for IAM resurface, companies are starting to understand that holistic, rather than tactical; approaches to IAM better address their needs. Even with this paradigm shift, solutions abound that are designed and marketed to address niche IAM requirements. This has resulted in an IAM solution landscape that resembles an incomplete puzzle, with some vendor offerings addressing several, but not all, of the functional pieces.

PricewaterhouseCoopers and Oracle understand this market shift. IAM has long been an integral part of PricewaterhouseCoopers' approach to enterprise security. We view IAM as the convergence of business process and technology, requiring that the proper people, processes and technology solutions are aligned to help an organization meet its objectives. PricewaterhouseCoopers' approach to IAM, combined with the end-to-end solution capabilities of Oracle IAM products, allows clients to address IAM challenges in a holistic manner and meet their objectives more quickly.

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

Building an IAM solution with Oracle's integrated tools

Today, more mature technology plus the sizable reserve of professional experience at PricewaterhouseCoopers can provide a uniform, service-oriented integration framework. The centralized IAM solution, built on Oracle technology, acts as the foundation on which to build cost and compliance efficiencies.

At the core of this framework is a detailed and complete set of identity data. Through its central user repository, the IAM solution provides a standard mechanism for leveraging the identity data to drive user provisioning and access control processes. Identity data that is centralized and complete is essential to the success of IAM processes.

Oracle Internet Directory and **Oracle Virtual Directory** allow central access to user information, without the overhead of storing duplicate copies of data, so the information can be harnessed for user-management decisions. This information includes data used to validate identities, personal information, role information, and passwords and credentials.

Because the data is stored in a central repository, IT teams can efficiently manage user accounts and privileges, including automatic removal of access as users leave the organization. Oracle Internet Directory provides industry-leading scalability and availability for storing massive amounts of identity data. Oracle Virtual Directory provides Internet- and industry-standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

This sort of thorough provisioning solution extends the central user repository to allow for establishment of real-time, consistent processes to manage identity information across the enterprise. The solution can also help ensure that identity data remains current and complete, enabling more accurate access control decisions. Additionally, automated provisioning and deprovisioning of users as they are hired, terminated, or transferred can greatly contribute to companies' security.

Oracle Identity Manager takes provisioning a step further by enabling organizations to manage a user's access across disparate systems, creating a complete picture. The solution provides automated, rule-based provisioning; work flow-based access request capabilities; and a number of feature-rich resource connectivity options. Oracle Identity Manager's flexible architecture can handle complex business requirements, easing the integration burden by adapting to current business processes rather than requiring process changes to meet the capabilities of the tool. Efficient monitoring and reporting capabilities across the connected resources enable the ongoing improvement of policies and security controls, and they assist in compliance monitoring.

This reach across the enterprise data landscape is key. Historically, in-house IT applications have been created and deployed on an application-by-application basis, each leveraging a unique user store and security model. When these are combined with the customized off-the-shelf (COTS), web-based applications already deployed, an employee may be forced to accrue a dozen credentials for different applications. This reduces the cost of development and support and increases end- challenge for many users who simply want to get their work done, not to mention the costly impact on the help-desk staff responsible for helping users navigate this challenge.

An effective IAM solution can help establish that application security controls are consistent. Instead of reinventing the wheel each time, COTS and in-house applications alike can leverage the access control model that is critical user productivity.

Oracle Access Manager further addresses enterprise-wide management of data by combining IAM control services to enable online authentication and authorization. Thanks to its ability to integrate with a number of web servers and web-based applications, Oracle Access Manager provides the flexible framework to extend a standard security model throughout the enterprise to enable single sign-on. The product also provides user self-service, delegated administration, and reporting and auditing, in addition to its access controls.

Some companies, however, may require added security to protect themselves from increasingly common incidents of online fraud and internal data breaches. To that end, **Oracle Adaptive Access Manager** comprises two tools that help safeguard the enterprise and augment the capabilities of Oracle Access Manager. Adaptive Strong Authenticator provides multifactor authentication security for sensitive information such as passwords and personal identification numbers, as well as one-time passwords or public key infrastructure authentication schemes. Adaptive Risk Manager delivers real-time risk scoring, alerts, and actions to identify and prevent fraudulent activity at critical transaction checkpoints. Both employ open application program interfaces to help facilitate easy use with external data sources to further enhance risk scoring.

To help promote that IAM security controls are consistently applied across the applications, many organizations use Oracle Entitlements Server. This solution provides the ability to centrally manage fine-grained authorization privileges for a broad range of applications. The flexible architecture of **Oracle Entitlements Server** allows for centrally managing authorization privileges for heterogeneous resources via a familiar, policy-based security model.

As businesses move toward closer relationships with partners, suppliers, and customers, they need the ability to share identity information securely and seamlessly across various security domains. **Oracle Identity Federation** is a self-contained solution that combines the ease of use and portability of a stand-alone application with a scalable, standards-based architecture for sharing data between business partners. This federated access control and management solution enables users to access applications at partner sites and gives organizations solutions that are inexpensive and simple, while helping improve compliance with privacy and security regulations.

These user-management and access control capabilities help firms to achieve regulatory compliance and cost savings — two business realities that are not likely to diminish. IAM solutions deliver visibility into individual access and flag activities that are out of policy. In addition, a detailed user-management solution provides the ability to monitor, analyze, and test change history, user permissions, and authorization — all of which are critical for sustaining compliance.

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

A new frontier capitalizes on 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 establish 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; since regulations such as SOX require that user access is precise and up-to-date.

When user-access records are faulty, 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: using IAM to support certification. Certification should be performed every year (or multiple times a year) to help facilitate regulatory compliance. Companies typically perform these certifications by 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 to a single employee in a systemized way.

As organizations move to certify user access, they may concurrently begin implementing a role-management solution. Role management aims to organize user-access rights based on similar responsibilities across the enterprise. For instance, a company might formalize job codes or responsibilities into particular roles that carry their own access rights and security levels. As users' roles change, so do their access permissions.

Oracle Role Manager provides a solution by helping businesses identify, define, and manage work and organizational roles and rights across disparate resources. As the system of record for role life cycle management, Oracle Role Manager integrates with Oracle Identity Manager to automate role-based provisioning and access control company-wide.

Another role-based tactic that is becoming a priority in a post-SOX world is 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 segregation of duties 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.

Role management also enables companies to align roles to business operations and policies, thereby automatically linking changes in business relationships to changes in role memberships. This is achieved by consolidating user information stored across the enterprise.

How finishing the IAM puzzle 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 initiative with access certification typically see the most success with cost reduction related to user-access reviews. IAM provides greater visibility into users' access across the enterprise and cleans up the clutter of access-related user data. 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. The timely availability of audit data will reduce the costs associated with conducting access control reviews.

Furthermore, employees 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.

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

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 more quickly allow recertification. And the use of common modules and application security services will help reduce technology development costs and speed up implementation.

These benefits will enable organizations to free up their IT staff for other projects.

Building a holistic identity and access management strategy

There is no shortage of IAM technology solutions on the market. Oracle's robust set of IAM technologies provides the right products for addressing a number of identity and access management needs. To leverage these products effectively, you'll need a detailed IAM strategy.

First, perform a thoughtful, detailed analysis of your processes and technologies to develop an IAM framework based 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.

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 requirements gives businesses a much better chance of realizing their goals.

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 efforts on repeatable processes that can be re-created for other areas of the business will help to promote success while minimizing duplicative costs. When new regulations and requirements roll around, simply extend the existing processes.

How to solve the IAM puzzle

PricewaterhouseCoopers believes that companies must adopt a holistic, centralized strategy to create an IAM solution aligned with their existing IT platform, regulatory needs, and business goals. A successful IAM solution is designed to create a series of centralized services that empower the organization to effectively manage user access and serve as an enabler to lines of business and strategic partners.

The biggest challenge with the IAM puzzle is finding, in a single company, the proficiency to put the pieces in place to draw a complete picture of security options. PricewaterhouseCoopers can supply the Oracle technology skills and business knowledge and fuse them with our experience at solutions integration. And that will give you an IAM solution with one primary investment and reduce the complexity of integrating components. The combination of PwC's in-depth IAM, regulatory compliance, and industry knowledge with Oracle's suite of technology solutions gives organizations a streamlined, enterprise-wide approach to address their IAM issues, reduce costs, and improve performance.

We can help you design a compelling, aggressive strategy around IAM 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	brad.bauch@us.pwc.com
Rik Boren	Partner	St. Louis	rik.boren@us.pwc.com
Kevin Campbell	Principal	Atlanta	kevin.campbell@us.pwc.com
Michael Compton	Principal	Detroit	michael.d.compton@us.pwc.com
Shawn Connors	Principal	New York	shawn.joseph.connors@us.pwc.com
Scott Evoy	Principal	Boston	scott.evoy@us.pwc.com
Kurt Gilman	Principal	New York	kurt.gilman@us.pwc.com
Joe Greene	Principal	Minneapolis	joe.greene@us.pwc.com
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

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

Gary Loveland
Principal, National Security Leader
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