

Streamlining Human Capital Management with Identity and Access Management

An Oracle White Paper

December 2008

NOTE:

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Streamlining Human Capital Management with Identity and Access Management

EXECUTIVE OVERVIEW

Human Capital Management (HCM) applications have become a ubiquitous element in modern corporate strategy to automate business processes with software solutions. From benefits, payroll, and performance management to recruiting and talent management, training, employee and manager self-service, many critical business processes surrounding lifecycle events for all members of the enterprise are automated and managed by an organization's HCM solution.

However for most companies, process automation and quality data management for personnel lifecycle events ends where the HCM application ends. The business processes outside of HR that are concerned with “identities” – role and access management, risk management and compliance, resource and account provisioning, authentication and authorization – also have a critical impact on a company's business yet more often than not these processes remain labor intensive, expensive, inefficient and error-prone. They are not scalable or easily distributed and are inherently difficult to secure and to audit.

Identity and Access Management (IAM) solutions have evolved to address this “other side” of employee and contractor lifecycle events outside the realm of HR and Finance. The purpose of this whitepaper is to describe this role for Identity and Access Management solutions in the framework of business process automation. The natural linkage between HCM and IAM processes afford organizations unique opportunities to reap benefits by unifying these solutions, by “extending” HCM with IAM. In doing so, an organization can, not only produce quantifiable gains in efficiency, security, and compliance, but can also enhance the quality of service delivered through its HCM solution.

INTRODUCTION

Once an employee or contractor is hired and entered into a company's HCM application, identity and access management processes usually begin to break down. Consider the following questions:

- How long does it typically take for a new employee to be provided access to the applications and systems necessary for his or her job?
- Are employees and contractors given the correct access according to policy? Is their access changed as their roles and responsibilities within the company change? Is their access ever de-provisioned when they leave the company?
- How accurate is your corporate "White Pages"? How much manual effort is involved tracking down and correcting the data that appears there?
- Are the authorized people making the appropriate decisions in accordance with business policy? How well documented are these processes?
- How easy is it to generate reports at the requests of auditors to show who has access to what in your critical business applications?

Relying on traditional processes and systems to manage the challenges of granting and maintaining such access for thousands of users connecting to thousands of systems, applications and devices creates far-reaching problems for even the smallest of organizations. The result is that most companies have no idea of the answers to these questions, and what's worse, no easy way of finding out.

Your HCM application was not designed to be an identity management solution, and your Human Resources IT staff were not hired to enforce your corporate security and compliance policies. While HCM applications help to streamline businesses processes, if not properly managed, they can also create an environment where user information is fragmented and difficult to manage centrally.

The important personnel lifecycle events that are captured by your HCM application – hires, transfers, promotions, changes in status, position, and reporting relationships, and so on – need to be broadcast throughout a company's application and technology infrastructure so that roles, accounts, and entitlements remain in consistent alignment with security policies and in compliance with access control requirements mandated by various regulations.

What if your HCM application could automatically trigger the provisioning of new employees and the de-provisioning of terminated employees? What if this system could be automated so that the necessary approvals could be delegated to the proper line of business managers? What if your "day one" new employee onboarding process of providing a new hire with a new computer, phone and voicemail, a cell phone, and accounts to all of the applications and systems took a total of 10 minutes, rather than two to three weeks? What if your HR department

Your HCM application was not designed to be an identity management solution, and your HRIT staff was not hired to enforce your corporate security and compliance policies. While HCM applications help to streamline businesses processes, if not properly managed, they can also create an environment where user information is fragmented and difficult to manage centrally.

could create additional business value by enabling organization-wide efficiency gains for your Operations, Security, and Compliance departments?

IDENTITY AND ACCESS MANAGEMENT CHALLENGES

What are the reasons for this breakdown in the flow of identity data and the processes to manage it? Challenges of the current state include the following factors.

Low quality identity and organization data

There is no single source of truth for identity information for persons of interest (inclusive of user groups such as employees, contingent workers, partners, etc.). Since applications have no reliable means of locating the data needed to make important decisions such as personalization, authentication, and authorization, local application administrators end up manually collecting and managing such information for themselves.

The same holds true for organizational information such as departments, cost centers, and locations. Key Finance and HR planning processes for events such as re-organizations rely on being able to match and align these hierarchies. Historical reports are difficult to generate because of missing or inconsistent data.

Once new identity and organization events occur, the changes take weeks or months to propagate through all of the relevant systems that need to consume this information. Updates to data are necessarily manual and therefore error-prone. The maintenance of all of this duplicate data with multiple, overlapping processes represents an enormous hidden cost for both the business and IT and a significant source of frustration for the IT staff.

Inefficient and scattered administrative processes

Not only are account creation processes duplicated across different applications, they are often manual and paper-based. Rarely are such things as centralized self-service processes put in place to ease this burden. Because of the ad-hoc nature of assigning access, multiple workflows, roles, policies and rules are managed within each application or system. Without a centralized means of control and standardization, not only is effort duplicated but there is no way to ensure that access decisions are made in accordance with business policy.

Poor and inconsistent security

The security picture that emerges from such a situation is grim. Administrators need to cope with complex and error prone manual processes for managing user privileges across disparate systems. Users have to maintain far too many passwords, which increases the likelihood that they will be managed in an insecure manner. As employees move from position to position, or as contractors leave

one organization and rejoin another, access privileges are not changed to reflect these changes in business function and responsibilities. Privileges are therefore accumulated over time, leading to security and compliance risks.

Because there is no defined or enforced access policy, the tendency is to institute an exception-based model: access control decisions are made by business and technology managers on a case by case basis – using approval workflows which quickly multiply into the thousands and become unmanageable.

Incomplete and crude audit and compliance framework

In order to demonstrate compliance with corporate policies and applicable regulations, businesses need to show that access controls have been in place and working as required. Without a centralized process in place to manage access policies and without an infrastructure designed to assign and track user entitlements in applications and systems, most companies have to start from scratch for each audit. This “pick up all the pieces and put them back together” approach is not only time-consuming and costly, but is increasingly causing organizations to fail standards of compliance that are currently being demanded by auditors. Manual attestation processes lack data and process integrity, and can only reactively detect such things as segregation of duties violations.

Non-scalable integration framework

When there are attempts to synchronize data across multiple systems, the likely resort is a series of custom hard-wired point-to-point integrations. Rarely do such customizations – usually built on the spur of the moment for tactical needs – leverage existing industry standards such as SPML and SAML. Because of the ad-hoc nature of this work, deployment, maintenance, and upgrade is expensive and time-consuming. Furthermore, such custom-developed infrastructures may fail basic assurance reviews required by external auditors who may be concerned about the effectiveness of the controls provided.

IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

Identity and Access Management solutions enable HR and HRIT departments to get out of the data management business and focus on the business processes of HCM. By extending the automation of the business processes beyond HCM, Identity Management solutions help to solve the above challenges in the following fundamental ways.

Establish an enterprise identity

The construction of an Identity Management infrastructure starts with consolidating relevant and accurate (i.e. trusted) data from multiple, complex identity environments into a single enterprise identity source. This enables automated linkage of employee and contractor records with user accounts, and the

Identity and Access Management solutions enable HR and HRIT departments to get out of the data management business and focus on the business processes of HCM. .

immediate elimination of rogue and orphaned accounts in systems. Once the data is consolidated, the inherently cross-functional nature of the business processes for identity lifecycle management – from on-boarding through promotion and transfer to off-boarding – can be much better managed with the assistance of automation, workflows, and reporting.

Establish an enterprise organization model

A complete picture of your working organization is just as critical to identity and access management as the complete picture of your authoritative identity. Consolidating department (“org chart”), cost center, reporting relationship, and location data into a single Organization Model captures the important business “context” that serves as the basis for role and policy-based provisioning and access management. Based up such a model, IT can deliver an authoritative and comprehensive White Pages for the entire organization. Administration is distributed according to policy through a graphical UI, allowing HR, Finance, and Facilities to each manage the information appropriate to their own areas of authority.

Establish and enforce enterprise-wide security policies

Upon this foundation of identity and organization consolidation, a consistent set of security policies can be established and maintained, providing a critical linkage to business operations. Comprehensive role-based access control policies for centralized enforcement across applications can be established. Segregation of duty rules that prohibit combinations of roles and entitlements that violate policy can serve as a proactive means of ensuring compliance. Uniform password policies across multiple applications can be implemented, and for high-risk and business critical applications strong authentication mechanisms offer greater protection against improper access.

Automate security-related processes

Once policies are established, a whole set of process automation capabilities can be deployed to reduce costs, reduce complexity, and improve services levels and efficiencies. Knowing an identity’s context within the larger organization is the basis for defining rules that dynamically determine role memberships based upon changes in the business. Users receive access based on the roles they hold and gain or lose access based on changes in roles, ensuring that people are granted the right access at the right time to effectively do their jobs.

Exceptions are managed through approval workflows that are audited to ensure alignment with business policies. Line of business managers need only attest to rules and these occasional exceptions, not to hundreds of individual requests, freeing them to focus on their core responsibilities.

Once a new employee or contractor is now entered into the HCM application, an automated role-based user provisioning process is kicked off to create the appropriate accounts and privileges in business applications. When an employee leaves the company, the same infrastructure ensures that such access is immediately revoked, closing security holes and lowering administrative costs.

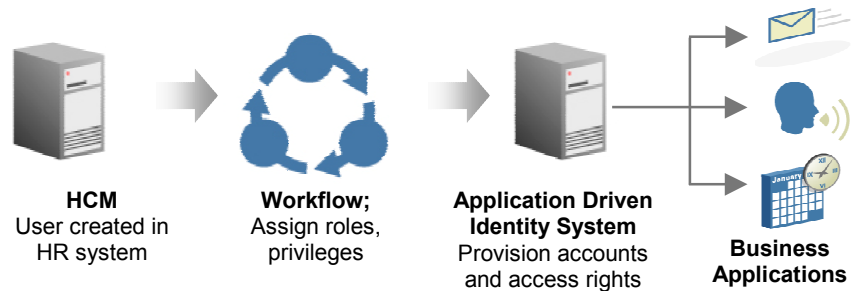


Figure 1. Automated user provisioning process with Identity Management.

Define an audit and control framework

Establishing a centralized and comprehensive view of people, roles, and privileges, will immediately result in more accurate and efficient compliance and reporting, and significant improvement of policies and controls. By centralizing identity management and access control, it is possible to automatically produce accurate reports documenting which users have access to which systems, and who accessed what at what time. It is also possible to determine who had access to which systems at any point in the past, using historic audit data and forensic analysis.

In order to ensure that roles, privileges, accounts, and access remain current and in alignment with the changing needs of the business, a feedback loop is needed that attests to the policies and processes that have been put in place, and certifies that correct access has been granted in accordance with those policies and processes.

Automated and workflow-driven attestation forms present this data to authorized reviewers for sign-off on the accuracy of the data and provides reviewers with the means to document and correct any violations or exceptions to policy. Attestation processes can be run on demand or can be scheduled for periodic execution at regular intervals, whether it is once a year, once every six months, or once every quarter.

Deploy a scalable integration architecture

Lastly, Identity and Access Management solutions provide an integration framework to enforce access management policies across all systems and applications. The use of a scalable and standards-based infrastructure provides for connecting all of the pieces of the puzzle together transparently and in a cost-

effective manner: from HCM to user directories to business applications and underlying databases and operating systems

Oracle leads the industry with award-winning Identity Management offerings that constitute the most comprehensive solution offered by any vendor.

ORACLE IDENTITY MANAGEMENT

Oracle leads the industry with award-winning Identity Management offerings that constitute the most comprehensive solution offered by any vendor. Not only do customers get a complete end-to-end solution, they also benefit from proven best-in-class functionality.

COMPREHENSIVE. Providing best-in-class technologies. This includes web access control; identity administration; user provisioning; federated identity management; directory services, including virtual directory technologies; and enterprise wide user provisioning.

HOT-PLUGGABLE AND OPEN. Interoperates with all major directories, application servers, portals, business applications, databases, and operating systems. Oracle works with standards bodies such as the Liberty Alliance and OASIS, and supports, SAML, SPML, WS-*, Kerberos, and many more.

APPLICATION-CENTRIC. Weaves security into applications as opposed to bolting it on, promising unprecedented efficiencies and ROI.

Oracle Access Manager

Oracle Access Manager is a state-of-the-art solution for centralized identity administration and access control. Oracle Access Manager delivers the functionalities of web single sign-on, access policy creation and enforcement, user self-registration and self-service, delegated administration, password management, and reporting and auditing. It supports all leading directory servers, application servers, web servers, and enterprise applications.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is a comprehensive solution for purely web-based strong authentication security and proactive, real-time fraud prevention.

Oracle Role Manager

Oracle's Role Manager provides unique features to speed the process of role discovery and to deliver automated enterprise role management solutions. Oracle Role Manager serves as the role management repository for identity and access management systems. It leverages previous investments in identity and access management, and synchronizes roles and policies with privileges in target systems

Oracle Identity Manager

Oracle Identity Manager is a highly flexible and scalable enterprise identity management system that centrally controls user accounts and access privileges within enterprise IT resources. It provides the functionalities of identity and role administration, approval and request management, policy-based entitlement management, technology integration, and audit and compliance automation. Oracle Identity Manager delivers flexibility and scalability with product features such as a J2EE implementation, N-tier deployment architecture, browser-based user interfaces and Oracle Grid compatibility.

Oracle Identity Federation

Oracle Identity Federation is an industry-leading federation solution providing a self-contained and flexible multi-protocol federation server deployable with existing identity and access management systems. Oracle Identity Federation is Liberty Alliance certified for Liberty ID-FF and SAML 2.0.

Oracle Internet Directory

Oracle Internet Directory is an LDAP v3 service that combines the mission-critical strength of Oracle's database technology with the flexibility and compatibility of the LDAP v3 directory standard. Supporting heterogeneous environments, Oracle Internet Directory can be synchronized against third party directories including Microsoft Active Directory, SUN Java System Directory Server, Novell eDirectory and OpenLDAP.

Oracle Virtual Directory

Oracle Virtual Directory allows you to rapidly deploy secure directory enabled applications by providing a real-time, virtual view of identity data from any data-store including directories, databases and Web Services without synchronization. With Oracle Virtual Directory, you can logically join identity attributes stored in multiple data-stores as well as prioritize requests to back-end directories on a per-server or per-connection basis, to maximize the native directory's processing potential.

Access Control	Identity Administration	Directory Services		
Strong Authentication & Authorization Risk Based Access Control Single Sign-On Federation	Identity & Organization Lifecycle Administration Enterprise Role Management Provisioning & Reconciliation Compliance Automation	Virtualization Synchronization Storage		
Audit & Compliance				
Audit Data	Attestation	Fraud Detection	Segregation of Duties	Controls
Management				
Service Levels	Configuration	Performance	Automation	

Figure 2. Oracle's Comprehensive Identity and Access Management Solutions

CASE STUDIES: SOLUTIONS IN PRACTICE

Let's look a few cases studies to see how Oracle Identity and Access Management products were used to deliver real-world solutions to clients.

Role automation for a retail brokerage

Challenge

A Fortune 500 company needed to manage rapidly-changing roles spread across 300 locations, 15 regions, 300 branches, and 6000 employees. Neither the corporate directory, the HCM system, nor the ERP system were authoritative for key identity attributes or could model an organization of such complexity. The company was using a series of spreadsheets to manually manage 42,000 separate role assignments across these various locations and organizations. These role assignments needed to be attested and reported to the NASD (National Association of Securities Dealers) monthly – far more often than before and with greater accuracy.

Solution

Oracle Role Manager was deployed to create a business-centric role management solution that provided a single source of the truth for role assignments.

- At the end of the project, only five roles remained un-automated, and the 42,000 separate role assignments were reduced to 77 role grants
- Employee lifecycle events such as new hires, transfers, and terminations result in immediate re-calculation of role assignments

- Attestation reports from this data are generated automatically and are guaranteed to be accurate
- Compliance violations have become virtually impossible. Any potential violation would result in proper notification in minutes after its occurrence.

Automated provisioning for a manufacturing firm

Challenge

Authorization workflows could not adapt to changes in the business environment to ensure the right people were making the right access decisions. Risks of compliance violations were steadily increasing as a result of this lack of effective control and insufficient auditing of user access privileges. Suffering from broken manual processes for password resets and account provisioning; the company could not cope with increasing volume of helpdesk calls, decreasing productivity, and skyrocketing operational costs. After unsuccessfully trying to implement a competitive identity management solution, the company turned to Oracle for help.

Solution

Oracle Identity Manager was selected to replace the obsolete provisioning framework, and was quickly integrated with PeopleSoft, Siebel, RACF, and the Microsoft Active Directory environment.

- The provisioning process was automated in response to business events, via integration with PeopleSoft HCM
- There was documented evidence of compliance with accurate “who has what” reporting across business-critical applications
- Help Desk costs were slashed by measurable reductions in call volume due to self-service password reset
- Within 2 weeks of rollout, 90% of rogue accounts and privileges across managed systems were eliminated

Pervasive identity management for an investment bank

Challenge

An investment bank determined that its mission-critical systems were vulnerable as a result of a large number of orphaned system accounts and improper control over user privileges. There were no detailed audit trails of each user’s access rights, making compliance with external regulations such as Sarbanes Oxley and Gramm-Leach-Bliley extremely burdensome if not impossible. The processes for onboarding new employees were manual, as were help desk and system administration processes for responding to such common requests as password resets.

Solution

Oracle Identity Manager was selected after a long and detailed evaluation process. It was immediately put to work to develop an open integration architecture to automate password resets and account provisioning.

- ‘Day one’ lead time for new employee access was reduced to under 5 minutes
- A single authoritative source for user access was created
- The compliance effort across fifty SOX-related applications was reduced by 12 man weeks
- Ghost accounts were eliminated via reconciliation changes in target systems
- To date, upwards of 1,200 systems have been brought under control

Oracle Identity and Access Management solutions are integrated to work with your Oracle PeopleSoft applications, helping you achieve the benefits of extending HCM with Identity Management more quickly with less risk..

Key Oracle Differentiators in Identity and Access Management:

- **“Application Centric”.** Oracle Identity and Access Management solutions are integrated to work with your Oracle PeopleSoft applications, helping you achieve the benefits of extending HCM with Identity Management more quickly with less risk. The Oracle Identity Management suite provides a common layer of security and control across all of your enterprise applications.
- **Complete, unified solution.** The Oracle Identity Management suite is a complete and integrated set of best-of-breed components that can be deployed individually and in tandem. It is the only suite in the marketplace with an integrated Enterprise Role Management solution.
- **Proven in the real world.** The solutions are proven for large-scale deployments, and leverage Oracle’s expertise in providing mass-scale information solutions for the world’s largest organizations. Oracle Identity and Access Management solutions enjoy a broad and referenceable customer base.
- **Best long-term investment.** This breadth and depth offers the best long-term investment for a company’s Identity and Access Management strategy. Oracle is committed to strong support of open standards and its “hot-pluggable” strategy. Oracle Identity and Access Management solutions integrate out-of-the-box with leading applications and infrastructure components.

CONCLUSION

Extending HCM deployments with Identity and Access Management solutions offers companies a unique set of capabilities to address business process, integration, and data management challenges across the enterprise in order to:

- Maximize productivity by ensuring that new employees have the tools and information they need to do their jobs on day one
- Increase security and compliance by ensuring that user access is based on business policy and that individual accountability is maintained
- Reduce administration costs and increase the security posture of the organization by automating employee and contractor on-boarding, transfer, and off-boarding processes
- Minimize the total cost of compliance and reduce the risk of a failed audit by providing accurate documentation of who has access to what, granted by whom, and when

These demonstrable and proven benefits have been realized by Oracle clients worldwide with the adoption the industry-leading suite of Oracle Identity and Access Management solutions.



Streamlining Human Capital Management with Identity and Access Management

Dec 2008

Author: Steve Wolford

Contributing Authors: Eric Maurice, Hormazd Romer

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

oracle.com

Copyright © 2007, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Other names may be trademarks of their respective owners.