ORACLE IDENTITY GOVERNANCE SUITE

KEY FEATURES

- Simplified Access Request with intuitive and extensible user experience drives user productivity, increases user satisfaction and optimizes operational efficiency
- Centralized and extensible access catalog to store and further define business friendly definitions for Roles, Applications & Entitlements
- Requests with approval workflows and policy-driven provisioning improves IT efficiency, enhances security and enables compliance
- Role based access control with Role Mining & Advanced Role Lifecycle Management
- Risk-based, business user friendly Identity Certifications & closed loop remediation of access rights
- Continuous IT Audit Monitoring and Reporting

KEY BENEFITS

- **Increased security:** Enforce internal security audit policies and eliminate potential security threats from rogue, expired and unauthorized accounts and privileges.
- **Privileged Account Management:** Allow users to gain access to sensitive applications in a timely manner, while providing sufficient audit trails
- **Enhanced regulatory compliance:** Cost-effectively enforce and attest to regulatory requirements (e.g. Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA) associated with identifying who has access privileges to sensitive, high risk data
- **Improved business responsiveness:** Get users productive faster through immediate access to key applications and systems, while enforcing security policies
- **Reduced costs:** Reduce IT costs through efficient, business friendly self service and platform-based architecture

Organizations need to balance the requirements to provide users with quick and easy access to the systems they need to perform their jobs with the organization's risk and compliance obligation to ensure such access is as restrictive as possible. To achieve this balance, organizations need to deliver intuitive ways for users to request access to systems and applications, appropriate policies and processes to approve such access, simple ways for managers to confirm that such access is appropriate and finally, monitoring tools for managers and administrators to periodically check and certify that access is properly assigned to employees. Further, these systems need to apply to both standard user accounts and high risk, privileged accounts, which are often shared. Oracle provides a complete Identity Governance solution that enables organizations to efficiently balance the objectives of access, security, and compliance, while enabling user self services to reduce total cost of ownership.

Oracle Identity Governance

Oracle Identity Governance reduces the total cost of ownership for organizations by empowering user self-service, simplifying audit tasks and streamlining future version upgrades. By delivering a comprehensive platform for access request, role lifecycle management, access certification, closed loop remediation and privileged account management, Oracle is delivering a solution that both simplifies the process to address today's requirements and enables organizations to address emerging requirements.

Simplified Access Request

Organizations are eager to reduce costs and accelerate processes by empowering user self-service. Embracing this paradigm, Oracle Identity Governance solutions include out-of-the-box, shopping cart style access request interfaces that are designed to follow common practices popular on commercial e-commerce sites, such as "add to cart", "review cart", "checkout out" etc. Core to empowering end user self service is the expressive Access Catalog: a glossary that includes user-friendly names for all systems and resources to simply the user process of searching for the right system or business application. Further, this catalog also includes enterprise items such as sensitive, privileged accounts, roles and entitlements, necessary to drive roles-based provisioning. While the out-of-the-box access request system is designed to be robust, customers requiring customizations will also benefit from the ability to easily develop durable customizations, which can upgrade to future versions of the product, reducing total cost of ownership for future upgrades.

ARCHITECTURE OVERVIEW

- **Integrated Solutions:** Oracle Identity Governance Suite solutions - Oracle Identity Manager, Oracle Identity Analytics & Oracle Privileged Account Manager work together to create an integrated governance process for the enterprise
- **Ease of Deployment:** UI Customizations and integrations are durable and can survive patching and upgrades
- **Flexible and Resilient:** Oracle Identity Governance can be deployed in single or multiple server instances. Multiple server instances provide optimal configuration options, fault tolerance, redundancy, fail-over and system load balancing
- **Maximum Reuse of Incumbent Infrastructure:** Oracle Identity Governance is built on an open architecture to integrate with and leverage existing software and middleware already implemented within an organization's IT infrastructure
- **Standards-based:** Oracle Identity Governance incorporates leading industry standards, such as J2EE, BPEL and OASIS

Advanced Role Lifecycle Management

In an effort to effectively managing the proliferating number of users, many organizations are leveraging roles to assign and manage rights and privileges. To support this approach, Oracle Identity Governance includes innovative and robust role discovery and lifecycle management capabilities, which both harvest roles as they are created and manage approval for entitlement changes against these roles, including real time impact analysis for role consolidations before changes are pushed to production. All role activities are fully audited and provide the ability to roll back changes, should it be necessary.

Streamlined Access Grant

While driving self-service for access request simplifies processes, access grants must be approved by authorized entities. Oracle Identity Governance leverages standards-based approval workflows, which include enterprise capabilities such as delegating approval and including supporting attachments on workflow requests to provide additional detail on decisions. Finally, customers can leverage the Identity Connector Framework connectors that extend benefits both for account creation/reconciliation and also support privileged account management requests.

Privileged Account Management

Within virtually every organization, there are sensitive, privileged accounts, such as Root Admin accounts. These accounts must be shared between multiple users and are frequently not managed securely. Oracle identity Governance enables organizations to extend core identity management policies to these sensitive, privileged accounts. Administrators, or super users, seeking access to these accounts can use the standard, access request interface and Access Catalogue to request access to these accounts. Standard approval workflows apply and organizations can leverage their existing Oracle identity manager connectors to manage passwords on these systems. By extending the existing identity management policies to privileged accounts, organizations have improved audit capabilities and can properly plug these accounts into a broader access certification processes.

Simplified Identity Certification

As the number of applications to which employees have access increases, certifying access becomes imperative, especially for larger enterprise organizations. In order to efficiently scale and sustain, these processes need to be both automated and resilient. With advanced, risk-based analytics and easy to navigate dashboards, Oracle Identity Governance offers a robust set of identity certification features that streamline the review and approval processes to effectively manage risk on an ongoing basis. Beyond understanding "who has access to what", in depth analytics can provide detailed, 360-degree views on how such access was granted and highlights outliers for individuals versus their roles. Finally, the solution offers closed loop remediation, which provides an automated way for reviewers to revoking improper access across target systems and includes alerts should remediation fail.

IT Audit Monitoring & Reporting

Oracle identity Governance provides both policy-based audit monitoring and detailed and flexible reporting capabilities. Comprehensive dashboards enable both system administrators and delegated administrators to run reports on virtually any artifact of a user's access rights, access grants and the genesis of each. The Oracle Identity Governance Suite offers the ability to define and enforce detailed security policies both within and across applications. This enables intelligent monitoring to identify imminent violations typically caused by access grants following job changes or other HR events. Finally, decisions made to identity certification reports are always stored and archived for audit purposes.

Contact Us

For more information about Oracle Identity Governance, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2012, Oracle and/or its affiliates. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1010

Hardware and Software, Engineered to Work Together

ORACLE