An Oracle White Paper
August 2011

Oracle Identity Analytics

A Business Overview

Disclaimer

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.

Table of Contents

1. Executive Summary

With the explosive growth in networked communications and collaboration, it's no longer enough for today's enterprises to know who has access to what. Effective role management and access governance requires knowing not just who has access, but what they are doing with that access.

This comprehensive understanding of access is essential to reduce the risk that an employee, contractor, or malicious third party with inappropriately assigned access will take advantage of that access. It is also critical to complying with regulations that mandate access controls; without it, companies have no way to provide meaningful evidence to auditors that explains how and why access was assigned within their environment.

For many enterprises, compliance is an ongoing challenge that is increasingly difficult to master as regulatory requirements continue to grow and change. The need to perform multiple, difficult tasks — such as certifying access, enforcing security policy, and remediating policy violations — is compounded by the reliance on slow, error-prone manual processes to handle them. These issues, coupled with the lack of a comprehensive, cohesive approach to compliance and auditing, make it nearly impossible to address the challenge in an effective and cost-efficient manner. As a result, enterprises are in the unenviable position of committing significant resources to compliance efforts with little assurance that they will prove successful.

In addition, most organizations today, struggle with satisfying stringent compliance mandates to perform access reviews of users with access rights to thousands of business applications and target platforms, and making it a sustainable and repeatable exercise.

Automation is the key to increasing the effectiveness and reducing the cost of compliance. Automation streamlines compliance related processes, reducing the need for resources while at the same time lowering the risk of manual error that can lead to audit failure. Most importantly, automation makes it possible to create sustainable, repeatable audit processes that enable the enterprise to address compliance in an ongoing manner without starting from scratch to address every new regulation or prepare for every audit.

A software solution that automates access control, particularly the processes of identifying, aggregating, and correlating access to individual users, can play a critical role in enabling sustain- able processes for achieving effective and cost- efficient compliance.

2. Oracle Identity Analytics – A Business Overview

Oracle Identity Analytics software provides enterprises with the ability to effectively achieve and manage access compliance and automate critical identity- based controls. Oracle Identity Analytics also allows roles to be defined, certified, and assigned, and then continues to deliver value throughout the user access lifecycle by:

- Providing a complete view of access-related data that includes the user's access; the "who, why, how, and where" of that access; whether the access violates defined SoD policies; how the access was granted to the user, whether it was previously certified, and activity associated with the access

- Automating the entire process of certifying and reviewing access and removing inappropriately assigned access

- Providing evidence that access is being defined according to established policies

- Enabling changes in access based on changes in users' roles to minimize the disruptive effects of change on user productivity

Oracle Identity Analytics reduces operational risk exposure by providing a 360-degree view of users' access—not just who has access to what, but whether access was appropriately assigned and how it is being used. This empowers an organization to make intelligent and informed decisions about the type and level of access assigned to users.

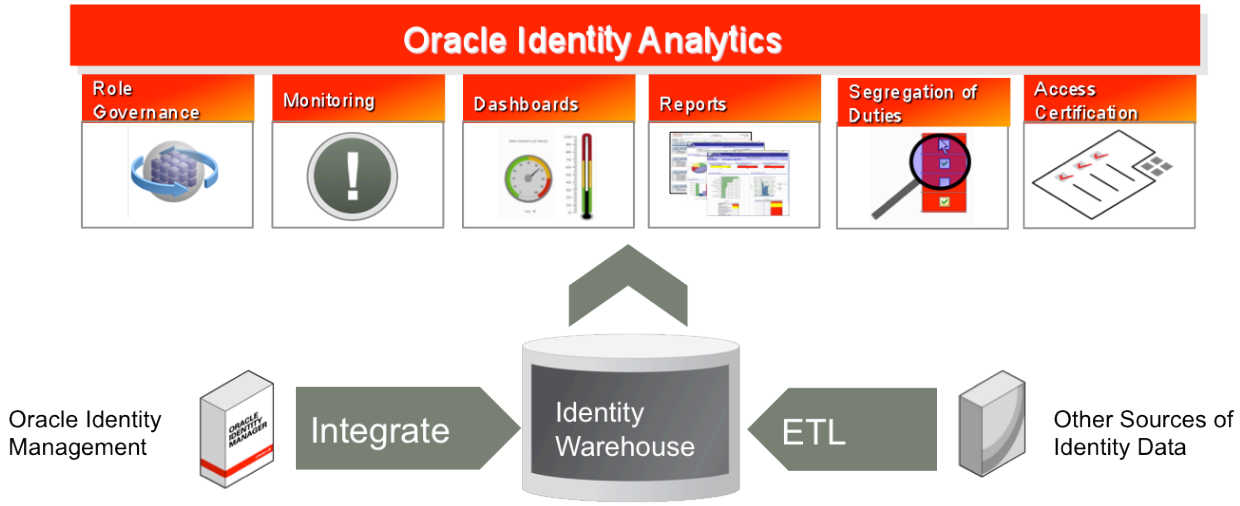
Oracle Identity Analytics provides metrics driven Identity Intelligence, powered by rich risk analytics, which is crucial in measuring how well IT supports the business and manages risk, and provides enterprises with the tools they need to mitigate risk, build transparency, satisfy compliance mandates and support business decisions.

The software also increases security effectiveness by reducing the number of users who are assigned access combinations that are inappropriate or that constitute SoD violations. For example, a user whose job includes setting up vendors should have to give up the access privileges associated with that role if he/she assumes a new position that involves writing checks to those vendors. Oracle Identity Analytics automatically detects this and other types of similar violations across the enterprise and automatically revokes access and verifies that remediation has taken place.

Oracle Identity Analytics is designed to help you better address regulatory mandates, automates manual processes, and quickly makes compliance a repeatable and sustainable part of business. It is a simple and cost-effective solution for user certification and enterprise segregation of duties (SoD) enforcement. You can address compliance challenges head-on with features that enable you to successfully certify access, enforce SoD, track requests, and report status.

Features

Identity Warehouse



Identity Warehouse is the central repository that contains identity, access and audit data, optimized for complex analytical queries and simulations. This data is imported from one or more databases within your organization on a scheduled basis. Oracle Identity Analytics import engine supports complex entitlement feeds saved as either text files or XML. Oracle Identity Analytics provides strong and robust integration capabilities with the provisioning products including Oracle Identity Manager and Oracle Waveset. The integration focuses on synchronization of common identity data with well-defined authoritative ownership of each entity.

The Identity Warehouse schema is optimized for complex analytical queries and simulations that are typically required for role governance. An optimized analytical schema is core to providing highly scalable and sustainable compliance features like attestation, segregation of duties analysis, role impact analysis, compliance dashboards and reports. Identity warehouse also provides data classification and ownership features for example ownership of entities and attributes, risk classification of attributes and identification of highly sensitive or privileged data. This helps organizations prioritize governance and analytical activities that may be performed on the identity warehouse data. Additionally, business glossary feature of identity warehouse allows organizations to capture, assign, and manage business-friendly descriptions of often cryptic IT entitlements for presentation to business users. This helps to ensure that business users understand what they are reviewing and are better able to make informed decisions.

Access Certification

Oracle Identity Analytics automates the complete process of consolidating and correlating identity and access data across the enterprise, presenting the collected access data to the appropriate business owner (application, manager, or data) for review while capturing the audit trail of the entire process. Certifications may be scheduled flexibly based on any segmentation of the user population as well as triggered automatically based on important events that occur during a user’s lifecycle (on-boarding, transfers, off-boarding, and so on). The Identity warehouse centric architecture allows customers to use a single, integrated certification solution to certify user’s resource entitlements, roles, exception access to defined policies and the access policies themselves. Enterprises that implement Oracle Identity Analytics as part of their security and compliance initiatives may expect to see an ROI within 90 days of implementation by automating the manual, complex and error prone certification process.

Oracle Identity Analytics reduces operational risk exposure by providing a 360-degree view of users' access – not just who has access to what, but whether access was appropriately assigned and how it is being used. Oracle Identity Analytics securely automates existing manual re-certification or attestation processes for certifying the user access rights by business managers and application owners. This significantly reduces costs associated with existing manual controls and enhances audit effectiveness, resulting in enforcement of "least privilege" across the enterprise. The solution includes capabilities to:

- Automatically collect, correlate and audit the identity data from multiple enterprise resources.
- Dynamically generate risk-based certification populations to ensure that certifications are performed by the appropriate business & application owners.
- Aggregate Identity Risk and provide an intelligent Sign-Off User Experience to business reviewers, taking into account last attestation histories, open audit violations and provisioning audit trails, i.e. identifying *How* resources and roles are being provisioned to users. In addition, spreadsheet like views, advanced sorting and filtering capabilities and bulk-certify options provide reviewers with the tools they need to sustain potentially large volumes of user access information in their attestation reviews.
- 360-degree view of assigned access which goes beyond "who has access to what" to reveal how the access was granted and what was done with the access, including policy violations and last attestation histories. This allows reviewers to make intelligent decisions concerning user access.
- Closed Loop Remediation, which provides an automated, end-to-end solution for reviewing and revoking access and automatically verifies remediation and sends alerts if remediation does not take place. This helps control the cost of compliance by automating remediation processes and reduces the risk of policy violations and compliance failures.
- Data Owner Certifications, which provide a bottom up view of user entitlements to, designated Data Owners allowing them to make accurate decisions.
- Certification of role definitions allowing business users to ensure that role and policy definitions continue to comply with corporate policies.

SoD enforcement

It is well known fact that majority of the computer-related criminal activity is a result of malicious activities performed by insiders. One of the most prominent threats is fraud that is particularly difficult to detect in computerized environments as automated through workflow systems. Therefore, it is of great importance to implement mechanisms to prevent such illegal activities. Segregation of Duties (SoD) is a key vehicle for preventing fraud and detecting errors in the process of conducting financial transactions. Segregation of duties is a time honored and universally practiced principle for this purpose. That is, no individual is given sufficient authority within the system to perpetrate fraud on his own. This is achieved by breaking larger actions into smaller steps executed by distinct individuals. For example issuing a check may be into preparing a voucher; having it approved, and finally writing the check. SoD policies then ensure that conflicting combinations or roles, entitlements and responsibilities of these smaller steps are not assigned to the same user.

With the ability to define and enforce a security policy both within and across applications, Oracle Identity Analytics delivers a comprehensive solution for enforcing SoD policies. Policies may be defined at fine-grained entitlement or coarse-grained role levels within an application or across applications, leveraging the complete set of identity and access data in the identity warehouse, collected from across the enterprise, and the enforcement process may be scheduled or executed on-demand. Oracle Identity Analytics offers the following for SoD policy enforcement features:

- Define SoD policies at roles or entitlement level within an application or across applications.
- Automatically identify imminent violations when users are provisioned especially after job changes that may affect their duties.
- Integrate with Oracle Identity Manager and Oracle Waveset to allow preventive simulation of SoD policies enabling compliant provisioning.
- Maintain an ongoing record of activities with the potential impact to SoD, such as job changes and password reset.
- Record and notify management of all attempts to access confidential, restricted, or other sensitive enterprise resources.

Remediation Tracking and Validation

Oracle Identity Analytics allows users to initiate a request to correct exception and unauthorized access during a regularly scheduled access review or when reviewing a SoD violation. These requests may be propagated automatically to change management systems (help desks) or leading user provisioning systems, or sent directly to an assigned administrator via email. Regardless of the destination for the change request, Oracle Identity Analytics tracks these requests and validates that the inappropriate access is corrected while capturing the associated audit trail.

Analytical Dashboards & Reports

Oracle Identity Analytics provides comprehensive dashboards and reporting capabilities based on user identity, access and audit data residing in the Identity Warehouse. Oracle Identity Analytics provides various compliance and operational dashboards for a quick review of compliance and operational status in context of roles, segregation of duty policies, audit policies and other controls. While compliance dashboards are typically used for executive level compliance monitoring, detailed out of box reports enables IT staff, business users and auditors to structurally analyze the warehouse data. The dashboards can further be customized for business users, compliance and audit officers and other end users on need basis. While Oracle Identity Analytics provides close to 50 out of box reports, its data dictionary is published to allow customers to extend these reports and build custom reports.

Some of the statistical dashboards provided out of box with Oracle Identity Analytics include:

- Complete progress statistics of all attestation types
- Progress of all pending and completed role owner approvals and attestation requests
- Percentage of open, closed and risk accepted Audit exceptions
- Status of high risk Audit exceptions
- Complete certification statistics of users roles and accounts across all attestations in the enterprise
- Health Monitors on percentage of outstanding attestation progress
- Percentage of high privileged entitlements assigned to Users
- Number of rogue accounts detected per month
- Number of role membership grants per month

Some of the reports provided out of box with Oracle Identity Analytics include:

- Roles assigned to Users within each business structure in the enterprise
- Accounts associated to Users within each business structure in the enterprise
- Roles and associated policies within each business structure in the enterprise
- List of all entitlements and their data owner
- High privileged entitlements associated to users in the enterprise
- Operational exception reports classifying any missing data required for important correlations such roles without any policies, users with no roles, users with no entitlements, business structures with no associated users and so on
- Import validation reports displaying data not imported to the Identity Warehouse due to correlation issues or missing fields and improper format
- Expiration forecast reports specifying user expiration, role expiration and role to user expiration
- Terminated user reports displaying terminated users in the enterprise for historical reporting
- Assigned vs. actual reports displaying users with access outside their roles

Role Lifecycle Management

Roles defined across an enterprise are subject to evolve over time, and require a robust administration and audit process. Oracle Identity Analytics provides role approvals upon detection of associated entitlement updates and performs real time impact analysis for role consolidation before changes are applied in a live environment. Role change approval process combined with role versioning, role change “what if” simulations and rollback features, it provides a complete role change and lifecycle management solution. As part of its role lifecycle management features, Oracle Identity Analytics fully audits all the changes made to role definitions including role assignment rules and entitlement mapping policies.

From a governance perspective, Oracle Identity Analytics provides role content certifications upon detection of entitlement updates and also performs impact analysis prior to initiating changes to live environments with respect to Roles. It also provides a complete audit trail around Role changes and role memberships. Oracle Identity Analytics enables role versioning, which creates an offline copy of a Role without disturbing the “live” version of a Role and provides capabilities to revert to any Role version recorded in the Warehouse. This improves the overall organizational flexibility by making it fast and easy to change access based on business needs and also improves the alignment between IT and business organizations.

Provisioning Integrations

By integrating with leading user provisioning solutions, such as Oracle Identity Manager and Oracle Waveset, Oracle Identity Analytics can take advantage of the existing connections to applications provisioned by these systems for collecting access data, completing automated remediation requests and exporting roles designed in Oracle Identity Analytics to the Identity Management solution for automated provisioning. The software also includes “what-if” scenario testing for determining the impact that changes to rules will have on assigning access. In addition, “provisioning method” integration, allows reviewers in Oracle Identity Analytics to accurately identify how the access was granted in Oracle Identity Manager, associated approval audit trails and identifying corresponding risk associated to the assignment.

Event Listeners

Event Listeners introduce automated post import evaluation of users by automatically triggering attestations or SoD policy scans based on user on-boarding or job transfers. This completely automates critical job transfer based access reviews; ensuring employees moving across business structures are not carrying forth-unnecessary access

3. Benefits

Scalable & Sustainable Compliance

By automating access review and revocation, Oracle Identity Analytics software helps control the overall cost of complying with regulations that man- date access controls. With Oracle Identity Analytics, the need for resources devoted to compliance and audit performance is significantly reduced. In addition, extending access to more users and keeping track of that access is bound to increase the cost of doing business if there is no solution in place for role-based access control. Oracle Identity Analytics addresses this concern by reducing the cost and complexity of extending access in the following ways:

- Ability to define and maintain a business glossary for the cryptic IT entitlements is key to automating the compliance process. Traditionally business users have struggled to use automated compliance processes due to lack of understanding of complex entitlement labels used in IT systems. Oracle Identity Analytics enables business users to leverage compliance automation by providing a business glossary of access data to them

- The use of roles lowers costs by simply reducing the number of objects that have to be managed for certification reviews and SoD monitoring. Instead of attempting to manage tens of thousands of individual entitlements across thousands of applications, Oracle Identity Analytics can be used to define and manage far fewer roles into which those individuals fit.

- Assigning roles to users speeds up and streamlines the processes associated with assigning access privileges, monitoring their access, and reporting on violations or potential violations.

- Oracle Identity Analytics provides an automated alternative to using slow, error-prone manual processes to create and manage roles. Manual processes place an undue burden on IT personnel and business managers and can lead to costly errors when responding to audit requests or proving compliance.

Operational Efficiency

Oracle Identity Analytics improves operational efficiency by simplifying and automating access-related processes and bridging the gap between the IT infrastructure and the business organization.

By creating and managing roles, Oracle Identity Analytics software eliminates the need to manually manage and audit access for each individual user. Consider, for example, how your organization can transform the process of finding out what resources a new employee needs to do his or her job. Without Oracle Identity Analytics, you might simply ask another employee (although there is always the possibility that the employee could be wrong). Regardless of the method used, determining resource needs on an employee-by-employee basis wastes an enormous amount of time that could be spent more productively. Oracle Identity Analytics eliminates such problems by managing access based on roles and automating all related processes.

Your organization can also improve operational efficiency by using Oracle Identity Analytics to bring the IT infrastructure and the business organization closer together and provide them with a common vocabulary. This is the result of mapping business roles to the underlying entitlements that are granted within enterprise applications. The establishment of a common vocabulary ensures that the roles reflect how responsibilities are assigned within your organization, which makes it easier for employees to request the access necessary to do their jobs.

Flexible Deployment Architecture

Different organizations have different priorities and business drivers for identity administration, provisioning and governance deployments. Flexible architecture of Oracle Identity Analytics allows customers to break down the overall deployment in multiple phases with a wide variety of choices for first few phases as follows:

- **Remediation Choices:** While typically phase-1 implementations focus on discovering and remediating unauthorized access by enforcing controls like attestation and SoD policies, Oracle Identity Analytics provides multiple choices to implement remediation of unauthorized or rejected access rights. They may integrate the remediation with existing provisioning deployments, existing ticketing systems or simply choose to implement an email notification based remediation system. While customers mature their remediation system from email based remediation to ticketing system based tracking to fully automated remediation through provisioning integration, Oracle Identity Analytics provides consistent audit and tracking of remediation for compliance purposes. The preventive and detective controls chosen for Phase-1 (attestation, SoD monitoring, dashboards, exception tracking & reporting etc) can evolve in a deployment independent of the remediation solution. This decoupling of compliance enforcement and remediation provides customers complete flexibility for how they choose to mature their identity governance solution.

- **Identity Warehouse Population:** Customers have multiple choices for how the identity warehouse is populated. Customers can deploy Oracle Identity Manager and set up file-based upload of entitlements in Oracle Identity Manager. This information can then be synchronized in Oracle Identity Analytics for governance needs using out of box integration between Oracle Identity Analytics & Oracle Identity Manager. Alternatively, Oracle Identity Analytics also provides a quick an easy way to import user and their associated entitlement data into its Identity Warehouse directly. Oracle recommends using Oracle Identity Manager as it enables customers to collect entitlements without investing into provisioning automation and connector deployment in the first phase, but it allows them to also organically innovate their existing deployment for closed loop remediation and active connector based provisioning in later phases.

- **Compliance Controls:** Oracle Identity Analytics architecture is flexible enough to support multiple variations of this architecture for example:

  - Customers can first perform continuous SoD monitoring in Phase-1 and then choose to do SoD exception attestation in Phase-2, followed by complete user and resource owner attestation in Phase-3.

  - If customers have existing provisioning and reconciliation deployment, they can transport data into OIA through provisioning synchronization, provided out of box for Oracle Identity Manager, and automate remediation/cleanup for exceptions and problems discovered in SoD analysis and attestation. Therefore, customers can extend their existing OIM or Oracle Waveset deployments into OIA or vice versa.

4. Conclusion

Today, compliance is a major driver for deploying identity management solutions. When considering vendor options, customers should carefully evaluate product quality and vendor vision in delivering a compliance centric solution. The selected solution should provide strong capabilities to not only define and enforce policies, including Segregation of Duty policies, but also to detect and remediate exceptions in a timely fashion. The solution must also satisfy the broad set of requirements in access certification for business users, line managers and application/resource owners.   And as compliance is often related to the auditing activities performed by internal and external auditors, the selected solution must be able to retain all historical records, allowing the records to be analyzed and rendered through reports and dashboard in an on demand basis. And last but not least, the solution must demonstrate the flexibility to provide both a quick ROI for customer facing immediate compliance needs - and a long-term strategic governance solution when combined with identity management components such as a provisioning solution or an access management solution. When these factors are considered, Oracle Identity Analytics is the ideal choice to start or complement your existing identity management deployment towards reaching your identity and access governance goals.

Contact Us

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

Oracle Identity Analytics
Business Whitepaper
August 2011
Author: Neil Gandhi
Contributing Author: Viresh Garg

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

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