ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Unified Identity Governance

A Business Overview

ORACLE WHITE PAPER | August 2017

ORACLE

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

Executive Overview

Application proliferation has created identity fragmentation as user identities are inconsistently managed across applications in the enterprise, increasing risk and cost. Enterprises need to ensure users have sufficient access privileges to perform their job functions, but for compliance and security reasons it's also important to constrain such access. Accordingly, enterprises must make it easy for users to acquire and provision access, and also easy for managers, resource owners, and system administrators to review and revoke access. Oracle's Identity Governance solution is designed to help enterprises balance these objectives of access, security, and compliance.

Business user experience is also a key factor for Identity Governance initiatives in most enterprises today. A simple, persona oriented end-user experience enables business users to complete key Identity Governance tasks seamlessly, while truly understanding the task they are performing or taking action on. Today, Identity Governance solutions are no longer geared solely towards administrative users; rather they enable business users to complete key tasks through intuitive self-service interfaces.

For large organizations, getting users the access they require can be a frustrating and time consuming task. Manual processes used to on-board users, link identities and terminate users are often times, inefficient and error prone. In addition, privileged account access is poorly managed, creating unnecessary risk. New users have little exposure to IT jargon that would enable them to request privileges by name. New users often resort to requesting the same kinds of access as their peers, who may have privileges that new users shouldn't. And as employees and contractors work on a variety of projects, transfer departments and locations, change their job functions, and get promoted, their requirements for access change. At a deeper level, system administrators require access to privileged, shared accounts that allow them to perform business-critical and administrative functions. Often, these accounts are "root-level" accounts that don't use an administrator's named account, so it becomes critical to grant access to the right individuals in a timely manner. For all of these scenarios, Oracle provides an identity governance solution to simplify access grants by enabling users to request access in simple web-based catalogs, and by routing those requests to appropriate approvers. The solution also provides privileged account management, which controls access to shared, root-level or admin accounts.

Similarly, access certification is an ongoing challenge for most enterprises, but necessary for compliance with regulations such as Sarbanes Oxley (SOX), HIPPA and GDPR. The need to perform multiple, difficult tasks—such as certifying user access rights, enforcing security policies, and automatically revoking unnecessary access rights—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 obliged to commit significant resources to compliance efforts. Oracle simplifies certification challenges by automating the review cycle. Oracle's Identity Governance solution automatically detects user privileges, segregation of duties violations and orphan accounts. It also notifies appropriate stakeholders of any action they need to take, applies risk scores to help stakeholders prioritize their certification tasks and makes changes to privileges and accounts once a decision is reached.

This white paper discusses how Oracle's Identity Governance suite components work together to create complete and converged identity governance process for the enterprise.

Oracle Identity Governance Suite – A Complete Approach

Oracle Identity Governance provides a modern and simplified solution for managing accounts and access privileges across business applications and platforms. With a complete and converged platform, Oracle Identity Governance provides numerous benefits, including:

- Helps organizations manage risk and reduce costs with a unified Identity Governance solution that manages standard and privileged user access.
- Increases end-user productivity with rapid user on-boarding, consistent and intuitive business friendly self-service interfaces, common business glossary and catalogs, immediate access to key applications and role lifecycle management.
- Increases IT productivity by automating provisioning tasks and streamlining controlled access to privileged accounts.
- Reduces cost and complexity by delivering Self Service, Access Request, Access Approval, Access Certification, Identity Audit and Provisioning services across a common identity platform. Independent research has shown that a platform approach to Identity Management can lower operational costs by 48% and result in 33% fewer audit deficiencies
- Reduces risk with guaranteed access revocation, detection and management of orphaned accounts, monitoring of IT audit policies, fine grained authorization controls, periodic re-certifications and continuous evaluation of policy and role based access
- Helps in improving business responsiveness by providing immediate access to key applications and systems, while enforcing security policies
- Helps in reducing IT cost by efficient, simple and business friendly self service and application on boarding UI.
- Simplified application on boarding will fasten the process on boarding application in OIG and significantly reduce the time and effort to go live.
- Helps in enforcing internal security audits policies and eliminates potential security threats from rogue, expired and unauthorized accounts and privileges
- Cost effectively enforcement and attestation of various regulatory compliances (SOX, HIPPA, GDPR etc).

The solution supports a variety of popular administrative styles such as roles, rules, and policies to enable flexible and scalable administration. The Solution offer very simple and business friendly application on boarding process. In addition, users can search an expressive catalog when requesting access to applications, data and platforms. The system routes requests to the appropriate approvers before granting access while enforcing various rules and performing the necessary segregation of duties analysis. The access request interface is a business friendly, web-based interface that allows a user to request access for themselves and for others.

In order to continuously monitor and effectively enforce compliance controls, Oracle Identity Governance provides automated periodic reviews of users access rights and monitors for exceptions to IT audit policies. These measures ensure employees aren’t able to acquire a combination of access rights that would allow them to perform fraudulent activities.OIG also let you choose groups of review which can define based on business process. Additionally, Oracle Identity Governance continuously monitors and detects segregation of duties violations and rogue access grants that originate outside the Identity Governance solution. Oracle Identity

Governance also provides rich audit and reporting capabilities that allows line of business managers, IT administrators and auditors to review not only who has/had access to what but also how they acquired that access. This level of insight also extends to use of privileged accounts. Oracle Identity Governance also provides continuous Role Lifecycle Management capabilities for role owners to approve content changes to roles by empowering them with intelligent analytics tools, thus providing increased accountability and prevention of role explosion in the enterprise.

Oracle Identity Governance provides automated provisioning and de-provisioning across many target applications and services. It uses grant assignment and removal to determine when to provisioning and de-provision access, and includes comprehensive auditing of all operations

Assembling the Blocks – Core Solution Components

Oracle Identity Governance provides a number of core services, each of which solves a unique governance challenge faced by many enterprises.

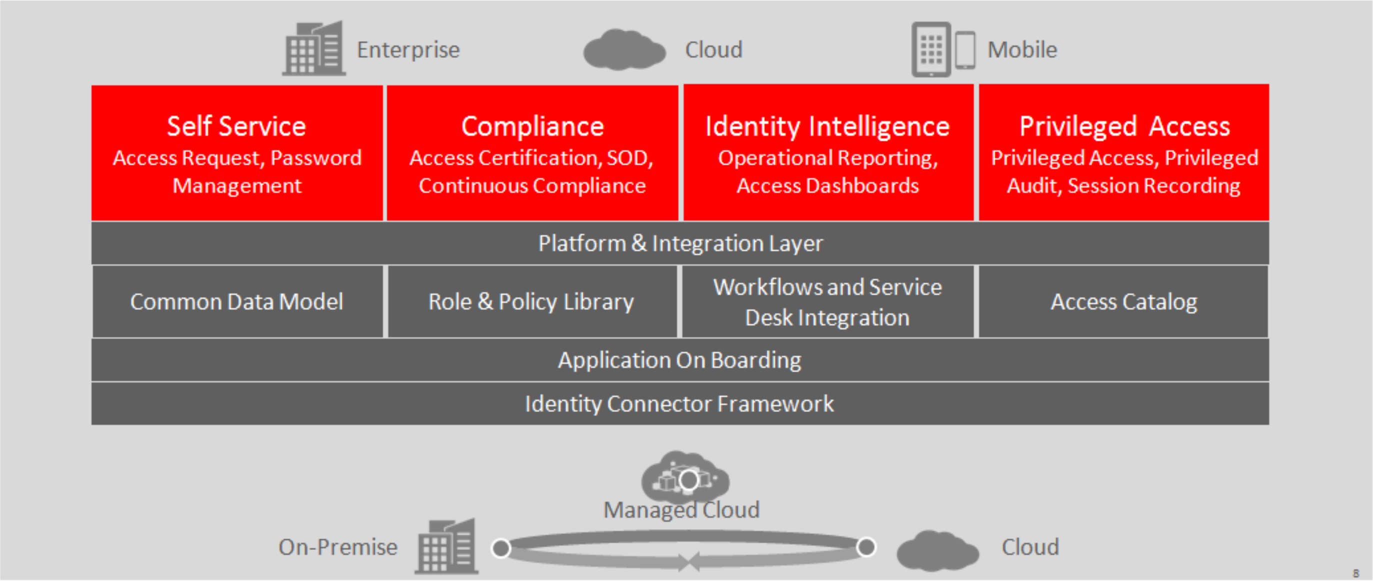

Enterprise
Cloud
Mobile
Self Service
Access Request, Password Management
Compliance
Access Certification, SOD, Continuous Compliance
Identity Intelligence
Operational Reporting, Access Dashboards
Privileged Access
Privileged Access, Privileged Audit, Session Recording
Platform & Integration Layer
Common Data Model
Role & Policy Library
Workflows and Service Desk Integration
Access Catalog
Application On Boarding
Identity Connector Framework
Managed Cloud
On-Premise
Cloud
8

Figure 1:-. Oracle Identity Governance Suite – Core Solution Components

Business Friendly Application on Boarding

Oracle Identity Governance provides a quick and convenient way to on-board applications (AOB) using the Applications option to business users. It quickly on boards the application into the OIG system and save the time and cost to bring one application on board. The wizard based simple approach allows business users to step through basic configuration to complete the application on boarding process. It just asks for the minimum details to on board an application.

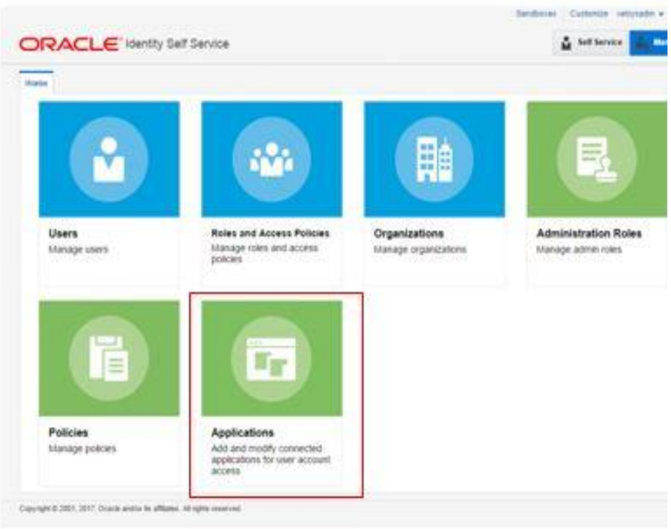

Sandboxes | Customize | xelsysadm ▾
ORACLE Identity Self Service
Self Service
Home
Users
Manage users
Roles and Access Policies
Manage roles and access policies
Organizations
Manage organizations
Administration Roles
Manage admin roles
Policies
Manage policies
Applications
Add and modify connected applications for user account access
Copyright © 2001, 2017, Oracle and/or its affiliates. All rights reserved.

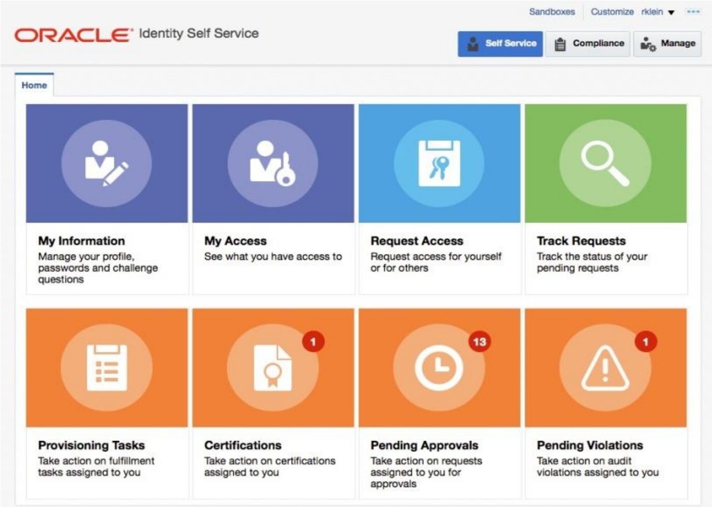
Figure 2:- Application On Boarding

This offers an interface to write business logic for validation and transformation business logic capabilities which need not to be complied and plugged in with binaries. It offers the application template creation and import export options by which one application can be easily import/export form one environment to other environment. Application on-boarding offers capability in Oracle Identity Self Service to create and manage applications, templates and instances of applications and clone applications. AOB templates cover most of the features offered by design console.

An application templates is just the xml representation of the application with some pre-filled values, with the help of application templates you can create any numbers of applications.

Business Friendly Self Service

Oracle Identity Governance provides a rich set of services to business users via a simple and intuitive self-service interface, which provides a guided, task driven experience that allows end-users to easily view and take action on Applicable tasks. The guided approach allows users to step through each task and know exactly what they need to do to complete the task, whether it involves changing a password, submitting an access request or completing a certification review of their direct reports. Delegated business administrators and Compliance administrators can also take advantage of these robust self-service capabilities to complete their tasks as well. The table friendly, self-service interface is persona-centric and only displays the tasks that pertain to a specific user persona, whether it’s a business user, a manager, an auditor,


Sandboxes | Customize | rklein ▾ ···
ORACLE Identity Self Service
Self Service
Compliance
Manage
Home
My Information
Manage your profile, passwords and challenge questions
My Access
See what you have access to
Request Access
Request access for yourself or for others
Track Requests
Track the status of your pending requests
Provisioning Tasks
Take action on fulfillment tasks assigned to you
1
Certifications
Take action on certifications assigned to you
13
Pending Approvals
Take action on requests assigned to you for approvals
1
Pending Violations
Take action on audit violations assigned to you

administrator, etc. The interface is also easy to customize using robust ADF customization capabilities that are durable and patch-safe.

The Access Catalog is at the heart of Oracle Identity Governance and an important component for enabling key self-service tasks. It provides a robust and intelligent catalog of access rights across various applications and platforms. This Catalog acts as the initiation point to request access, approve access and provision access. Approved access – for standard and privileged users – are fulfilled through a comprehensive set of Identity Connectors.

OIG has huge numbers of connectors; with the help of these connector automatic provisioning/de-provisioning happens immediately. OIG connector stacks includes:-

Business Applications: Oracle Fusion Applications, Oracle E-Business, PeopleSoft, JD Edwards, Siebel and SAP
LDAP stores: Oracle Internet Directory, Oracle DSEE, Oracle Unified Directory, Active Directory and e-Directory
Security systems: RSA, RACF, Top Secret, ACF2
Collaboration Suites: Exchange/Domino and GroupWise
Operating systems: OEL, Red Hat Linux, HP-UX, AIX, Solarix, AS/400 and Windows
Ticket Management systems: BMC Remedy
Cloud Connectors: Oracle CRM On- demand, Google Apps, Office 365, Salesforce, ServiceNow, Concur, Box, DropBox, GoToMeeting, WebEx and SuccessFactors
Databases: Oracle, MySQL, SQL Server, DB2, Sybase
Technology Integrations: SSH, Telnet, Flat File, JDBC, LDAP V3, SOAP, Generic Scripting Connector(BeanShell, Groovy and JS), REST and SCIM

Organizations then monitor this access and enforce compliance with Identity Certifications, IT Audit Monitoring, Rogue Access Detection and Audit and Reporting capabilities. These services are described in detail in sections below.

The Access Catalog

Oracle Identity Governance provides a catalog of access rights, including enterprise and application roles, application accounts, and entitlements. A common data model provides a 360-degree view of access rights and history to strengthen compliance. The catalog automatically *harvests* privileges when new definitions of entitlements are detected in a target application or when the roles are defined or modified using the built-in role administration features. Catalog administrators, along with application administrators, then enrich the harvested data to make it friendly for the business users. In particular, for each role, application and entitlement in the catalog, administrators can author business friendly descriptions, list the audit objectives, and set risk levels. While the catalog management system automatically populates a set of search tags based on names and descriptions of the catalog entities, catalog administrators can also seed keyword tags by which business users may find the roles and entitlements in various search results. Additionally, administrators can provide metadata for the catalog items. For example, they can specify the users or roles that will be involved in approval, certification or manual provisioning fulfillment activities related to the corresponding roles, accounts or entitlements. Once configured, catalog information is available across the identity governance functions including request creation, request tracking, approval, request history, manual provisioning and certification.

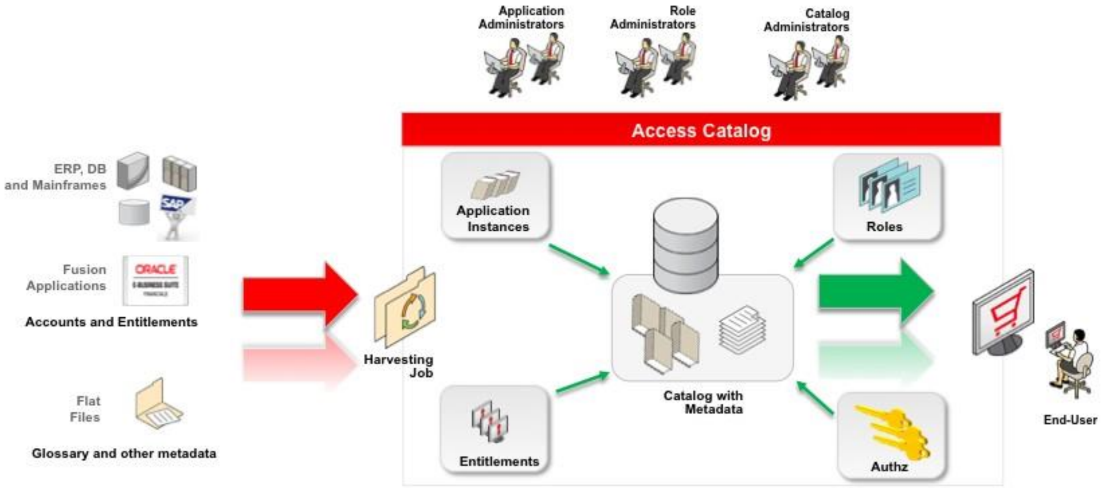


Figure 2. Oracle Identity Governance Suite – Access Catalog

Access Request

The Oracle Identity Governance Suite provides a browser-based tool to request access. The access request experience is similar to the “shopping cart” metaphor used in many e-commerce websites, so users are able to request access without the need for thorough training and require only a basic understanding of the organization’s roles applications, and entitlements. Users simply search for the roles and entitlements they require by entering keywords they are familiar with. They can further refine and filter search results by using the tool’s automated suggestions. Once users find the entitlements they need, they simply place the appropriate entitlements in a cart and submit the request.

Access Request provides a robust set of capabilities around business user friendliness, monitoring and UI customization, as described below.

Business User Friendliness of the Access Catalog

The Access Catalog makes it easier for requestors to quickly request the access rights they need across a variety of applications and target resources. These access rights can be granted via roles, entitlements or accounts in various applications. In addition to these, end users can save search results in a saved request cart and share these carts with other users. These “request profiles” can be used as a template for requesting a *basket* of frequently requested privileges.

The Access Catalog itself features robust search capabilities that follow the semantics of a web-based search engine. End users are not required to know the cryptic names of accounts and entitlements or complex search operators, rather they can rely on business friendly keywords or partial words (e.g. “pay” will return “payroll”) to quickly search for, find and request the access rights they need in order to perform their job responsibilities. Also, they can browse the catalog via smart forms that enable them to build their own filtering results to display the access privileges that match a specific set of search criteria (for example, a category of applications, or applications that belong to a specific geography or department, and so on).

The roles, entitlements and applications residing in the Access Catalog feature extensible metadata, with the ability for administrators to create business level glossary descriptions such as creating high level categories to organize access rights, providing multiple search tags for these access rights, as well as defining user friendly descriptions, risk levels and audit objectives. Each Role, Entitlement and Application can also be assigned owners for approvals as well as certification. Once this catalog metadata is configured, it is consistently available across the various identity governance functions including access request, request tracking, approval, request history, manual provisioning, and certification.

Preventative IT Audit Policy Analysis during Access Request

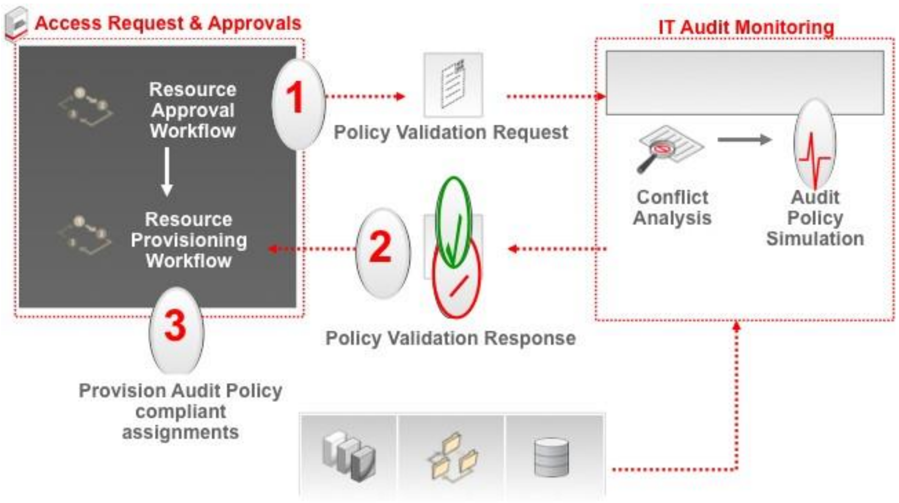

Access Request & Approvals
Resource Approval Workflow
Resource Provisioning Workflow
1
Policy Validation Request
2
Policy Validation Response
3
Provision Audit Policy compliant assignments
IT Audit Monitoring
Conflict Analysis
Audit Policy Simulation

Figure 3. Oracle Identity Governance Suite – Preventative IT Audit Analysis & Simulation

As shown in Figure 3, Oracle Identity Governance provides a comprehensive solution for automating and enforcing preventative IT Audit policies. During an access request, a “what if” policy validation request is initiated from the provisioning process and run through a preventative simulation to determine if undesired access rights are being requested. This ensures that undesired access is not granted to a user, enforcing compliant provisioning practices.

Tracking a Request

Users and help-desk administrators can track the progress of their requests online through the solution’s comprehensive tracking tool. The tracking tool graphically displays the current state of the request approval in the provisioning workflow with a business friendly image that displays what steps are complete and what steps remain to fulfill the request. Using this tool, users can ensure their requests are handled in a timely fashion.

UI Customization & Durability

Oracle Identity Governance UI customizations can be performed using drag-and-drop editing in a web browser, without any complex programming or proprietary scripting. The UI customizations are separated from UI functional code and are stored in a specialized, reserved namespace in the solution’s metadata repository, ensuring that UI customizations are durable and survive patching and upgrades, eliminating the expensive merge and testing cycles often associated with customized interfaces.

Privileged Account Management

The seemingly endless stream of highly visible security breaches and public disclosure of classified information at major organizations and enterprises conspicuously exposed the existing problems with privileged user management. Organizations have sensitive systems and applications with highly privileged accounts or shared schemas whose passwords are shared by multiple administrators. These accounts are powerful by nature, which can prove disruptive to the business if not managed and monitored appropriately. Privileged users perform sensitive activities that involve extended access to corporate resources. In most companies, privileged accounts are not clearly defined, and different individuals often share some of these accounts. When privileged accounts are not tightly managed, they present a high security risk for the enterprise. In addition, regulations typically require enterprises to trace, authorize, track and audit all shared privileged account usage.

The number of privileged accounts grows with the number of servers, devices, and applications that need to be managed. In most large enterprises there are hundreds, sometimes thousands of privileged accounts for which multiple individuals know the username / password combination, which means organizations struggle to know who actually used a privileged account at a specific time. Because an inflation of privileged accounts is hard to manage, passwords are rarely changed thus compromising overall security and violating corporate password policies.

To address these challenges, Oracle Privileged Account Manager, an integral part of Oracles Identity Governance, provides the ability to associate an individual to the use of a privileged account. It provides self-service access to authorized privileged account passwords and tracks privileged account assignment and use across managed systems. From a compliance perspective, Oracle Privileged Account Manager contributes to securing Global Trade Management (GTM) strategies, in particular as they relate to compliance with regulations such as the Sarbanes-Oxley Act.

Oracle Privileged Account Manager (OPAM) is a server-based password vault designed to generate, and manage passwords and sessions for privileged users accessing specific systems and applications. Through secure session management, control and reporting, OPAM enables historical records to support forensic analysis and auditing.

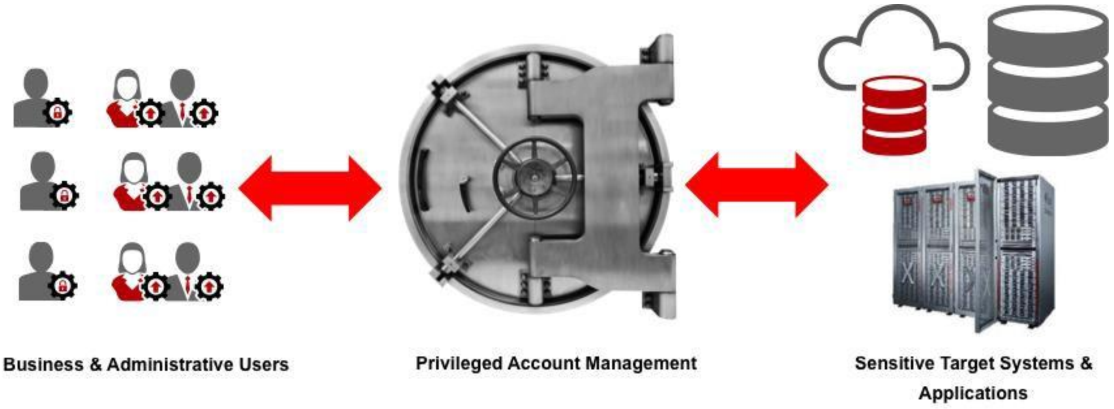

Business & Administrative Users
Privileged Account Management
Sensitive Target Systems & Applications

Figure 4. Oracle Identity Governance Suite – Privileged Account Management

For example as show in Figure 4, OPAM allows a privileged user, for example a system administrator or an application developer, to use a privileged account by “checking out” a password for a particular application, operating system, or database server. Once the password “check-out” is approved, the password is issued to the administrator. The administrator uses the credentials, then “checks-in” the password, indicating that the administrative task is complete. The system can be configured to automatically change the password on check-in, thereby precluding the administrator from reusing the same password again.

Also, *Break-glass* access enables administrators to request emergency access to privileged accounts they are not normally entitled to (the break-glass metaphor comes from breaking the glass to pull a fire alarm). Such a situation may occur when a critical server is down and the designated server administrator is not available. In this case, the administrator goes through the request process indicating a break-glass emergency request. Submission of the request kicks off a break-glass workflow with minimal or automatic approval (based on the customer’s processes and policies), which provisions the user to the privilege accounts LDAP group, allowing access to the privileged credentials. A special alert is generated for the event and is sent to security administrators. The access is automatically de-provisioned based on the security policies defined by the customer.

Every action of request, approval, check-in, checkout, who used it, when it was used, etc. are audited from a monitoring perspective. Privileged account information is also made available for identity certification, by allowing risk to be calculated on privileged accounts and how it was provisioned. Finally, the solution also provides out-of-box integration with Oracle Enterprise Single Sign-On to eliminate manual credential handling where secure passage of a token is not possible.

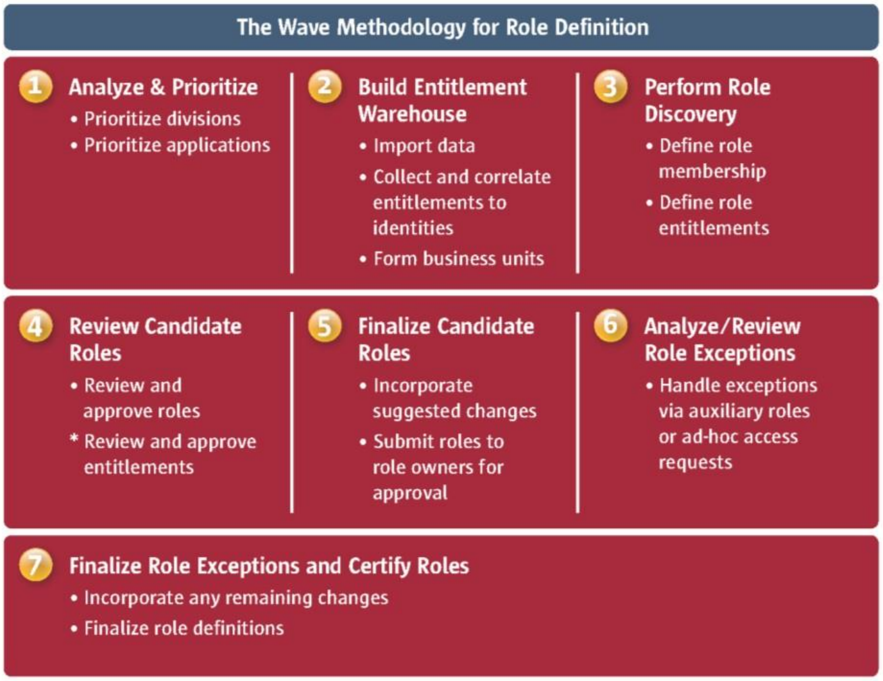
Role Lifecycle Management

Role lifecycle management is the process of defining and assigning roles to individuals who require access to organizational resources and of then managing their access according to those roles. Creating roles based on usage and enterprise policies enables greater visibility and better control. A limited number of appropriate roles make access much more manageable than dealing with a large number of individuals and infinite number of permutations of access rights. Role lifecycle management is therefore an efficient and effective way to address the challenges of access control for a large and constantly changing universe of users.

It all begins with the definition of Roles, and Oracle Identity Governance provides a unique combination of tools and methodology to allow organizations to define enterprise Roles, in addition to combining them with a robust Role based access control and role governance process. Role Discovery is a comprehensive set of market-leading role mining and analytics features that utilize a *hybrid approach* to discovering roles in the enterprise.

This hybrid approach leverages the combination of bottom-up (or user entitlements) and top-down (user HR attributes) access rights and business descriptions of users as part of its robust clustering algorithms to design suggested roles. Advanced analytics capabilities that showcase popularity of users in entitlements, role similarity comparisons, IT Audit violations within role definitions, percentage of users in engineered roles and so on, provides role engineers with comprehensive information to further refine role definitions.

Coupled with the industry leading *wave methodology*, which is a practical approach to Role Definition, Oracle Identity Governance provides a robust set of capabilities for organizations to solve their access control challenges.



The Wave Methodology for Role Definition

1 Analyze & Prioritize

- Prioritize divisions
- Prioritize applications

2 Build Entitlement Warehouse

- Import data
- Collect and correlate entitlements to identities
- Form business units

3 Perform Role Discovery

- Define role membership
- Define role entitlements

4 Review Candidate Roles

- Review and approve roles

* Review and approve entitlements

5 Finalize Candidate Roles

- Incorporate suggested changes
- Submit roles to role owners for approval

6 Analyze/Review Role Exceptions

- Handle exceptions via auxiliary roles or ad-hoc access requests

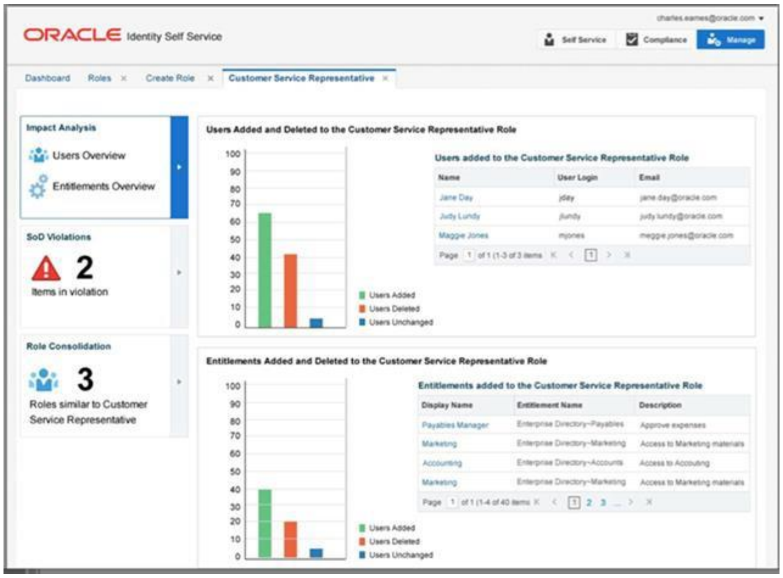
7 Finalize Role Exceptions and Certify Roles

- Incorporate any remaining changes
- Finalize role definitions

Figure 5. Oracle Identity Governance Suite – Wave Methodology for Role Definition

Based on years of experience in helping companies to adopt a role-based model for access control, Oracle's Wave Methodology for role definition, shown in Figure 6, has proven to be an effective method for engineering roles. This seven-step process walks administrators through 1) analyzing and prioritizing the divisions and applications most urgently requiring access controls, 2) building a warehouse to store data critical to effective role definitions, 3) performing role discovery, 4) defining policies for candidate roles, 5) finalizing candidate roles, 6) analyzing and reviewing exceptions to the roles, and 7) finalizing role exceptions and certifying the roles defined.

The solution also offers incremental role mining capabilities to take into account new applications being on-boarded or applications being phased out, allowing existing role definitions to be dynamically modified and to automatically update the role definitions. This ensures that the underlying role content always stays current and is available for assignment, provisioning and compliance.



Users added to the Customer Service Representative Role

Name	User Login	Email
Jane Day	jday	jane.day@oracle.com
Judy Lundy	jlundy	judy.lundy@oracle.com
Maggie Jones	mjones	meggie.jones@oracle.com

Page 1 of 1 (1-3 of 3 items

Entitlements added to the Customer Service Representative Role

Display Name	Entitlement Name	Description
Payables Manager	Enterprise Directory–Payables	Approve expenses
Marketing	Enterprise Directory–Marketing	Access to Marketing materials
Accounting	Enterprise Directory–Accounts	Access to Accouting
Marketing	Enterprise Directory–Marketing	Access to Marketing materials

Page 1 of 1 (1-4 of 40 items 1 2 3 ...

Enterprise roles, once defined, continue to evolve over time, and thus require a robust administration and audit process. The Oracle Identity Governance Suite provides role approvals upon detection of associated entitlement updates or termination of roles and performs real time impact analysis for role consolidation before changes are applied in a live environment. Role creation and modification approval processes, combined with rich analytics such as “what if” simulations and rollback, inline SoD violation detection and role consolidation metrics provides insight and educated decision-making, while enforcing accountability. As part of its role lifecycle management features, the solution fully audits all the changes made to role definitions including role assignment rules and entitlement mapping policies.

From a governance perspective, the Oracle Identity Governance Suite 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. The solution 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.

Identity Certifications

As shown in Figure 6, most organizations today struggle with satisfying stringent compliance mandates to perform access reviews (or certifications) of users with access rights to thousands of business applications and target platforms, let alone making the process a sustainable and repeatable exercise. In addition to meeting the challenge of scale, automation is the key to increasing the effectiveness and reducing the cost of compliance. Automation streamlines and accelerates the processes, by reducing the need to rely on help-desk and administrative resources and at the same time lowering the risk of manual errors 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.

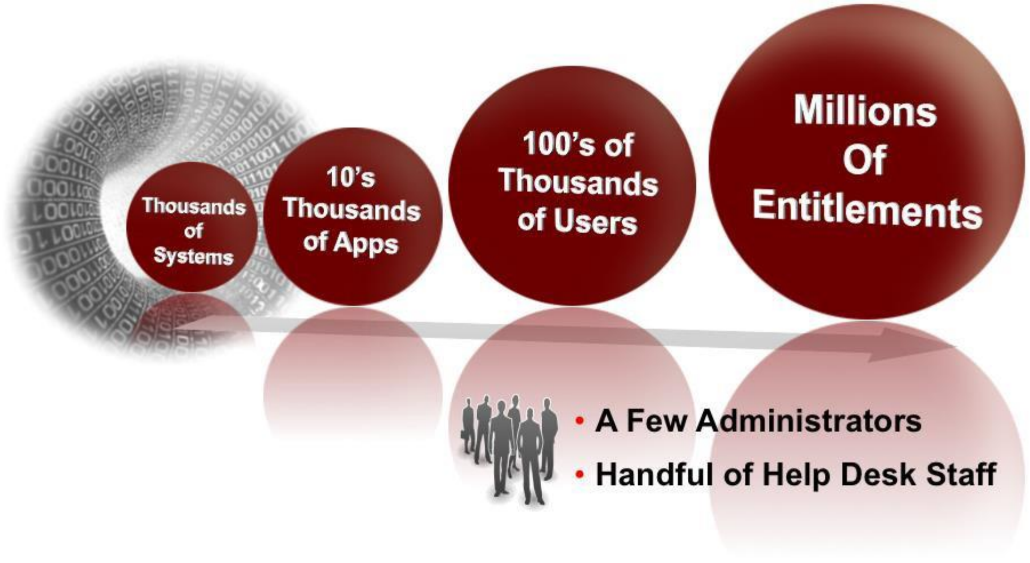


Figure 6. Dealing with the Challenge of Scale

With highly advanced identity intelligence capabilities, in-depth risk analytics, persona-specific business user friendly certifications and actionable dashboards, the Oracle Identity Governance Suite offers a robust set of Identity Certification features that provide a dramatic time and cost savings in access certification processes, and provide valuable insight to support business decisions. By automating access review and revocation processes, the solution helps control the overall cost of complying with regulations that mandate access controls, at the same time, reducing the need for resources devoted to performing compliance and audit activities.

The certification solution provides capabilities to automatically collect, correlate and audit identity data from multiple enterprise resources and applications, dynamically generating risk-based certification campaigns that are presented to business (i.e. managers) and IT reviewers (such as application owners, data owners and role owners), with their own personalized, business friendly UIs. Given that certification is an integral part of Oracle Identity Governance, it is built on the same foundation as the provisioning service, i.e. uses the same set of connectors for data loading, utilizes business context information from the access catalog, uses the same workflow orchestration and UI customization, and uses the same set of connectors to automate closed loop remediation workflows.

A spreadsheet-like view, provides advanced sorting and filtering capabilities and auto-certify options provide reviewers with the interactive tools they need to sustain large volumes of user access information in their attestation reviews.

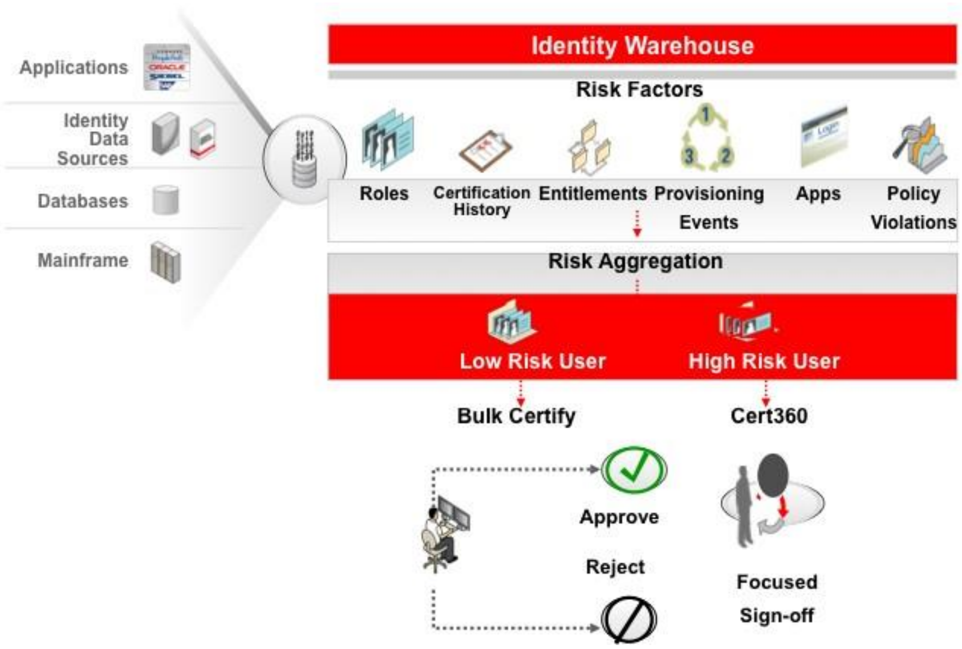


Figure 7. Oracle Identity Governance Suite – Risk Based Certifications

As shown in Figure 7, the solution provides a business-centric certification user interface and a certification campaign generation tool. When coupled with rich Identity Risk Analytics these tools provide reviewers with the contextual information they need to complete their certifications quickly. Risk aggregation and presentation across the user's identity lifecycle provides the core foundation of performing certification reviews in an efficient and sustainable manner. An end user's risk profile is determined with a clear High/Medium/Low Score associated to user roles, resources, entitlements and events - such as last attestation decisions, open audit violations and provisioning events. This allows reviewers to focus on "what matters most" to quickly prioritize and recognize high-risk user access, thus enabling smoother certification sign-off processes and improved user satisfaction.

In addition, the solution reduces operational risk exposure by providing reviewers with 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. The 360-degree view provides a holistic view of useful audit information such as previous certification decisions, rules or access policies used for assignment, role and entitlement metadata such as business glossaries and entitlement hierarchies, role usage analysis, IT Audit violations and so on, providing comprehensive forensics capabilities and actionable business context to reviewers to make intelligent certification decisions.

As part of the robust integration between certification and provisioning, reviewers can determine *how* the access was assigned to a user and using visual risk indicators, determine high risk provisioning events. For example, if access rights were provisioned to a user using access request, the reviewers can view in the certification, any associated approval trails, and qualify it to be a lower risk event. However, if access rights were assigned to users directly in the target platform or application, as part of provisioning reconciliation, those access rights are monitored and flagged as high risk provisioning events, given that they might be rogue assignments. All high-risk events are immediately flagged in certifications to allow reviewers to make intelligent decisions concerning user access. This significantly reduces costs associated with existing manual controls and enhances audit effectiveness, resulting in enforcement of *"least privilege access"* across the enterprise.

To meet the ever-growing demand of scale, innovative features such as allowing reviewers to export certifications to MS Excel files to complete offline are also supported. In addition, workflow based certifications for Business and IT teams to collaborate on a single certification campaign with advanced delegation capabilities are also included.

The use of roles lowers costs by reducing the number of objects that have to be managed for certification reviews and provides business reviewers with a better understanding of what they are attesting to. The solution provides *Role Vs. Actual* review capabilities that allow reviewers to quickly and efficiently attest to roles that users have access to, as well as the exception access rights, or the access rights that lie outside of the role assignments.

Incremental certifications, which allow reviewers to certify only the access rights that have been modified since the previous certification cycle, provide the means to further reduce the burden saving time and cost, while increasing efficiency.

Events such as employee transfers are common within an enterprise and the certification solution adapts to these events by dynamically generating event based certification reviews, focusing managers on new access assigned to transferred users, while ensuring unwanted access is automatically remediated, thus enforcing compliant provisioning activities.

Finally, the solution offers *closed loop remediation*, which provides an automated, end-to-end solution for reviewing and revoking access across target systems and business applications, automatically verifying remediation and alerting 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.

IT Audit Monitoring

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, which can be difficult to detect across computerized environments with automated workflows. To reduce this threat it is critical that organizations implement mechanisms to identify, notify and remove excessive access. IT Audit policies can ensure that conflicting combinations of roles, entitlements and responsibilities are not assigned to the same user. With the ability to define and enforce a security policy both within and across applications, Oracle Identity Governance delivers a comprehensive solution for enforcing these policies, with continuous IT Audit Policy Monitoring. 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. The enforcement process may be scheduled or executed on-demand. The solution features a robust notification and exception lifecycle management engine that enables designated remediators with the ability to take immediate action to cleanse these violations, via closed loop remediation or by providing compensating controls.

The IT Audit Monitoring engine can automatically identify imminent violations when users are provisioned especially after job changes that may affect their duties and maintains an ongoing record of activities with the potential impact of audit conflicts such as job changes, password resets, and so on.

Account Reconciliation & Rogue Detection

Account reconciliation is a key control objective for regulatory compliance, as it allows administrators to detect changes in access privileges originating outside the identity management system. These account changes are potentially rogue activities, and therefore trigger various remediation activities including exception approvals, certification cycles, and de-provisioning of entitlements or disabling accounts.

Accounts are linked to users' identities based on correlation rules. If the correlation rules are unable to link an account to an existing identity, administrators can map accounts manually. Typically, this happens for some of the older accounts that were created before a strict user ID generation policy was in place. After manual linking there may still be accounts that may not be linkable to any user identities. These accounts are typically either recognized as specialized privileged or service accounts or orphaned accounts. Accounts may become orphaned because they were created at a given point of time for some special purpose and may not be required anymore. Orphaned accounts can be de-provisioned directly and the process of automatic and manual linking, identifying accounts, and remediating orphaned accounts is typically part of data cleansing that is performed as the first phase of on-boarding a new application with Oracle Identity Governance. Periodic reconciliation can also help with detecting orphaned accounts created.

Audit & Reporting

Oracle Identity Governance provides comprehensive, actionable dashboards and advanced analytics capabilities based on user identity, access data and audit data residing in the Identity Warehouse of the solution. It 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, remediation tracking and other controls. While compliance dashboards are typically used for executive level compliance monitoring, detailed out-of-the-box reports using BI technology enable IT staff, business users and auditors to structurally analyze the wealth of identity data within their organization. The dashboards can further be customized for business users, compliance and audit officers and other end users as needed. The solutions data dictionary is also published to allow customers to extend these reports and dashboards and even build their own interfaces.

From a certification perspective, all completed certification data is archived for audit purposes. This provides detailed information to auditors regarding *who has and who had access to what* rights and whether revoked access rights were actually removed from target systems and applications. A robust certification history of every action taken on user access rights is also available, thus providing crucial information to organizations to successfully pass their audits.

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

- Roles assigned to Users within each business unit in the enterprise
- Accounts associated to Users within each business unit in the enterprise
- Roles and associated policies within each unit in the enterprise
- Lists of all entitlements, roles, applications and their owners
- 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 unit with no associated users and so on
- 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
- Orphan Account dashboards providing the ability to accurately determine rogue accounts or assign accounts to their rightful owners
- Remediation Tracking Dashboards providing a comprehensive audit trail of revoked access (during certification reviews) and their remediation status
- Identity Audit Violations with a comprehensive exception management audit trail displaying action taken by remediators to correct IT Audit exceptions caused due to toxic combinations of user access
- Reports detailing who checked out privileged account passwords over a given period of time

Conclusion

Organizations today face multiple challenges when balancing the need for users to require sufficient access rights to perform their job functions, but at the same time enforcing stringent governance processes to meet their compliance mandates. Oracle Identity Governance solves these governance challenges by providing a unique focus in Identity Governance by amalgamating access grants and access monitoring to ensure that while users are able to procure access when they need it via intuitive and business friendly self-service interfaces, there are sufficient preventative and monitoring controls in place to ensure that they have no more access than they need in order to fulfill their job responsibilities. This type of closed loop governance requires a comprehensive identity solution and Oracle Identity Governance uniquely distinguishes itself in its integrated capabilities, common data model and platform based architecture.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Hardware and Software, Engineered to Work Together

Oracle Identity Governance Business Whitepaper
August 2018

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